



Symantec Endpoint Protection 11.0

Windows Small Business Server 2003
Best Practices White Paper

Updated for Maintenance Release 2 - March 2, 2007

Contents

Scope.....	3
What is Microsoft Small Business Server (SBS) 2003?	3
What is Symantec Endpoint Protection (SEP) 11.0?	4
General note on compatibility	5
Recommended hardware.....	5
Phase 1: Planning and Preparation	5
Phase 2: Installing and configuring the Symantec Endpoint Protection Manager	6
Phase 3: Importing and assigning the Windows Small Business Server 2003 specific policies	8
Phase 4: Installing the Symantec Endpoint Protection client.....	9
Phase 5: Recommended post-installation tasks	9
What to expect from this point onward.....	10
Potential issues.....	11
Symantec provided template policies	12
Identifying running processes	12
Frequently Asked Questions	13
Useful Online Resources	15

Important! The latest version of this document can always be accessed via the following Symantec webpage:
http://www.symantec.com/enterprise/stn/articles/article_detail.jsp?articleid=symantec-endpoint-protection-11

Scope

This white paper focuses primarily on providing guidance on how to successfully deploy the core Symantec Endpoint Protection 11.0 management and protection components to a Microsoft® Small Business Server 2003. This white paper does not discuss in detail the topics of upgrading the Symantec Endpoint Protection components from a previous version, deploying Symantec Endpoint Protection 11.0 to workstations and other more general administration concerns; for guidance on these topics, please refer to the [product documentation](#). Note also, to date the content of this document has only been validated with the US English version of both Windows Small Business Server 2003 and Symantec Endpoint Protection 11.0.

What is Microsoft Small Business Server (SBS) 2003?

Microsoft Windows Small Business Server 2003 is a version of Windows 2003 server with tailor made wizards and management tools designed with ease of use in mind for the small business market. SBS includes, as standard, many common, popular Microsoft server applications. There are two different versions of SBS 2003, standard and premium. The matrix below shows which key server applications are included with each:

Component	Standard SP1	Premium SP1	Standard R2	Premium R2
Exchange 2003	✓	✓	✓	✓
Sharepoint Services	✓	✓	✓	✓
Windows Server Update Services	✓	✓	✓	✓
SQL Server 2000 Standard Edition		✓		
SQL Server 2005 Workgroup Edition				✓
ISA Server 2004		✓		✓

Some points to note (primarily intended for those who are not so familiar with Microsoft Small Business Server):

- A Windows Small Business Server 2003 can perform most of the typical roles associated with a Windows 2003 server, such as Active Directory domain controller, file server, DNS server, DHCP server, web server (IIS), etc.
- Microsoft recommends SBS for a maximum of 75 users/workstations, and after that customers need to migrate to full versions of the provided Microsoft server software.

- The original Windows Small Business Server 2003 (not SP1 or R2) included ISA 2000, not ISA 2004.
- Windows Small Business Server 2003 is available in 32-bit versions only, no 64-bit support.
- Even though more complete versions of MS-SQL are provided with Premium, typically the provided install wizards for the server applications that require a database will utilise MSDE 2000 instances by default.
- Two database instances are setup by default, MSSQL\$SBSMONITORING (disabled by default) and MSSQL\$SHAREPOINT.
- Windows Small Business Server 2003 R2 comes with a customised version of Windows Server Update Services (WSUS) 2.0 on the SBS CDs. It provides the same core functionality but also includes simplified administration and reporting views.
- On an SBS 2003 machine, Windows Server Update Services 2.0 and 3.0 create a new website in IIS called 'WSUS Administration', which is configured to listen on TCP port 8530.
- If installed, by default Windows Server Update Services 2.0 (from SBS CDs) utilises a MSDE instance called MSSQL\$WSUS.
- If installed, by default Windows Server Update Services 3.0 utilises a custom version of MSDE 2000 called "Windows Internal Database". This is essentially a version of MSDE with no restrictions on the size of the database or the maximum number of allowable concurrent connections.
- If installed, by default ISA Server 2004 utilises a MSDE instance called MSSQL\$MSFW.
- Much of Microsoft Small Business Server's server software heavily utilises Internet Information Server.

What is Symantec Endpoint Protection (SEP) 11.0?

