

Symantec Endpoint Protection 11.0

Installation Guide



SYMANTEC ENDPOINT PROTECTION 11.0

TABLE OF CONTENTS

A NEW SECURITY APPLICATION	1
INTRODUCTION	1
WHAT IS SYMANTEC ENDPOINT PROTECTION (SEP) 11.0?.....	1
LICENSING OPTIONS	1
MANAGEMENT OPTIONS	2
IF EDUTECH WILL BE MANAGING YOUR CLIENTS	3
WEB-BASED INSTALLATION	3
DOWNLOADING THE INSTALLER	3
INSTALLATION	3
IF EDUTECH WILL NOT BE MANAGING YOUR CLIENTS	4
MANAGED AND UNMANAGED CLIENTS.....	4
INSTALLING SYMANTEC ENDPOINT PROTECTION MANAGER	4
TO INSTALL SYMANTEC ENDPOINT PROTECTION MANAGER.....	4
CONFIGURING THE MANAGEMENT SERVER	5
CREATING CLIENT INSTALLATION PACKAGES	6
APPENDIX A: SYSTEM REQUIREMENTS	7
APPENDIX B: INSTALLING SSL CERTIFICATE IN INTERNET EXPLORER	8
APPENDIX C: BACKING UP A SYMANTEC ENDPOINT PROTECTION SERVER	9
SERVER CERTIFICATE	9
THE SITE	9
EMBEDDED DATABASE ON DEMAND	10
MICROSOFT SQL ON DEMAND	10
MICROSOFT SQL WITH MAINTENANCE WIZARD	11
MISCELLANEOUS DETAILS.....	11

A NEW SECURITY APPLICATION

Introduction

Symantec Endpoint Protection (SEP) is the latest desktop computer security application purchased by EduTech for distribution to North Dakota's K-12 schools. It is an update and enhancement to the Symantec Client Security used by many districts.

What is Symantec Endpoint Protection (SEP) 11.0?

Symantec Endpoint Protection 11.0 combines Symantec Antivirus with additional security measures provide defense against malware and other security threats for laptops, desktops and servers. These are integrated into a single agent and management console.

Symantec Endpoint Protection 11.0 includes:

- Antivirus and Anti-spyware
- Desktop Firewall
- Intrusion Prevention (both Network and Host based)
- Device Control

Licensing Options

EduTech has purchased a sufficient number of SEP licenses to provide desktop antivirus/security software to every K-12 desktop computer and file server. We distribute these licenses to public K-12 schools at no cost and to private K-12 schools at a minimal charge. The software is not licensed for home use and may not be installed on any non-district computers. Computers located on your district's computer network, but are not the property of your school district are not eligible to participate in this licensing program and will be required to obtain their antivirus/security software from a different source.

Before your district's Symantec Antivirus software can be updated or installed, you district's technology coordinator will need to fill out the License Request form located on the EduTech Antivirus page (www.edutech.nodak.edu/antivirus).

When your technology coordinator has completed this form, the EduTech Help Desk will create components allowing you to perform Web-based installs of the software to your Windows desktop computers and file servers. EduTech will also manage the SEP installations for all of these devices.

You may request installation CDs for Macintosh computers. If you are choosing to manage your own clients you will receive a CD with the appropriate software. No installation CD is necessary if installing to Windows PCs that will be managed by EduTech.

No software or installation method will be distributed or licensed if the License Request form is not completed.

Management Options

You have two options on how to deploy SEP within your district. You may choose to have each Microsoft Windows computer¹ in your school receive its definitions and management options from EduTech's servers or you may choose to run your own SEP management servers. There are benefits to each method as illustrated in the following chart:

Comparison of Deployment Options

	Pros	Cons
EduTech Manages Clients	<ul style="list-style-type: none">• Easiest Installation Method (preconfigured web install)• No server administration duties	<ul style="list-style-type: none">• Limited control over configuration options and custom firewall settings for clients.• Cannot have different computers managed in different ways (school labs, teacher machines, laptops, etc...).
District Manages Clients	<ul style="list-style-type: none">• May configure groups of computers with different management options• May train firewall to allow specific types of traffic	<ul style="list-style-type: none">• Must install, configure and manage server.• Must configure options for antivirus and apply firewall policies to clients.

¹ The SEP clients are Windows only applications. EduTech distributes a stand-alone, unmanaged version of *Norton Antivirus for Mac* for Apple Macintosh systems.

IF EDUTECH WILL BE MANAGING YOUR CLIENTS

If EduTech will be managing your client(s), it is best to use the Web-based installer.

Web-based Installation

If your technology coordinator has not filled out the License Request form at www.edutech.nodak.edu/antivirus, they must do so before you can proceed with a Web-based installation.

