WHITE PAPER: BEST PRACTICES

Confidence in a connected world.

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

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 - The key consideration is resource utilization on the target machine, 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	X	X
Windows XP	X	X
Windows 2000 (SP3 and later)	X	
Windows 2008	X	X
Windows 2008 Small Business and Essential Business Servers		X
DATABASE		
Embedded	X	X
CLIENT		
Windows Vista	X	X
Windows 2003	X	X
Windows XP	X	X
Windows 2000 (SP3 and later)	X	X
Windows 2008	X	X
Windows 2008 Small Business and Essential Business Servers		X

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 non-production 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.*

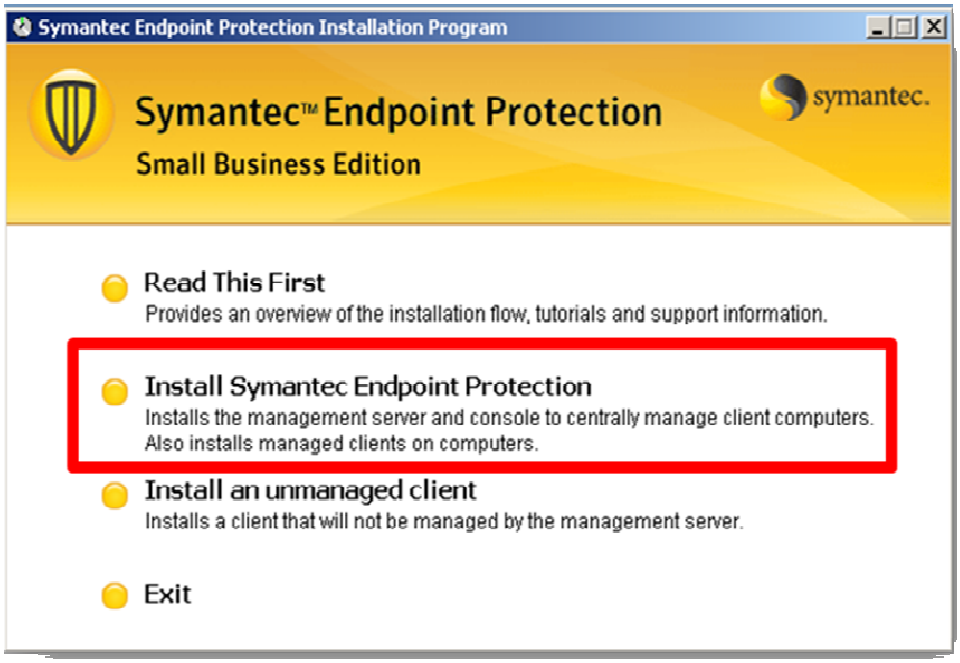
If you have a Symantec System Center and/or SAV Reporting Server installed on the SBS machine, they must be relocated through Add/Remove Programs before continuing. A reboot is not required.

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.

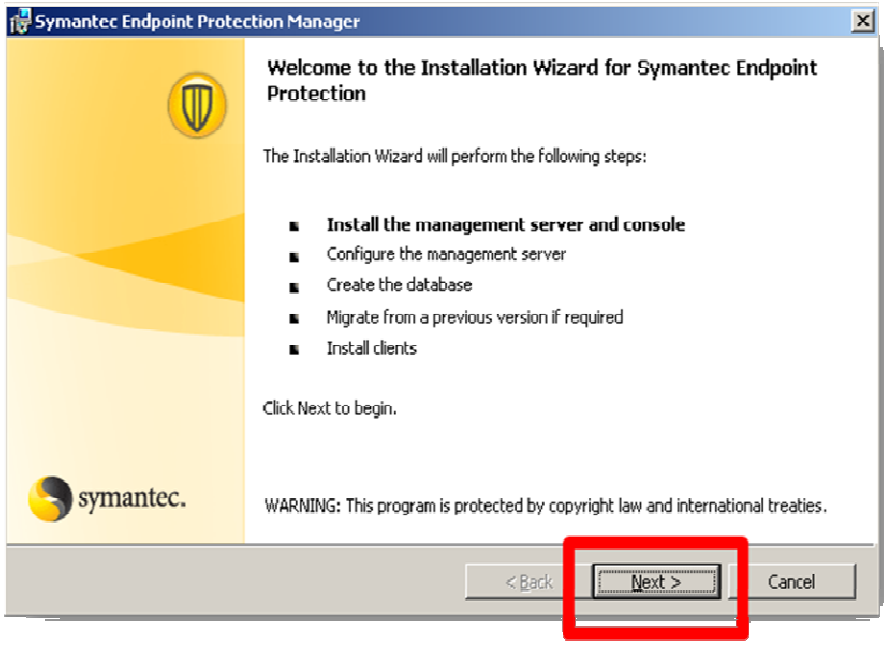
PHASE II SYMANTEC PROTECTION CENTER INSTALLATION (SPC)

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**:

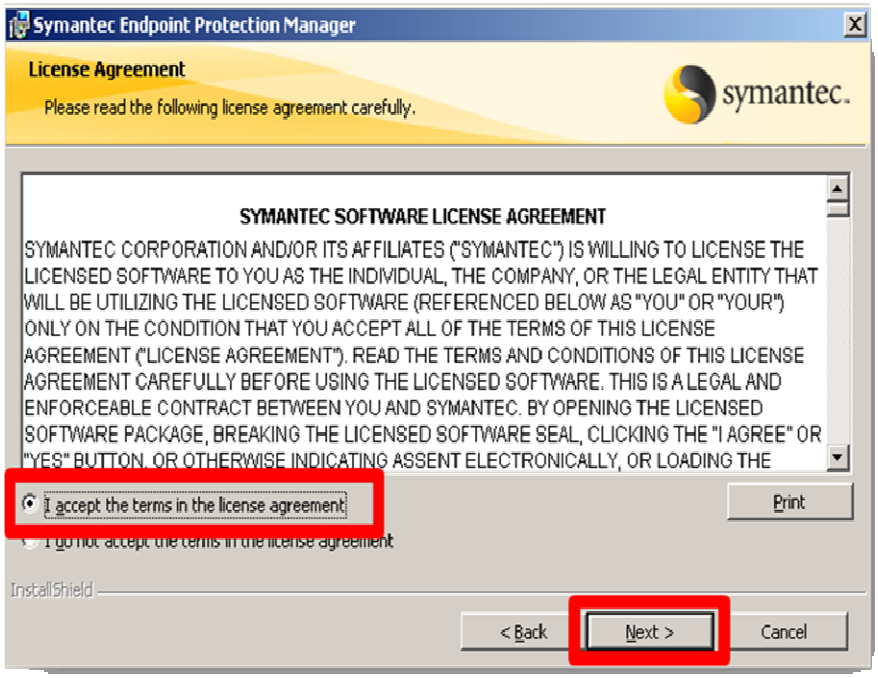
Locate and execute the **Setup.exe** file located on Disc 1 of the installation files. The installation menu should appear. Select **Install Symantec Endpoint Protection**.