Symantec Endpoint Protection 11.0 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 agent and management console, increasing protection and helping lower total cost of ownership.

Specifically, Symantec Endpoint Protection 11.0 provides the following protection technologies:

- Antivirus and Antispyware
- Firewall
- Intrusion Prevention (both Network and Host based)
- Device Control
- Network Access Control (optional add-on)

The core components required to run a centrally managed Symantec Endpoint Protection 11.0 environment include:

- Symantec Endpoint Protection client (on each machine you wish to protect, including the Manager)
- Symantec Endpoint Protection Manager (a web server, utilising Microsoft IIS and Apache Tomcat)
- Database (by default, the SEPM automatically installs an embedded database, based upon Sybase Adaptive Server Anywhere version 9)
- Symantec Endpoint Protection Manager console (Java-based, can be run from anywhere with network access to the Manager)

General note on compatibility

It is very possible to run a Symantec Endpoint Protection Manager and Symantec Endpoint Protection client on the same machine as a Microsoft Windows Small Business Server 2003. By default, there are no technical conflicts between the two. If you are considering this approach, the key consideration is resource usage on the target machine, plus as a general best practice, good planning and preparation are also strongly recommended (this document will provide guidance on those topics).

Recommended hardware

While every environment varies, below are some high-level guidelines on recommended (not mandatory) hardware that will help to ensure the Windows Small Business Server 2003 machine will run smoothly with Symantec Endpoint Protection 11.0:

Processor	Dual-Core / Dual CPU
Memory	1.5GB RAM (total installed in the machine)
Disk space	5GB of free disk space (mostly to allow room for the database to grow over time) Note: At least 500mb of free space is required on the system drive (usually C:) as temp space, even if not installing to this drive.

Important! It is strongly recommended that you take some time to review how utilised the resources are currently on the target machine before moving ahead with the installation of the Symantec Endpoint Protection 11.0 components, especially memory and processor. Below are some guidelines on how much memory the components require on average:

- **Symantec Endpoint Protection Manager (including Database)** – Approximately 250MBs
- **Symantec Endpoint Protection client** – Between 25MBs (idle) and 50MBs (running content update or scan)
- **Symantec Endpoint Protection Manager Console (when in use)** – Approximately 100MBs

Note: The Console can be run from a remote machine also. See the "[Frequently Asked Questions](#)" section for more detail.

If you believe the resource requirements to run Symantec Endpoint Protection may be too high for your Windows Microsoft Small Business Server, it is possible to run Symantec AntiVirus Corporate Edition 10 as an alternative. See the "[Potential Issues](#)" section for more details.

Phase 1: Planning and Preparation

- Take time to familiarise yourself with the software: Read the [product documentation](#) and it is strongly recommended to also test all core components completely in a non-production environment (ideally one which has at least a very similar configuration to that of your production SBS environment).
- As a precaution, ensure you have a complete backup of your existing Microsoft Windows Small Business Server 2003 environment, and ensure the backup has been tested and confirmed to work.
- Schedule to do the actual installation to your production Windows Small Business Server 2003 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.
- If another vendor's antivirus or firewall product is currently running on the Windows Small Business Server 2003, this will need to be removed in advance of installing the Symantec Endpoint Protection 11.0 software.
 - If this means the server will be unprotected for a short period of time, you could consider unplugging the server from the network for the duration of the installation work, and carry out the installation locally on the server.
- **Important!** Ensure you are installing **Symantec Endpoint Protection 11.0 Maintenance Release 2**, which contains a number of significant improvements since the previous releases. To download Maintenance Release 2, via a web browser, go to <https://fileconnect.symantec.com> and enter a valid serial key (which you received when you purchased the software) when prompted to do so.

Phase 2: Installing and configuring the Symantec Endpoint Protection Manager

Important! If a Symantec Antivirus primary/parent server version 10 or 9 is running on the Windows Small Business Server 2003 machine, please be aware:

- It is strongly recommended that you review the following online migration tutorial before continuing:
http://www.symantec.com/business/support/endpointsecurity/sep11x_topic2/index.htm
- Installing the Symantec Endpoint Protection Manager will not replace/upgrade an existing Symantec Antivirus Server version 10 or 9. They will run in parallel as part of a phased migration.
- Installing the Symantec Endpoint Protection client later on (in Phase 4) will replace an existing Symantec Antivirus Server version 10 or 9.
- If you have a Symantec System Center and/or Reporting Server installed on the SBS machine, they should be removed through Add/Remove Programs before continuing (no reboot required). Please note though:
 - If you still require a Symantec System Center available, it can be installed on a remote machine.
 - All historical data from the Reporting Server will be lost at this time.