DOWNLOADING THE INSTALLER

1. Open a browser window and go to www.edutech.nodak.edu/support/antivirus/sepwebinstall
2. On the Symantec Endpoint Protection Web Install page, verify the correct City and Client Group are being displayed. Contact the EduTech Help Desk if this information is incorrect.
3. Select the link for your operating system type: **32 Bit:** link for Windows 2000/XP/Vista or Server 2003/2008 or the **64 Bit:** for the 64-bit versions of these same operating systems with the exception of Windows 2000.
4. Click **Save** when the file download box appears. Save the SEP zip file to computer's Desktop (it will be named SEP_x32 or SEP_x64 depending on your selection in step #2). Click **Close** when the download completes. You may now close your browser.

NOTE: This SEP zip file is portable and can be copied to a network share, portable drive, or USB flash drive and carried to other computers to be installed.

INSTALLATION

1. Locate the SEP zip file. If you followed the previous instructions, it should be on your computer's Desktop (or wherever you chose to download it) **NOTE:** If running Windows 2000, the SEP_x32 folder does not automatically unpack. You'll have to unpack it before proceeding.
2. Double click on **SEP_x32** to open the zip folder, then locate and double-click on **setup (or setup.exe)**.
3. If a *File Download – Security Warning* screen appears, click **Run**.
4. The install process will automatically begin. Please be patient, it may take some time. Eventually a LiveUpdate window will appear. **DO NOT CANCEL**. Again, be patient, this process may take a few minutes or longer, depending on the speed of the computer.
5. If an *Old Virus Definition File* window appears, click **Close**.
6. The LiveUpdate window will close automatically when it is finished. Next a Restart Notification window will appear, click on **Restart Now**. After the restart the computer is still installing and updating files. When completed the yellow shield in the taskbar will change from a yellow dot to a green dot.
7. When the shield changes to a green dot, close any remaining open windows, delete the SEP zip folder from the desktop and restart your computer.

IF EDUTECH WILL NOT BE MANAGING YOUR CLIENTS

Managed and Unmanaged Clients

Your desktop clients may be installed as either Managed or Unmanaged clients. It is recommended that whenever possible, you set up the clients in your district as Managed.

Managed Clients receive their updates directly from their Symantec Endpoint Protection Server whenever new definitions come out. You may also view the current status and run reports on managed clients (for example when scans have been done, whether viruses have been found, what action was taken, etc...). Also, the server may initiate a scan on a machine it manages.

Unmanaged Clients receive their definitions from Symantec based on a pre-defined schedule.

Information from an unmanaged client is not reported to any SEP management server.

To create a client install package, refer to the **Creating Client Installation Packages** area at the end of this section.

Installing Symantec Endpoint Protection Manager

Symantec Endpoint Protection Manager (SEPM) is a module for the Microsoft Management Console. With this program you will interact with and manage your district's SEP servers and clients. SEPM can be installed on many servers and managed from any as well as managed from a web interface. Also used in this version is a database and depending on your environment you will use the embedded Microsoft database (less than a 5000 clients) or Microsoft's SQL database if over 5000 clients. The database can but doesn't have to be installed on the same server as the SEPM console. Typically SEPM is installed on one server along with the database and possibly a second SEPM on a different server for load balance.

IMPORTANT NOTE: SEP doesn't upgrade any previous installation of Symantec antivirus protection, it runs "along side of" or "instead of" those installations. **Reinstallations of clients will be necessary.**

TO INSTALL SYMANTEC ENDPOINT PROTECTION MANAGER

1. Select a computer that you will use to administer your district's SEPM (this can even be the same server currently installed with SCS). Please ensure it meets the system requirements for SEPM identified in Appendix A.
2. Make sure you have Internet Information Services (IIS) installed first before preceding onto the SEP install.
3. Insert the CD for SEP. A screen with 3 choices will be displayed.
4. Click **Install Symantec Endpoint Protection Manager**, on the Welcome screen click **Next**, accept the licensing terms, then click **Next** again to begin the installation.
5. Select your Destination Folder (you either change the path or click **Next** to stay with the default).
6. Once you've selected the Destination Folder, you will select the Web site used to deliver the software. If you wish to have the SEP Web server run with other Web servers on this server, select Use the default Web site, otherwise, select Create a custom Web site. Click **Next**.

7. Click **Install** to begin the installation, after completion click **Finish**.

CONFIGURING THE MANAGEMENT SERVER

Upon completion of the SEP Management Server, a Management Server Configuration Wizard will start, asking you to select Simple or Advanced. If you have 100 or fewer clients, select Simple, otherwise select Advanced.

Simple Configuration

1. After you selected Simple Configuration, you will be asked to setup the system administrator account. Admin is the default user name, enter a password and type it again to confirm it was entered accurately. The email address field is optional. Click **Next**.
2. A summary of the configuration will be displayed. Please print and store a copy of this information for your records. Click **Next**.
3. Select **No** when prompted to run the Migration and Deployment Wizard. Click on **Finish** and you are done with the Management Server installation and configuration.