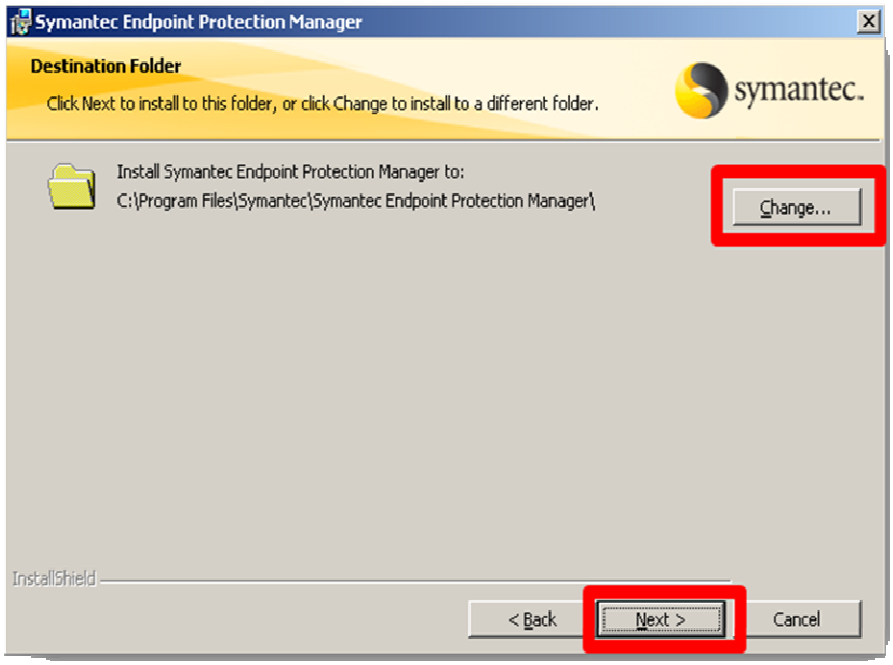
Select **Next**



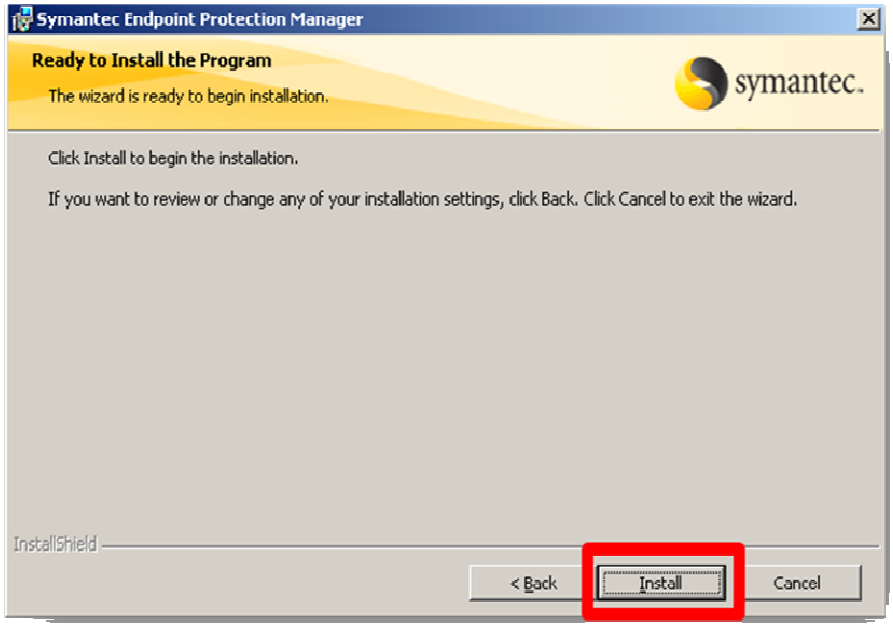
Select **"I accept the terms in the license agreement"** and then select **Next**



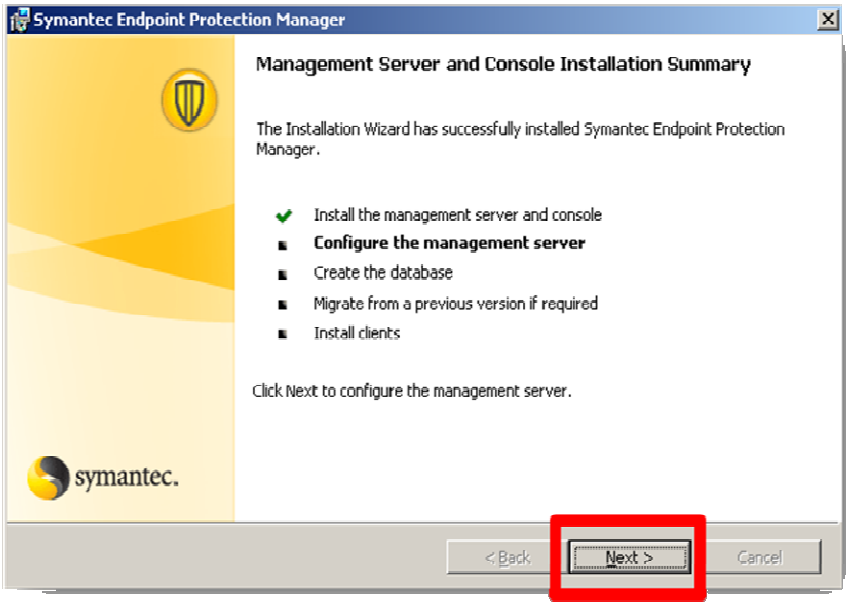
(Select "Change" if you need to change the path from the default and then select Next.



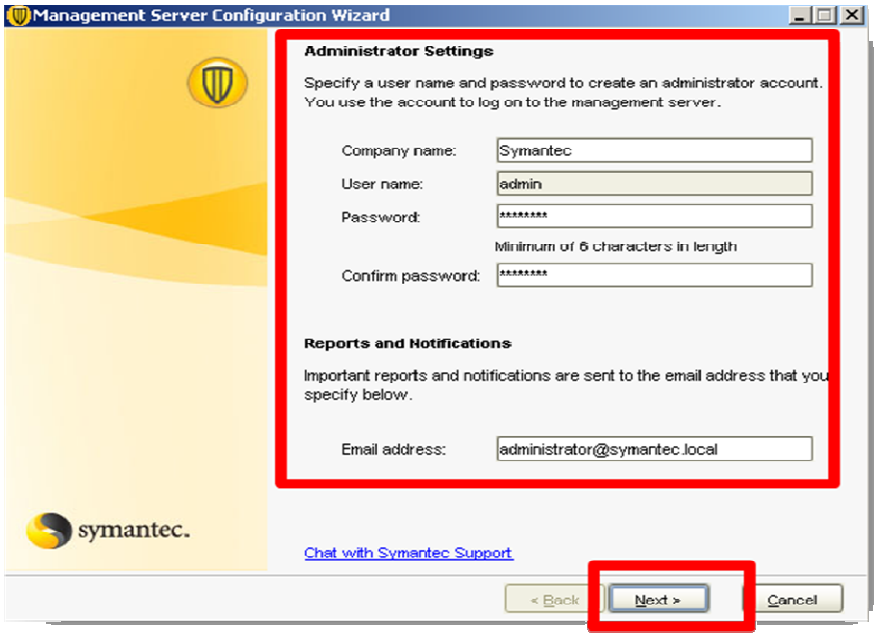
Select **Install**



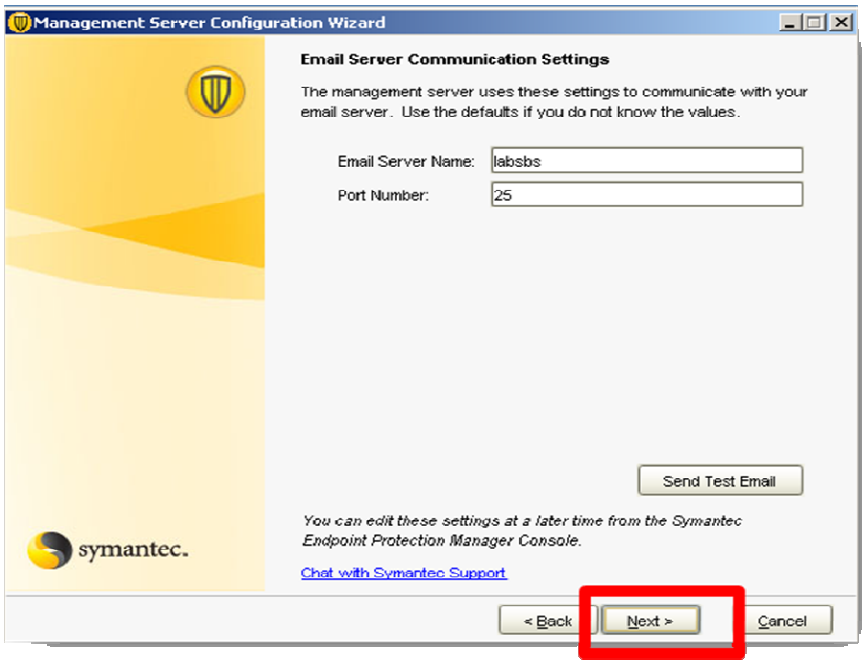
Select **Next**



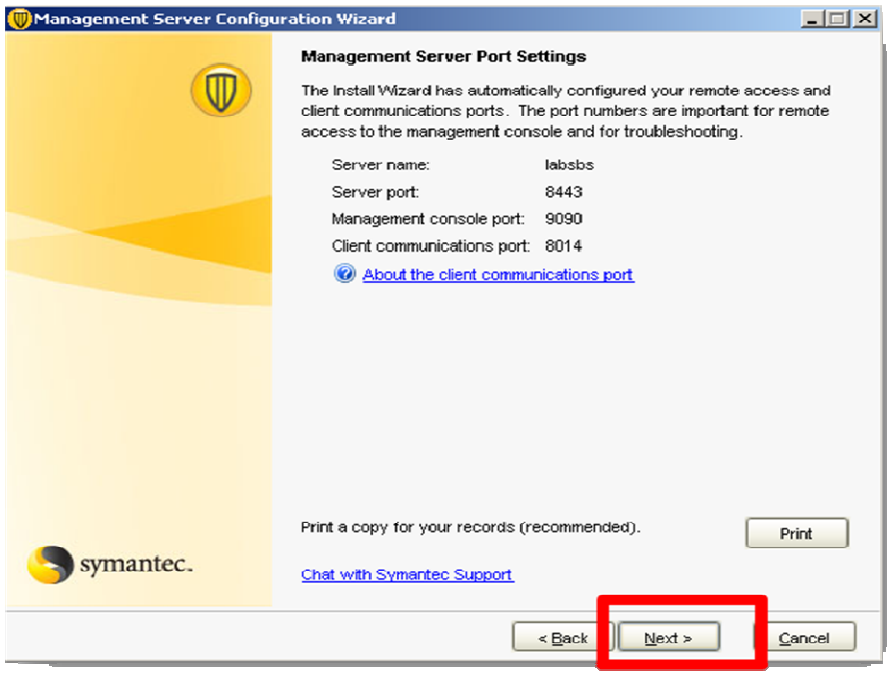
Enter your **Company Name** and **Password**. The User name will default to Admin which can't be changed at this time. Enter an **Email address** of an administrator that will receive notification messages. Symantec provides multiple notification messages out-of-box that will send Security Status information 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.**"