1. Insert the Symantec Endpoint Protection 11.0 CD into the CD/DVD drive, the CD should auto run and the menu should appear.
2. Click **Install Symantec Endpoint Protection**
3. Click **Install Symantec Endpoint Protection Manager**
4. A wizard will launch and a welcome dialog will appear, click **Next**
5. Select **I accept...** then click **Next**
6. Select the location to which you wish to install the Symantec Endpoint Protection 11.0 Manager, then click **Next**
7. **Use the default website** will be selected by default, click **Next**

Note: Selecting **Use the default website** will ensure the Windows Small Business Server 2003 application websites that utilize the IIS Default Website will continue to run as normal.

8. Click **Install** to kick off the installation. This can take up to 5 minutes to complete. When prompted, click **Finish**.
(At this point, the **Management Server Configuration Wizard** will launch automatically)

9. Ensure the **Simple** configuration type is selected, then click **Next**

(This will ensure the Symantec Endpoint Protection Manager is configured to suit an environment with less than 100 clients to manage)

Note: If you are upgrading from a previous version of the Symantec Endpoint Protection Manager, it is normal to not see this dialog. See the “[Frequently Asked Questions](#)” section for more detail.

10. Enter a password and email address for the admin user, click **Next**

(Configuration will begin and can take up to 5 minutes to complete)

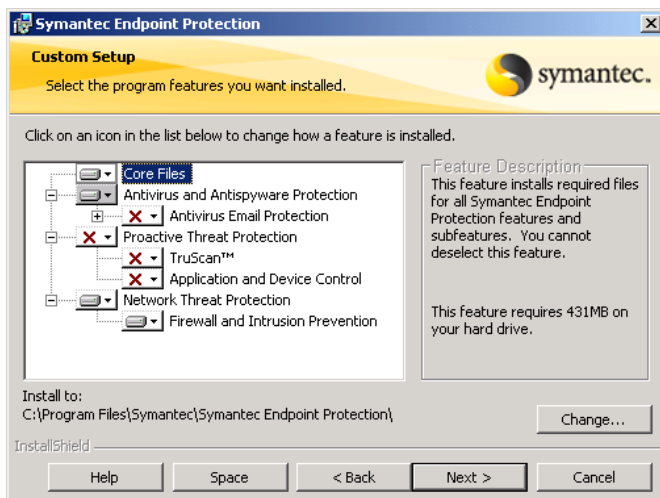
11. When prompted, ensure **Yes** is selected, then **Finish** (The Migration and Deployment Wizard will launch automatically)

12. The Welcome dialog will appear, click **Next**

13. Ensure **Deploy the client is selected**, click **Next**

14. Select **Specify the name of a new group...** and enter a name of **Microsoft Small Business Server**, then click **Next**

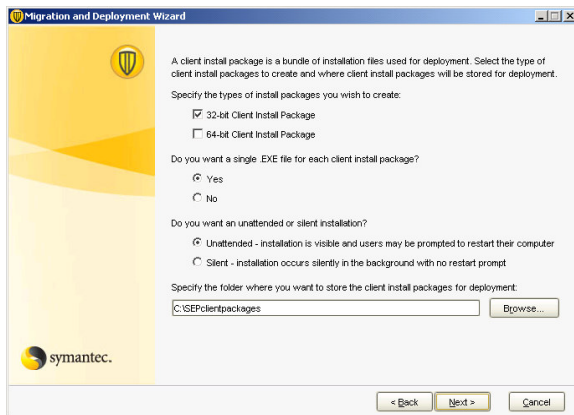
15. Select specifically the features shown below, then click **Next**



Note:

- The behavior-based **TruScan** feature of the Proactive Threat Scan component is **not** supported on Server operating systems currently, therefore it is recommended that this feature **should not be selected** for this client installation package.
- The **Antivirus Email Protection** features are aimed at providing additional protection to client-side email applications such as Microsoft Outlook and Lotus Notes, therefore if you won't run these directly on the Small Business Server, these **features should not be selected**.
- **If you are currently running the ISA 2004** firewall on the Microsoft Small Business Server, you should **not** install and run the Symantec Endpoint Protection client firewall component, therefore you must ensure that **Network Threat Protection feature is not be selected**.