Advanced Configuration

1. The next screen you will choose approximately how many computers will be managed by this SEPM. After you have chosen the appropriate radio button click **Next**.
2. Installation of site is the next screen. Choose the appropriate radio button and click **Next**.
3. The next screen displays the server name, server port, Web console port, and server data folder. The defaults are recommended but can certainly be changed. As always right down this information for your records and then click **Next**.
4. The site name is next (stay with the default or change it) and click **Next**.
5. Next is the encryption password used between the server and clients. Type in a password and confirmation password and click **Next**.
6. Next choose the embedded database (for fewer than 5000 clients) or an already installed Microsoft SQL Server database (for more than 5000 clients) and then click **Next**. Follow the setup instructions in the appropriate section.

CONFIGURING THE EMBEDDED DATABASE

1. The next screen is to configure the system administrator account. Admin is the default user name now type in a password and again to confirm. The email address field is optional. Click **Next**.
2. Select **No** when prompted to run the Migration and Deployment Wizard. Click on **Finish** and you are done with the Management Server installation and configuration.

CONFIGURING THE MICROSOFT SQL DATABASE

1. Next choose the radio button to create a new database or use an existing and then click **Next**.

2. If chose to create new database the next screen with display information for and about the SQL database. Either stay with the defaults or change the information. The DBA user and password is the database information you typed in when you installed Microsoft SQL and again make a copy of the information on this screen for your records. NOTE: if using Microsoft SQL make sure you have SP2 installed for MS SQL.
3. The next screen is to configure the system administrator account. Admin is the default user name now type in a password and again to confirm. The email address field is optional. Click **Next**
4. Select **No** when prompted to run the Migration and Deployment Wizard. Click on **Finish** and you are done with the Management Server installation and configuration.

CREATING CLIENT INSTALLATION PACKAGES

There are many ways to install SEP onto your clients. The most common way is to create an install package within the SEPM under the Admin icon which will contain an MSI file or an executable and then execute that file from the client.

Information on creating a client install package can be found at the Symantec Support Knowledge Base(<http://www.symantec.com/business/support/>). Search the Knowledge Base for Document ID:2007072016360948. For information on creating custom install packages, please refer to Document ID: 2007110513361348.

APPENDIX A: SYSTEM REQUIREMENTS

SEP may be installed on Windows 2000 or later, including server versions. Protected systems should meet the following requirements:

- Memory: 256 MB or higher
- Hard Disk: At least 700 MB free
- CPU:
 - 32-bit client
 - Minimum of 400 MHz Intel Pentium III
 - Minimum of 1 GHz for Windows Vista client
 - 64-bit client
 - Minimum 1 Ghz or better x64 processor (not Itanium).
 - AMD 64-bit Opteron
 - AMD 64-bit Athlon processors
 - Intel 64-bit Xeon with EM64T support
 - Intel 64-bit Pentium IV processors with EM64T support

For a more detailed list of system requirements, refer to

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007082112580548>.

APPENDIX B: INSTALLING SSL CERTIFICATE IN INTERNET EXPLORER

Even if EduTech is managing your district's SEP installations, you can view your protected computer list and see reports on their status from a Windows XP computer. Viewing these reports is optional, but may be of use to you.

If you are using Internet Explorer 7, you must import a certificate into your Internet options in order to log into EduTech's SEP Management Page to view your clients and reports.

To obtain login information and install the security certificate:

1. Contact the EduTech Help Desk and request a SEP management login. The Help Desk will send an e-mail message with login information, instructions, and a security certificate. Save the certificate to your Windows XP computer's Desktop
2. Start Internet Explorer and select **Tools**→**Internet Options**
3. Click on the **Content** tab and then the **Certificates** button.
4. Click the tab labeled **Trusted Root Certification Authorities** and click **Import**
5. The **Certificate Import Wizard** will begin, click **Next**
6. Using the **Browse** button next to the **File name** field, locate the certificate you placed on your Desktop. Select "PKCS #7 Certificates" from the **Files of type** menu
7. Select the certificate file send by the Help Desk and click **Open**, then **Next**.
8. On the Certificate Store screen, make sure "Place all certificates..." is checked and **Trusted Root Certification Authorities** is displayed in the Certificate store. Click **Next**. When the completion screen appears, click **Finish**.
9. A Security Warning screen will open and ask "Do you want to install this certificate?", click **Yes**
10. Again the same Security Warning screen will display, click **Yes** once again.
11. Next screen should display "The import was successful", click **OK**
12. Click **Close** on the Certificates screen and **OK** on the Internet Options screen, you are done.

APPENDIX C: BACKING UP A SYMANTEC ENDPOINT PROTECTION SERVER

You will want to periodically backup three different sections of your SEP install; server certificate, the site and the database (embedded or Microsoft SQL).