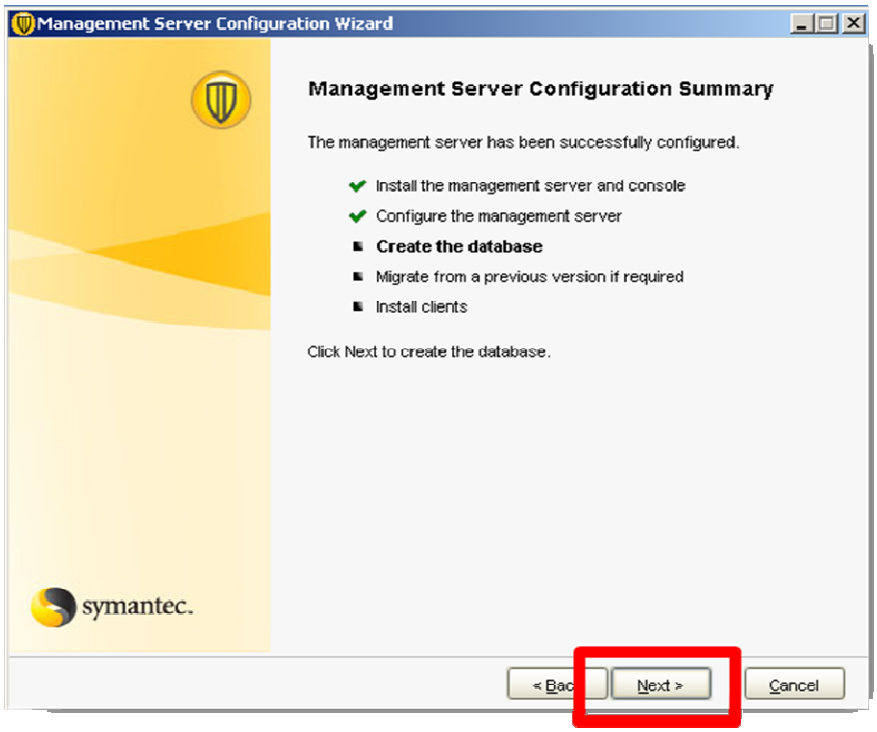
Verify that the **Email Server Name** and **Port Number** are correct and alter if necessary. If you do not know this information choose the defaults and select **Next**



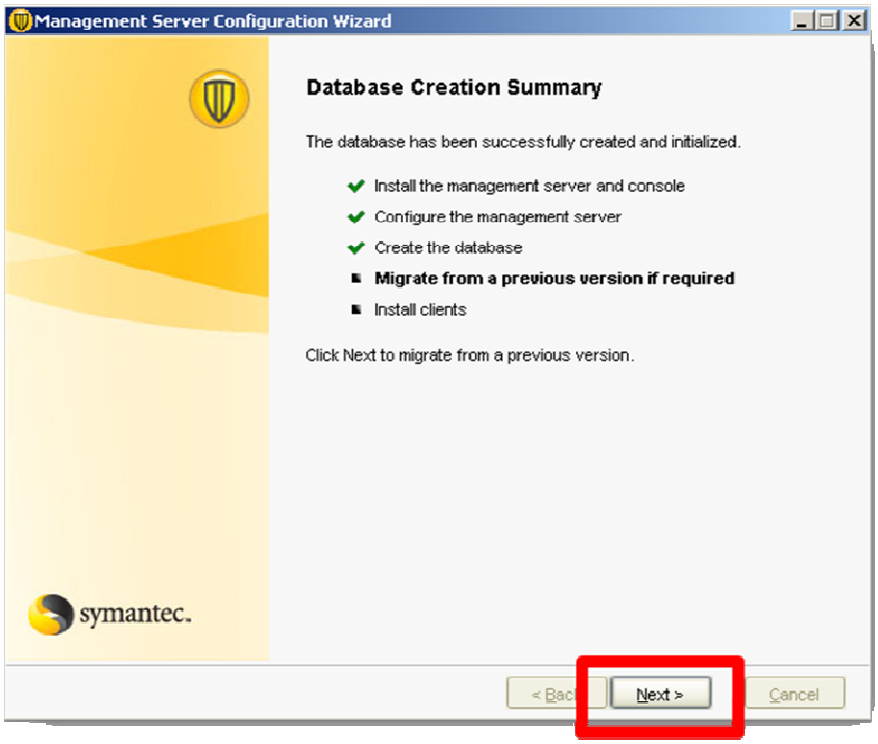
Select **Next**



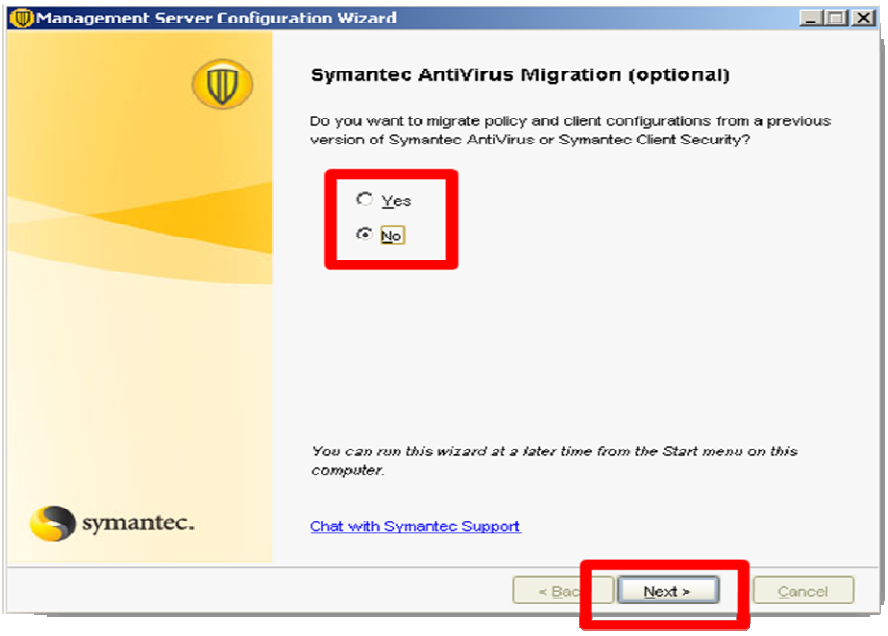
Select **Next**



Select **Next**

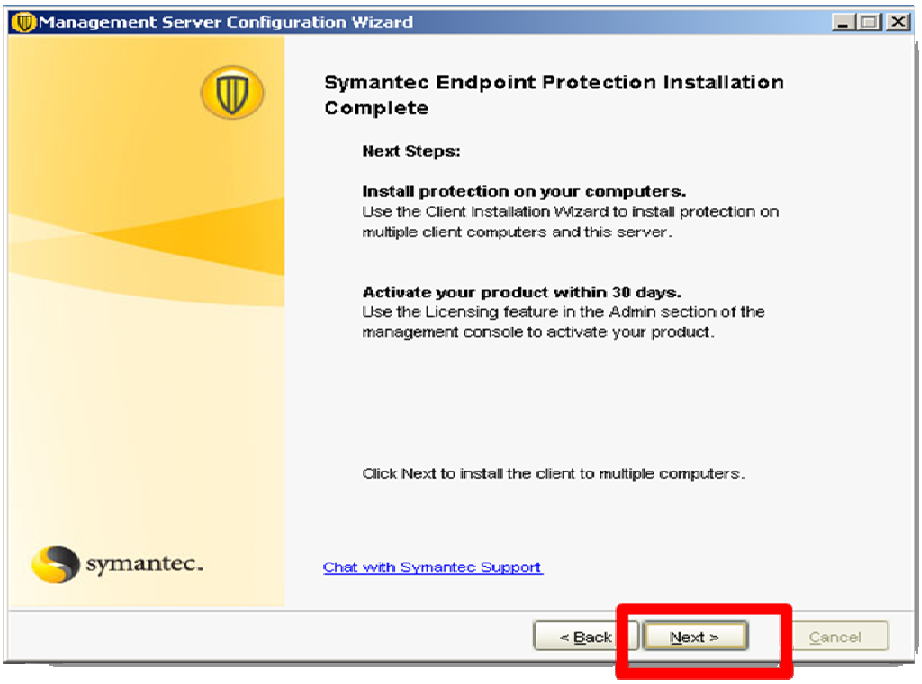


Select **Yes** if you wish to migrate the legacy SAV/SCS Group and settings into the SEP SBE 12 SPC. If you do not wish to do this at this time select **No**