20. Enter a path such as that shown below in the **Specify the folder...** field, then click **Next**



21. Select **No, just create them...** then click **Next**. Creation of a client package will begin, this can take up to 5 minutes
22. Once the client package has been created, the management console will automatically launch
23. Login using the following credentials - **Username:** admin, **Password:** <as you specified earlier>

Note: Liveupdate will begin to run silently in the background at this point, as part of an automated post-install task. Its purpose is to download the latest content (Antivirus and Antispyware definitions, etc) to the Symantec Endpoint Protection Manager. This process can run for varying lengths of time depending on the speed of the internet connection available to the Small Business Server. The total size of the initial content download is typically approximately 30MB. You do **not** need to wait for this process to complete before progressing to Phase 3, but you should be aware it is running in the background and therefore may impact the user experience temporarily.

Phase 3: Importing and assigning the Windows Small Business Server 2003 specific policies

To retrieve the policy files for use in this Phase:

Download the following zip file and extract the contained policy files to a local directory on the SBS machine:

http://www.symantec.com/business/support/endpointsecurity/migrate/SEP_SBS2003_BestPractice_PolicyFiles_MR2.zip

Once logged into the console, you can go ahead with assigning the Symantec provided Windows Small Business Server 2003 specific policies to the group in which the machine resides. Follow the instructions detailed below:

1. Click on the **Policies** tile icon on the navigation menu
2. Click **Firewall** under **View Policies**
3. Click the task to **Import a Firewall policy**
4. Browse to the Symantec provided **Firewall policy - Windows SBS 2003.dat** file, highlight it then click **Import**
5. Right-click the newly imported policy and click **Assign**
6. Select the **Microsoft Small Business Server** group, then click **Assign**
7. Click **Centralized Exceptions** under **View Policies**
8. Click the task to **Import a Centralized Exceptions policy**

9. Browse to the Symantec provided **Centralized Exceptions policy - Windows SBS 2003.dat** file, highlight it then click **Import**
10. Right-click the newly imported policy and click **Assign**
11. Select the **Microsoft Small Business Server** group, then click **Assign**
12. Log off and then close the Symantec Endpoint Protection Manager Console

Phase 4: Installing the Symantec Endpoint Protection client

Important! If a Symantec Antivirus primary/parent server version 10 or 9 is running on the Windows Small Business Server 2003 machine, please be aware:

- A Symantec Endpoint Protection Manager cannot directly manage Symantec Antivirus clients.
- Installing the Symantec Endpoint Protection client will replace an existing Symantec Antivirus primary/parent server version 10 or 9.
- Installation of the client will be blocked if a Symantec System Center is still installed on this machine.
- While not essential, the Symantec recommended best practice is to upgrade all workstations in your environment from a managed Symantec Antivirus version 10 or 9 client to a Symantec Endpoint Protection 11.0 managed client before you proceed with this phase (since otherwise these workstations will have an unmanaged client running until they are upgraded to a Symantec Endpoint Protection 11.0 managed client). Refer to the [product documentation](#) for guidance.

1. Locate the recently exported **setup.exe** file, which typically will reside in **C:\SEPclientpackages\Microsoft Small Business Server_32-bit**
2. Double-click this **setup.exe** file to launch an unattended install of the Symantec Endpoint Protection client
3. After approximately 10-15 minutes, a **Restart Notification** dialog will appear, click **Restart Now**


Note: The Antivirus and Antispyware protection component will typically be active before reboot but the firewall requires a reboot, so in the Symantec Endpoint Protection client user interface, it is normal to not see the firewall protection component present in the client user interface until a reboot has occurred.

4. After restart, log back into Windows

That's it!

Symantec Endpoint Protection 11.0 is now successfully deployed and running on your Microsoft Windows Small Business Server 2003.