Server certificate

In case the management server is damaged, you must back up the private key as well as the files that represent the certificate.

To back up a server certificate

1. In the Symantec Endpoint Protection Manager console, click **Admin**.
2. In the Admin page, under Tasks, click **Servers**.
3. Under View Servers, click the management server whose server certificate you want to back up.
4. Under Tasks, click **Manage Server Certificate**.
5. In the Welcome to the Manage Server Certificate Wizard pane, click **Next**.
6. In the Manage Server Certificate panel, click **Back up the server certificate**.
7. In the Backup Server Certificate panel, type the pathname or browse to the folder into which you want to back up the private key. Note that you back up the management server certificate into the same folder.

The JKS Keystore file is backed up during the initial installation. A file that is called *servertimestamp.xml* is also backed up. The JKS Keystore file includes the server's private and public key pair and the self-signed certificate.

8. In the Backup Server Certificate panel, click **Next**.
9. In the Manage Server Certificate panel, click **Finish**.

The site

When you back up information about a site, you perform the same task as you do when you back up a database for a site.

To back up a site

1. In the Symantec Endpoint Protection Manager console, click **Admin**.
2. In the Admin page, under Tasks, click **Servers**.

3. In the Admin page, under View, click **localhost**.
4. In the Admin page, under Tasks, click **Edit Backup Settings**.
5. In the Backup Site for Local Site: *Site name of local site* dialog box, select the name of the backup server from the Backup server list.

By default, the pathname is Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup.

However, you can change the name of the backup path by using one of the available backup utilities.

6. Select the number of backups that you want to retain from the Number of backups to keep list.
You can select up to 10 backups that you can retain before a backup copy is automatically deleted.
7. Click **OK**.

Embedded database on demand

You can perform an on-demand backup of an embedded database from the Symantec Endpoint Protection Manager console.

To back up an embedded database from a Symantec Endpoint Protection Manager console

1. In the Symantec Endpoint Protection Manager console, click **Admin**.
2. In the Admin page, click **Servers**.
3. Under View Servers, click the icon that represents the embedded database.
4. Under Tasks, click **Back Up Site Now**.

This method backs up all site data, including the database. You can check the System log as well as the Backup folder for status during and after the backup.

5. Click **Yes** when the Back Up message appears.
6. Click **Close**.

Microsoft SQL on demand

The Symantec Endpoint Protection Manager console includes a site backup that you can use to back up and later restore the database. In addition, you can set up a maintenance plan on the Microsoft SQL Server Agent.

The following procedure includes recommended settings.

You may need to use different settings depending on the following criteria:

- The size of your organization.
- The amount of disk space you have reserved for backups.
- Any required guidelines at your company.

To back up a Microsoft SQL database on demand from a Symantec Endpoint Protection Manager console

1. In the Symantec Endpoint Protection Manager console, click **Admin**.
2. In the Admin page, click **Servers**.
3. In the Admin page, under View Servers, click the icon that represents the Microsoft SQL database.
4. In the Admin page, under Tasks, click **Backup Site Now**.

This method backs up all of the site data, including the database. You can check the System log as well as the Backup folder for status during and after the backup.

5. Click **Close**.

Microsoft SQL with Maintenance Wizard

The Microsoft SQL Server Enterprise Manager provides a wizard to help set up a database maintenance plan. You can use the Database Maintenance Plan wizard to manage the database and to schedule automatic backups of the Microsoft SQL database.

Note: Make sure that the SQL Server Agent is started. Sysadmin access rights are required to run on the Database Maintenance Plan wizard.

Refer to the Microsoft SQL Server documentation for details on how to maintain a Microsoft SQL Server database.

Also more information can be found in the <http://www.symantec.com/business/support/> and in the Search the Knowledge Base field, search for **Document ID:2008042407391148**.

Miscellaneous details

Some other details to be aware of:

- If currently running your own definition server for SCS and you have ALL workstations and servers installed with SEP, uninstall SCS.

- On the computer you have chosen to be your SEPM, remember to create an installer package for that computer as well.
- Other security software, such as other antivirus or antiadware, and antispysware can affect the performance and effectiveness of Symantec Endpoint Protection. It is not recommended that you run two antivirus or two antiadware or spyware programs on one computer. If both programs provide real-time protection, they can create a resource conflict and drain the computer's resources as the programs try to scan and repair the same files.
- Each district can request a login/password from the EduTech helpdesk Symantec support staff to enable you to log into SEP to display your client workstations information and create reports. At that time you'll be emailed the certificate needed for the browser and instructions for logging into SEP. In Appendix B of this document are instructions for installing the certificate. To access this report section you have to be running the browser on Windows XP.
- If running Microsoft Defender, during the installation you will be prompted to close Defender, click Close.