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



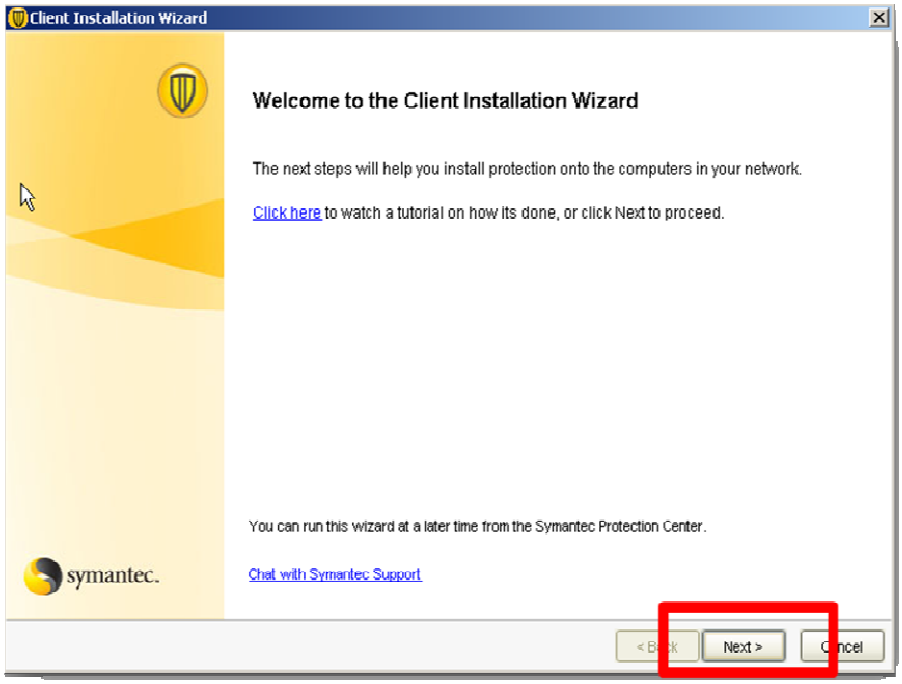
The installation of the management server has been completed. The Client Installation Wizard will now appear. You can deploy the Clients at this time. If you wish to deploy the Clients at a later time select cancel and continue to Phase III Post Installation Tasks.

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.*

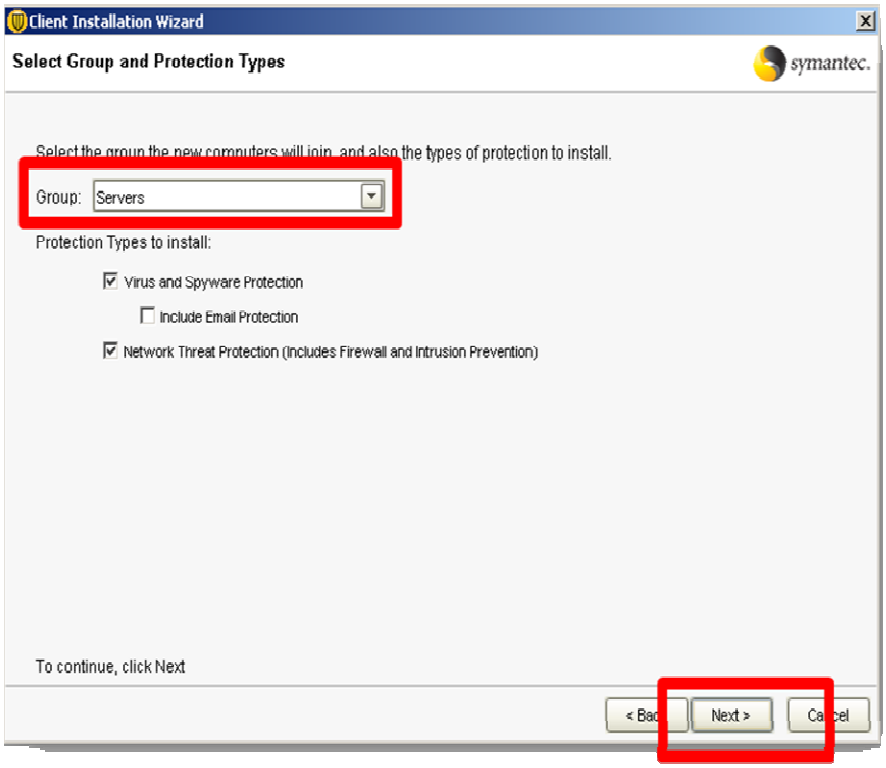
If the Symantec System Center (SSC) is installed it will need to be removed prior to the installation of the SEP SBE 12 Client.

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.

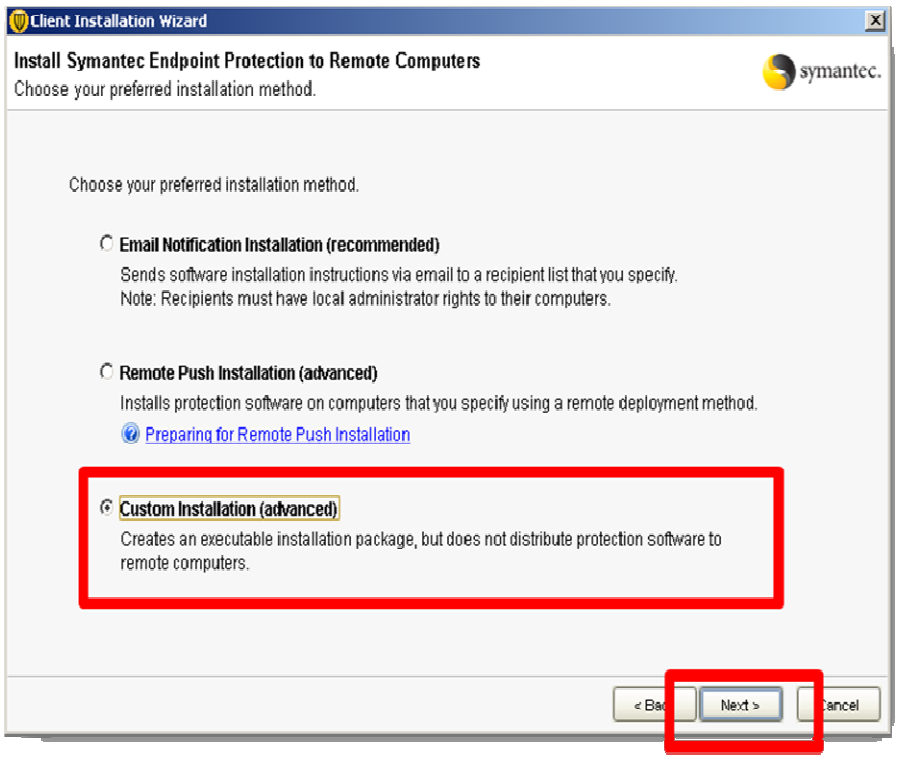
To install the Client on the Manager select **Next**



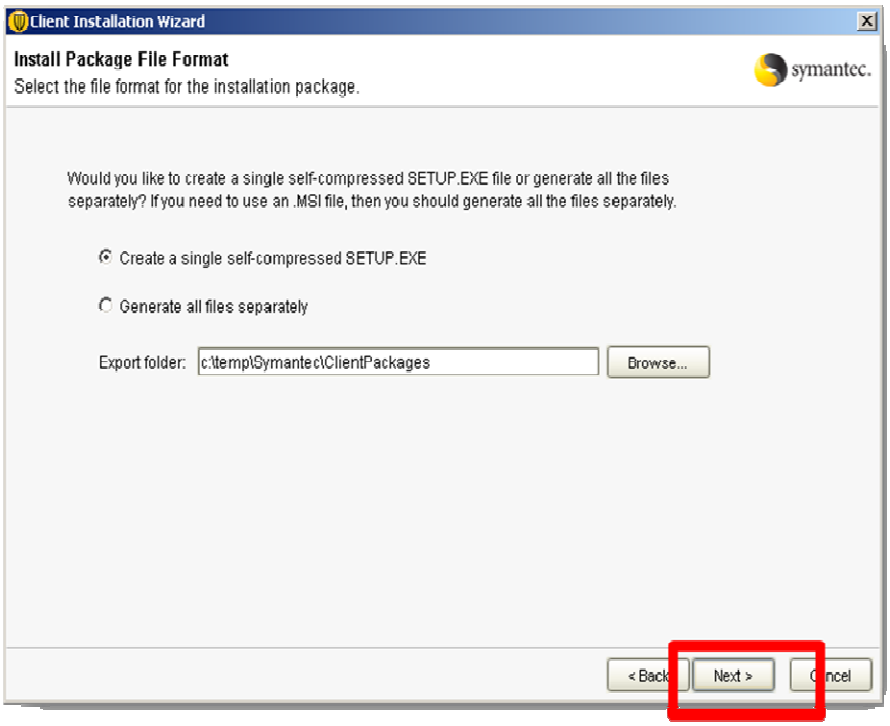
Select **Servers** from the dropdown list and select **Next**