Phase 5: Recommended post-installation tasks

1. After a few minutes, verify a yellow shield icon with a green circle above it now appears in the system tray... 
(Initially, the icon may appear with a yellow exclamation mark above it; this is expected, as the client retrieves and loads the latest content from the manager)

2. Login to the Symantec Endpoint Protection Manager Console, click **Clients** on the navigation menu, then highlight the **Microsoft Small Business Server** group, and confirm the client is present.
3. Schedule weekly automatic database backups to occur. Below is guidance on how this can be achieved:
 - a. While still logged into the Console, click **Admin** on the navigation menu, then click **Server**
 - b. Under View, click the icon that represents database
 - c. Under Tasks, click **Edit Backup Settings**
 - d. In the **Backup Site for Local Site** dialog box, click **Schedule**
 - e. Choose a specific day and time that suits for the weekly automatic backup to occur (typically it makes sense to choose an off-peak time such as Sunday at 2am).

Note: By default the database backup file is created in `<drive>:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup\`. It is strongly recommended to regularly copy these back up files to a secure **remote** location, so if the local hard disks ever fail, you are still in a position to recover the database content.

 - g. A backup of the private key, public key and server certificate was automatically taken as part of the install. Copy all files from `<drive>:\Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\` to the same secure remote location as the database backups. This should be a task you only need to complete once.
4. Configure the Symantec Endpoint Protection Manager to only download new content at an off-peak time (not during normal business hours), to ensure minimal disruption to server performance. Below is some guidance on how this can be achieved:
 - a. While still logged into the Console, click **Admin** on the navigation menu, then click **Server**
 - b. Ensure the “Local Site” is highlighted, then click **Edit Site Properties** in the Tasks menu
 - c. Click the **Liveupdate** tab
 - d. In the **Download Schedules** section of the dialog, change the **Frequency** to Daily
 - e. Set the **download start time** window to **Start: 3:00AM, End: 7:00AM**
 - f. Click **OK**
5. For all groups (accessible via the ‘Clients’ page in the console), set the “Communication Setting > Download” method to PULL with a heartbeat of 15 minutes.
6. Ensure the Windows Firewall is **not** enabled on the network connections in Windows (Start > Settings > Network Connections), since the Symantec Endpoint Protection client firewall is now protecting these.
7. Ensure the installed client has received the latest content updates by launching the Symantec Endpoint Protection client interface (you can double-click the icon in the system tray) and reviewing the content date and revision beside each protection component.
8. Via the console, review the policies and settings currently assigned to the **Microsoft Small Business Server** group and update them to suit your requirements. Refer to the [product documentation](#) for guidance.

What to expect from this point onward

Now that Symantec Endpoint Protection 11.0 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:

- Content updates (such as Antivirus and Antispyware definitions) will be automatically and silently downloaded by the Symantec Endpoint Protection Manager and distributed to the managed Symantec Endpoint Protection clients.

- The Symantec Endpoint Protection client firewall is currently running with a relatively open policy, so will accept connections from remote sources but at the same time, will scan all network traffic destined for the SBS machine with the Intrusion Prevention component (current content updates contain 1000+ signatures for this component). Please review and modify the firewall policy via the Symantec Endpoint Protection Manager console to suit your requirements.
- The database will automatically purge data as it becomes old or as the database fills up. In general, no manual intervention should be required to ensure this occurs.

Potential issues

The following are issues which could potentially be encountered while deploying and running Symantec Endpoint Protection 11.0 with Windows Small Business Server 2003:

- You select “Use a custom website” during the installation of the Symantec Endpoint Protection Manager, and since then, you notice the default website has been stopped in IIS, which results in many Windows Small Business Server 2003 web-based services becoming unavailable.

Resolution:

Uninstall the Symantec Endpoint Protection Manager, then install it again, this time ensuring to select the default option of “Default Web Site”.

- The Symantec Endpoint Protection Manager program files and processes are taking up more resources than expected

Resolution:

Symantec are currently working on further reducing and optimizing the resource usage of the Symantec Endpoint Protection Manager and Client. These optimizations will appear in future maintenance releases. If after applying the recommendations in this document, you still feel the Symantec Endpoint Protection Manager software is too resource intensive for your server right now, you can also opt to run Symantec Antivirus Corporate Edition 10 in the interim.