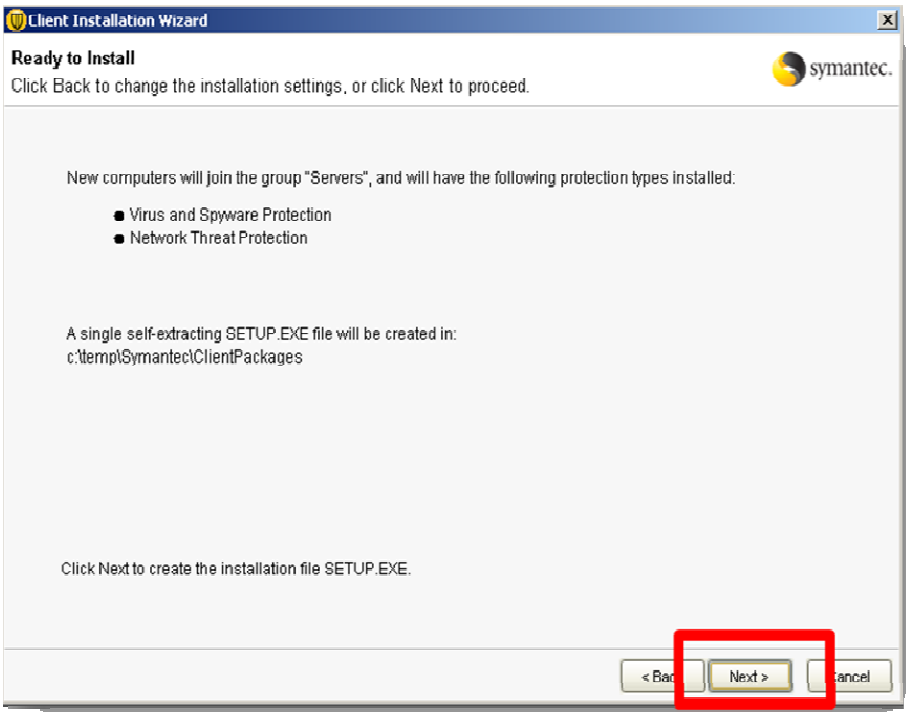
Select **Custom Installation (advanced)** and select **Next**



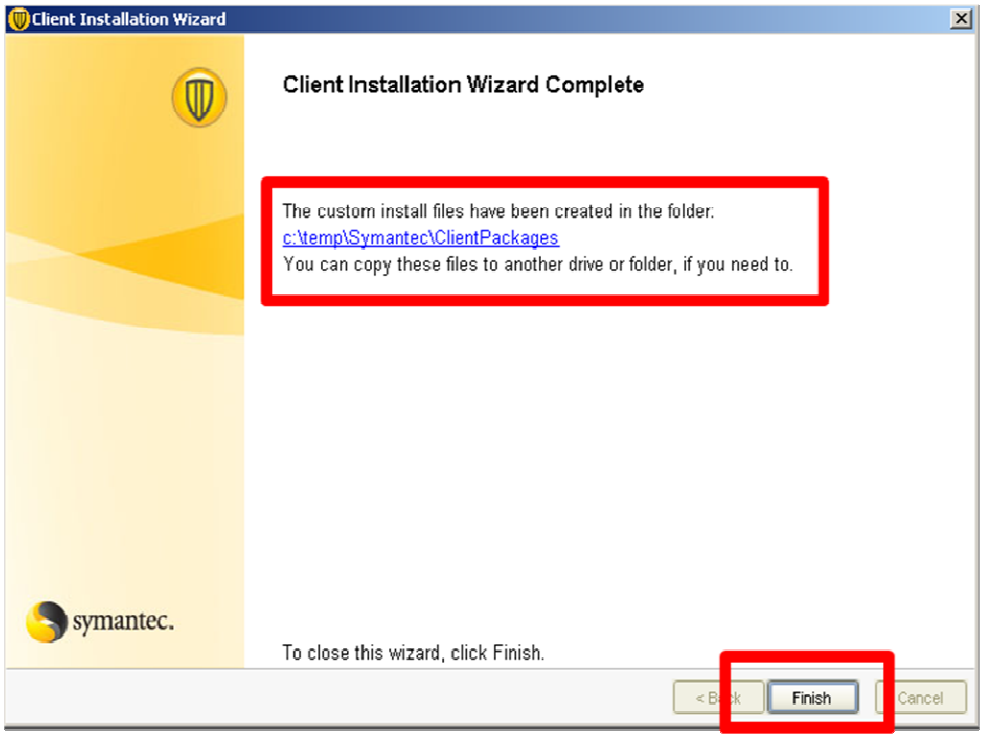
Select **Next**



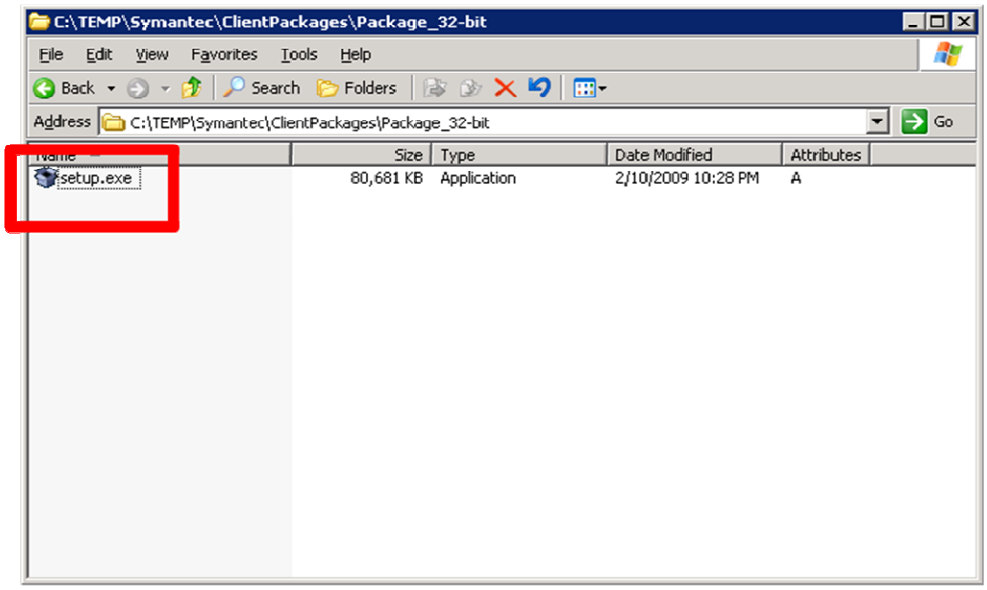
Select **Next**



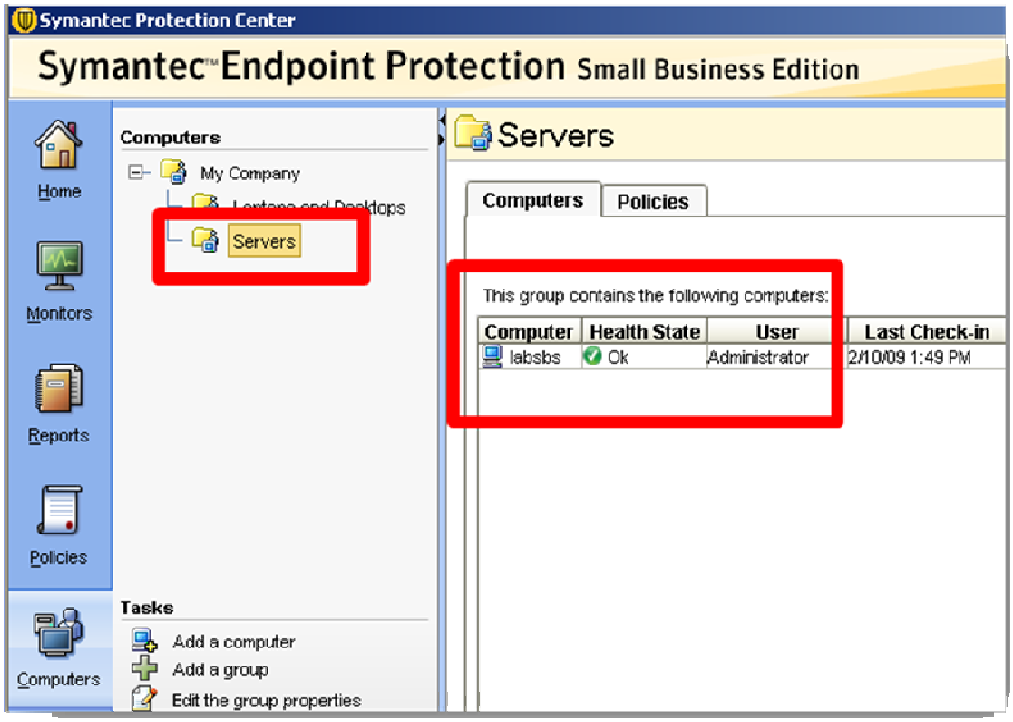
Click on the **c:\temp\Symantec\ClientPackages** link and Select **Finish**.



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



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.



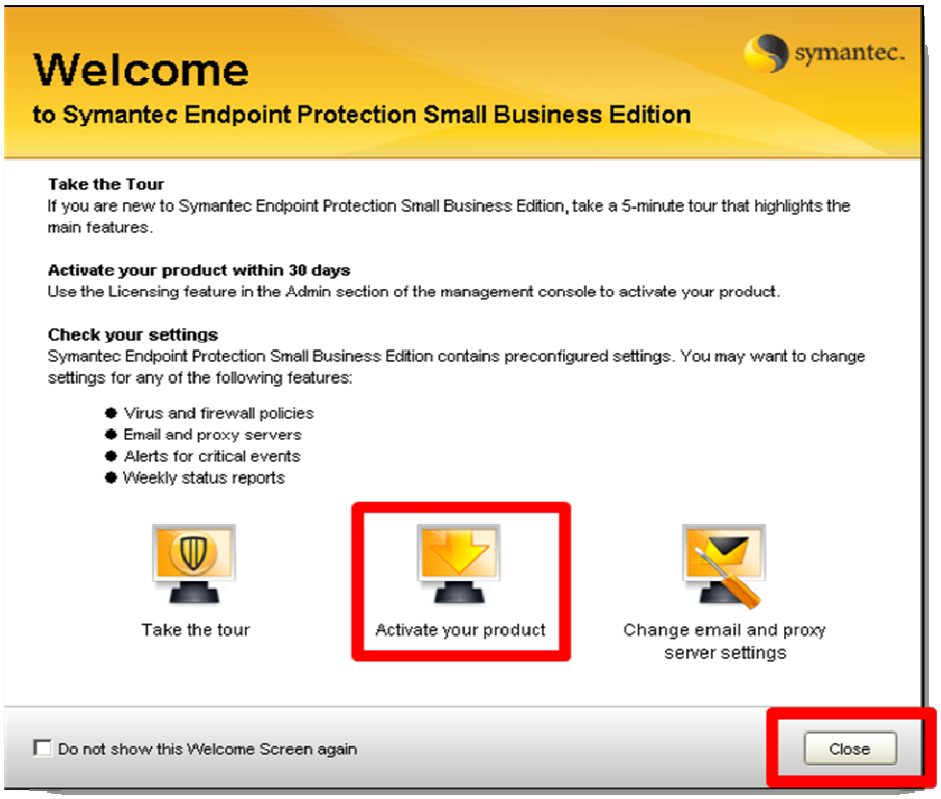
Note: *The Antivirus and Antispyware protection component will typically be active before reboot. However the Network Threat Protection components require a reboot. It is normal to not see the Network Threat Protection technologies under the Client UI until a reboot has been performed.*

PHASE III POST INSTALLATION TASKS

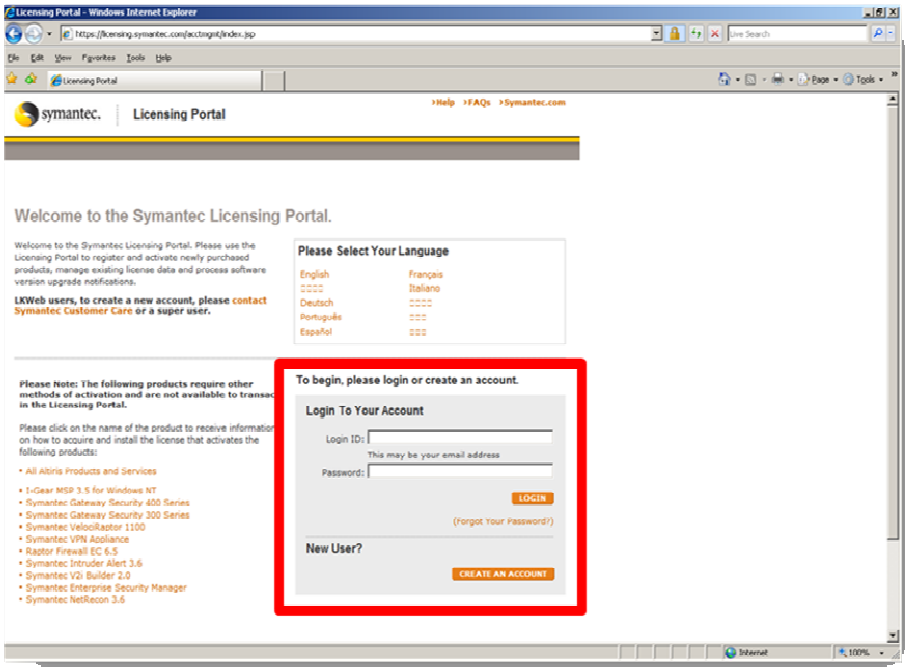
Once you have completed installation of the Manager and Client, you will need to register your serial number to obtain your license file and upload it to your Manager. Login to the Manager using the following credentials - **Username:** admin**, Password:** <specified earlier>

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,* ***http://(SBS Hostname_or_IP):9090****. Follow the instructions to setup the remote console on your machine.*

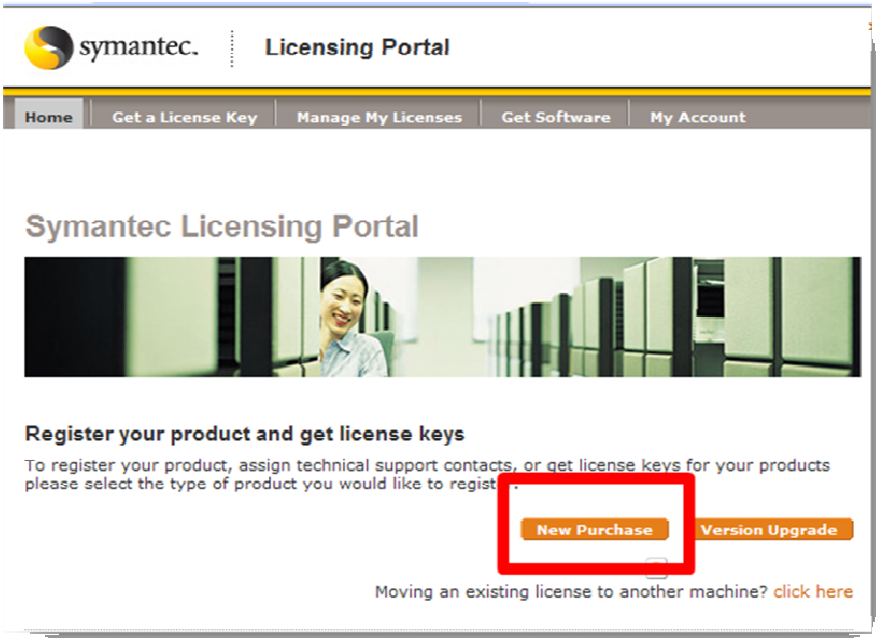
To register your serial number select **Activate your Product** from the Welcome Screen. You can also navigate to the **Admin Tab – Licensing Tab** and select **Register Serial Number** in the management console.



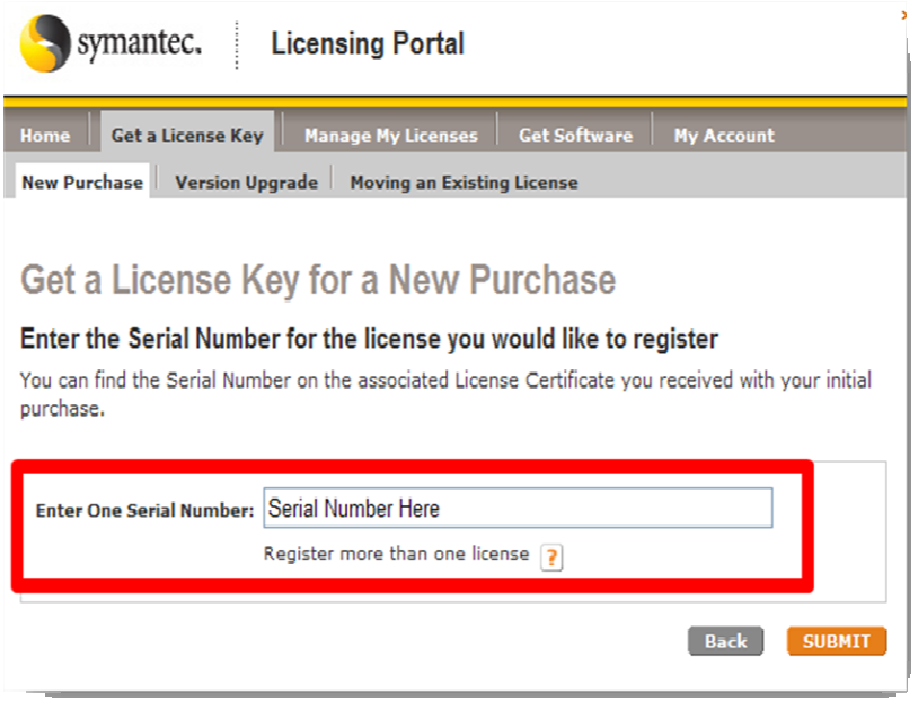
Enter your login credentials and select **Login** if you already have an account. If you do not have an account, select **Create An Account**. Once you have created an account a confirmation email will be sent to the email addressed specific during the account creation.