- You experience issues when attempting to access the Symantec Endpoint Protection Manager console or you don't see the client appear in the console.

Resolution:

The following knowledge base articles provide good guidance on troubleshooting these situations:

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007101711103548>

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007110214173248>

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007101711140148>

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007101711103548>

Note: To review currently hot topics and search the Symantec Endpoint Protection 11.0 knowledge base for further issues you may encounter, see: <http://www.symantec.com/enterprise/support/overview.jsp?pid=54619>

Symantec provided template policies

Along with this white paper, two template policies are provided by Symantec, which are tailor-made for Windows Small Business Server 2003. Environment variables have been used for the paths where possible but please double check the paths to ensure they are applicable for your specific environment.

Firewall policy – Windows Small Business Server 2003

This policy provides Firewall configuration; the following are differences between this policy and the default one:

- Added a rule to allow DHCP server traffic

Centralized Exceptions policy - Windows Small Business Server 2003

This policy provides Antivirus and Antispyware scanning exceptions for the following:

- Symantec Mail Security for Exchange version 6.x scanning directory
- Windows Server Update Services database and logs
- Sharepoint Services database and logs
- SBS monitoring database and logs
- ISA 2004 Server database and logs

Note: If required, the Symantec Endpoint Protection client will automatically enable silent files and directory exceptions specifically for Microsoft Exchange 2003, Active Directory Domain Controllers and the Symantec Endpoint Protection Manager's local database. There is no further action required for the administrator to ensure this occurs.

Identifying running processes

The following matrix should help you to pinpoint what the purpose is of the key Symantec Endpoint Protection 11.0 and Windows Small Business Server 2003 specific processes that run:

Process name	Used by	Purpose	When it runs
SemSvc.exe	SEPM	Server	Always
dbsrv9.exe	SEPM	Embedded database engine	Always
Rtvscan.exe	SEP	Antivirus, Antispyware and Proactive Threat Protection client-side management	Always
Smc.exe	SEP	Responsible for the SEP client communicating with the SEPM.	Always
SmcGui.exe	SEP	SEP client system tray icon	Always

SymCorpUI.exe	SEP	Client user interface	Only when client UI is run
ccApp.exe	SEP	Client proxy service	Always
ccSvcHst.exe	SEP	Client proxy service	Always
leEmbed.exe	SEPM	Console (Home, Monitors and Reporting views)	Only when console is run
javaw.exe	SEPM	Console and for certain SEPM operations	When console is run, or during certain SEPM operations
LUCOMS~1.exe	SEPM, SEP	Liveupdate	Only when Liveupdate runs
SescLU.exe	SEPM	Liveupdate	Only when Liveupdate runs
LuCallbackProxy.exe	SEPM, SEP	Liveupdate	Only when Liveupdate runs
LUALL.exe	SEPM, SEP	Liveupdate	Only when Liveupdate runs
sempub.exe	SEPM	Publish content updates and related files so clients can retrieve	After new content updates are downloaded by the SEPM
sqlservr.exe	SBS	SQL server instance (one for each instance)	Always
mad.exe	SBS	Exchange System Attendant	Always
Inetinfo.exe	SBS	Internet Information Server	Always
owstimer.exe	SBS	Windows SharePoint Services Timer service	Always
store.exe	SBS	Exchange Information Store (core process)	Always
exmngmt.exe	SBS	Exchange WMI Provider	Always
spoolsp.exe	SBS	Spooler SubSystem App (Print & Fax)	Always
sqlmangr.exe	SBS	Microsoft SQL Server Service Manager	Always
sbscrexe.exe	SBS	SBS Licensing Service	Always
IMBservice.exe	SBS	Exchange POP3 Connector	Always

Frequently Asked Questions

Q. I'm upgrading from a previous version of Symantec Endpoint Protection Manager as opposed a fresh installation, are there any specific points I should be aware of?

A. In general, all the guidance contained in this paper is still applicable but there is one step you should take. Launch the console, login, click Admin, Servers, right-click on the Site and select Properties. Click the Liveupdate tab, then in the section at the end of the dialog, change the number of stored content revisions to 3.

Q. I'm running SBS 2003 R2 Premium, should I use MS-SQL 2005 Workgroup Edition instead of the default embedded database for the Symantec Endpoint Protection Manager?

A. While it is possible to use MS-SQL 2005 Workgroup Edition for the Symantec Endpoint Protection Manager database, the Symantec recommended approach is to use the default embedded database as it is more suitable for use with SBS 2003. The default embedded database uses Sybase Adaptive Server Anywhere version 9, and its core process, dbsrv9.exe, typically utilizes approximately less than half the memory that a MS-SQL 2005 Workgroup Edition instance would use. Also, the embedded database can accept an unlimited number of connections and grow to an unlimited size, so provides no loss of functionality.

Q. Do I need to apply a license key/file to Symantec Endpoint Protection 11.0 to enable functionality?

A. There is no technical license key/file enforcement included with Symantec Endpoint Protection 11.0.

Q. Can I access the Symantec Endpoint Protection Manager console from remote machines?

A. Yes, by opening a web browser on any machine with network access to the Microsoft Small Business Server, and connecting to the URL, http://<SBSserver_hostname_or_IP>:9090

Q. Do I need to worry about any potential conflicts between Windows Server Update Services and the Symantec Endpoint Protection Manager?

A. No. With a standard version of Windows 2003, the Windows Server Update Services install wizard does, by default, suggest the Default Web Site for IIS integration BUT with Windows Small Business Server 2003, this same wizard shows the Default Web Site option as grayed out and only allows the user to select Custom Web Site, which means WSUS is setup with a new website for IIS integration and a custom TCP port of 8530.

Q. I plan on running Symantec Mail Security for Exchange on my Windows Small Business Server 2003 machine, as well as Symantec Endpoint Protection. Any extra steps I should take to optimize the environment?

A. No. In general, technically these two products will work on the same server and as part of Phase 3, you should have applied a Centralised Exception policy which ensures the Symantec Endpoint Protection client doesn't scan the SMS for Exchange version 6.0 scanning directory. The key consideration is the resource usage of running these two products in parallel so it is recommended you take some time to review available resource on the Microsoft Small Business Server before proceeding.

Useful Online Resources

Symantec Endpoint Security Migration and Installation website **Hot!**

<http://www.symantec.com/enterprise/support/endpointsecurity/migrate/index.jsp>

Symantec Endpoint Protection 11.0 - Free online tutorials providing an overview and migration walkthrough **Hot!**

<http://www.symantec.com/business/theme.jsp?themeid=sep11x&header=0&footer=1&depthpath=0>

Comparison Tour - Symantec System Center vs. the new Symantec Endpoint Protection Manager Console **Hot!**

http://www.symantec.com/business/support/endpointsecurity/ssc_sep/

Symantec Endpoint Protection 11.0 - Top customer frequently asked questions and resolutions

http://www.symantec.com/content/en/us/enterprise/media/stn/pdfs/Articles/faq_customer-installations-issues-resolutions.pdf

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007071909500548>

Symantec Endpoint Protection 11.0 - Product Documentation

<http://www.symantec.com/business/support/documentation.jsp?pid=54619>

Symantec publicly accessible user forums (peer to peer forums, not a replacement for technical support):

<https://forums.symantec.com/>

Symantec Endpoint Protection 11.0 – Support homepage (search the Knowledge Base from here)

<http://www.symantec.com/enterprise/support/overview.jsp?pid=54619>

Top security recommendations for small and mid-sized businesses

http://www.symantec.com/business/library/article.jsp?aid=ten_security_recommendations_for_smb

Microsoft virus scanning recommendations for computers running Windows 2003

<http://support.microsoft.com/kb/822158>

Various sources of information on Windows Small Business Server 2003

<http://www.microsoft.com/windowsserver2003/sbs/evaluation/features/default.aspx>

<http://www.microsoft.com/technet/prodtechnol/sbs/2003/plan/sbssp1whatsnew.aspx>

<http://www.microsoft.com/windowsserver2003/sbs/evaluation/faq/prodinfo.aspx>

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 800 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
408 517 8000
800 721 3934
www.symantec.com

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Copyright © 2007 Symantec Corporation. All rights reserved. 09/04 10318317