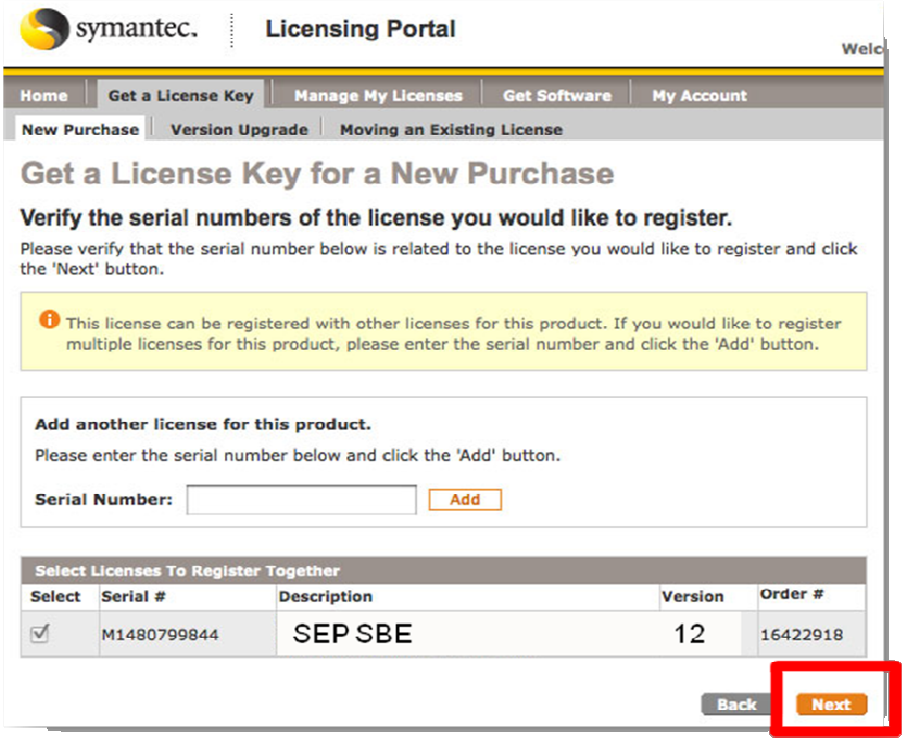
Select **New Purchase**



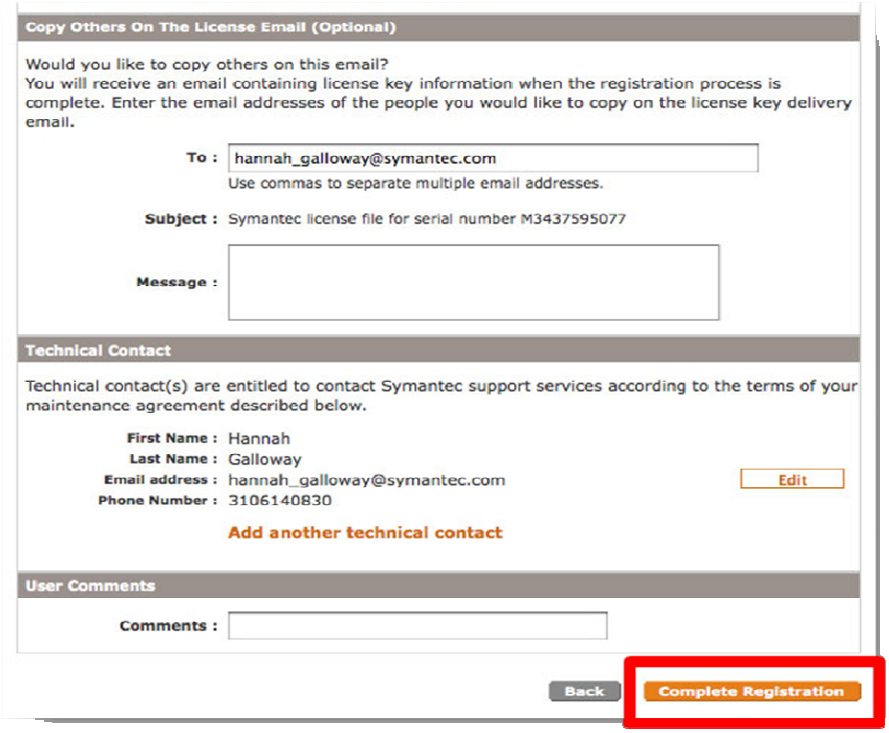
Input your **Serial Number**



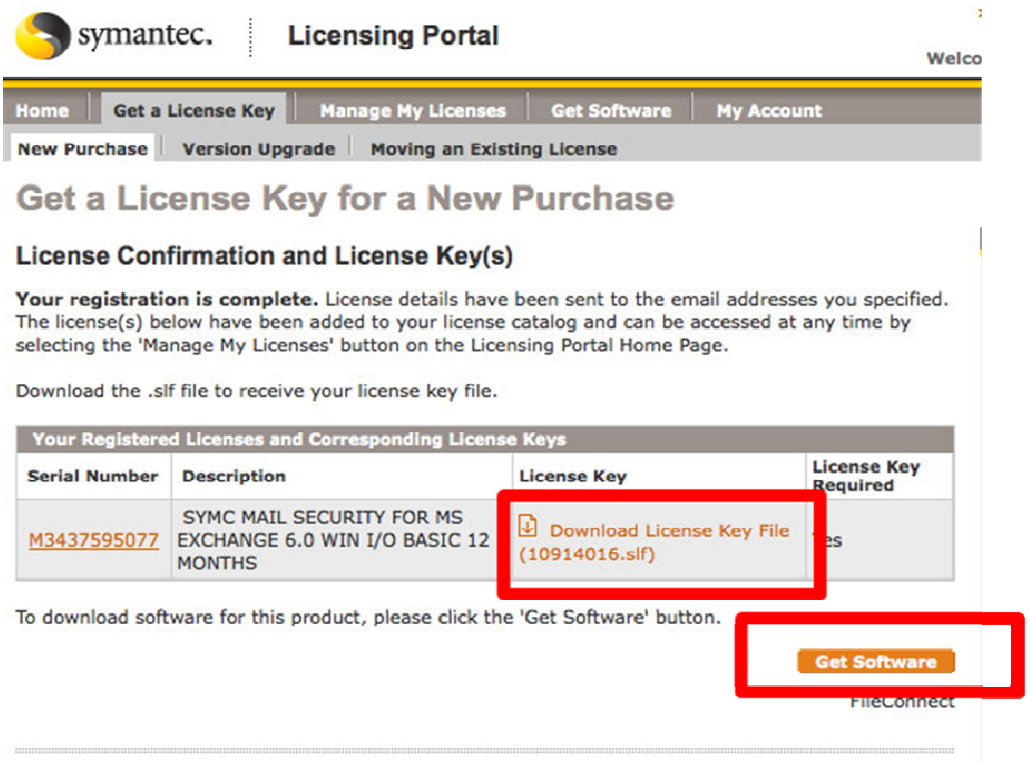
Select the SEP SBE 12 license and select **Next**



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



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



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: M3437595077
License Key: Download Attached Symantec License File(10914016.zip)

To download software for this purchase, go to: https://fileconnect.symantec.com

License Information:

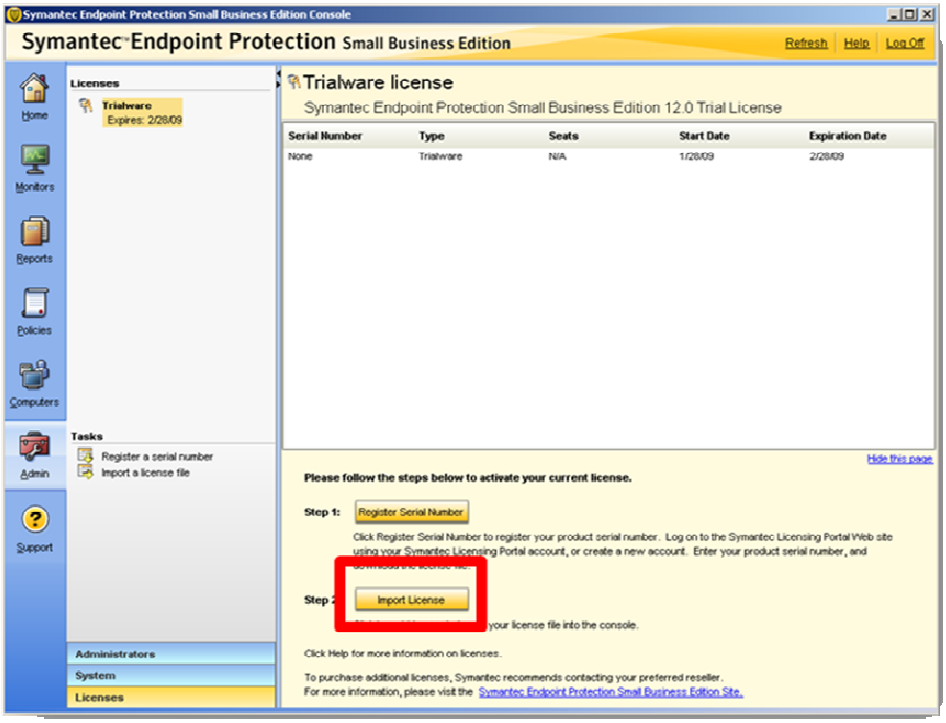
Order Details

Customer Name:	STARK INDUSTRIES
Customer Number:	58864454
Order Number:	16422918
Quantity Purchased :	2

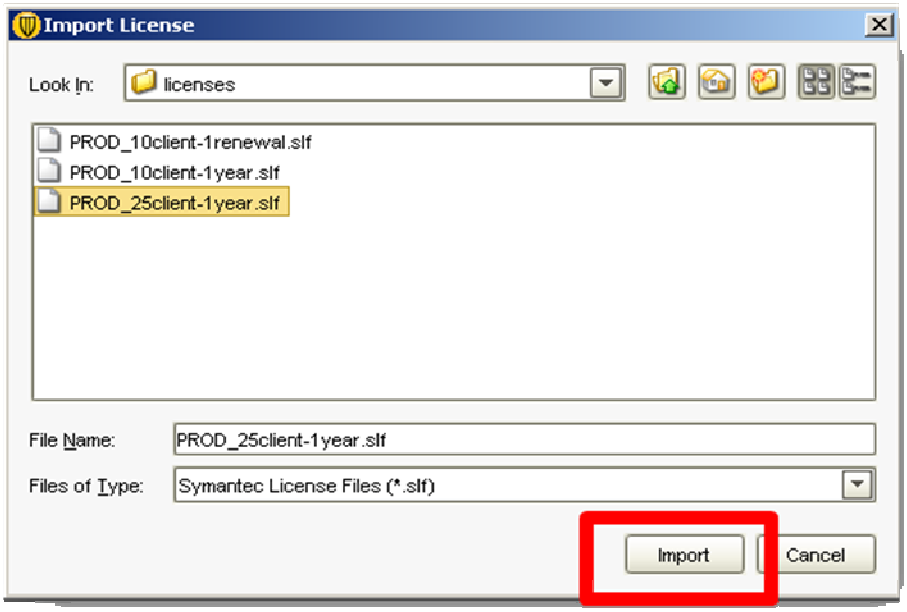
Installed At Address
26900 PACIFIC COAST HIGHWAY
MALIBU BEACH, CA 90265-9998
US

Instructions:
IMPORTANT Your license file is contained within the attached .zip file. This file must be opened using a decompression utility such as Winzip or Winrar. The .slf file contained within the .zip file is the actual license 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 Notepad or Wordpad as this will corrupt your license file and prevent your product from working properly.

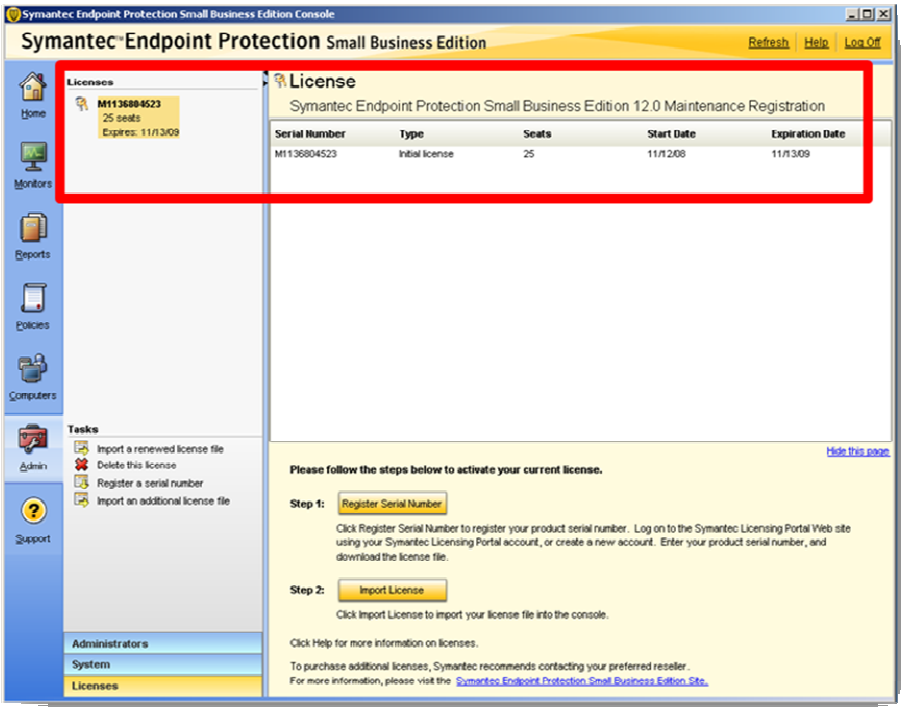
Now that you have your license file you can import it to your management console. To do this navigate to the **Admin Tab – Licensing Tab** and select **Import License**



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



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



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/ent-security.nsf/854fa02b4f5013678825731a007d06af/8cf31c11c88a96ce652574c00072b312?OpenDocument

How to configure Proxy Settings

http://service1.symantec.com/support/ent-security.nsf/854fa02b4f5013678825731a007d06af/5a8f40b6478675438825733e007163dd?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

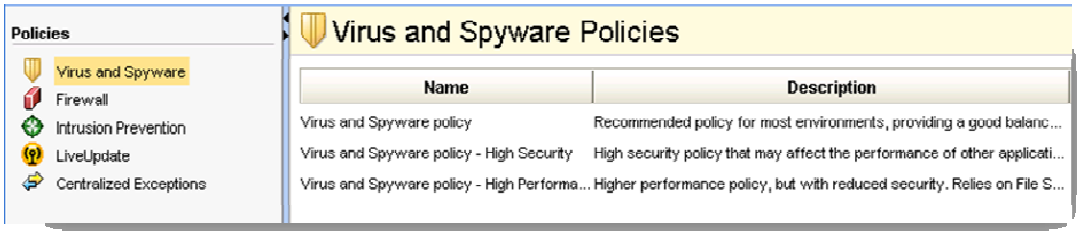
In most cases, very few changes are required or recommended for virus protection policies. Symantec always recommends running SEP SBE 12 with Auto-Protect enabled along with scheduled scans. The frequency and depth of the scheduled scan is usually best determined by analyzing the results of the scan. 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.



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 10.0.0.0/24, 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 **Appendix A**. 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/ent-security.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 Ini-Killer, Phase Zero, Stealth Spy	666 Satanz Backdoor	1001 Silencer, WebEx	1011 Doly Trojan	1170 Psyber Stream Server, Voice	1234 Ultors Trojan
1243 SubSeven 1.0 - 1.8	1245 VooDoo Doll	1492 FTP99CMP	1600 Shivka-Burka	1807 SpySender	1981 Shockrave
1999 BackDoor 1.00-1.03	2001 Trojan Cow	2023 Ripper	2115 Bugs	2140 Deep Throat, The Invasor	2801 Phineas Phucker
3024 WinCrash	3129 Masters Paradise	3150 Deep Throat, The nvasor	3700 Portal of Doom	4092 WinCrash	4567 File Nail 1
4590 ICQTrojan	5000 Bubbel	5000 Sockets de Troie	5001 Sockets de Troie	5321 Firehotcker	5400 Blade Runner 0.80 Alpha
5401 Blade Runner 0.80 Alpha	5402 Blade Runner 0.80 Alpha	5400 Blade Runner	5401 Blade Runner	5402 Blade Runner	5569 Robo-Hack
5742 WinCrash	6670 DeepThroat	6771 DeepThroat	6969 GateCrasher, Priority	7000 Remote Grab	7300 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 HackÂ´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					