



Symantec Client Security 3.1 Installation Guide



Copyright © 2006 EduTech

Symantec, the Symantec logo, Microsoft, Microsoft Windows, Novell and Novell NetWare and all named applications within this document are trademarks and property of their respective owners

All rights reserved.

Introduction

Thank you very much for your participation in the North Dakota K-12 Computer Virus Protection Plan. This manual is provided to North Dakota K-12 schools to assist them in deploying Symantec Client Security within their districts.

In order to keep the size to a minimum, this guide does not cover all facets of the Symantec Client Security and its related applications. Complete information is located in a complete assorted PDF installation guides on the CD and on the Symantec website. If you would like more detailed instructions, please look in the /Docs folder on the SCS 3.1 CD media distributed by EduTech.

If you have any questions, please contact the EduTech Help Desk.

The EduTech Support Staff
sendit.helpdesk@sendit.nodak.edu
800.774.1091
PO Box 6154
Fargo, ND 58105-5164

Table of Contents

Introduction	ii
Table of Contents	1
Section 1: A New Security Application	2
Introduction.....	2
Licensing.....	2
Architecture.....	2
<i>Comparison of Deployment Options:</i>	3
Primary Server and Secondary Servers.....	3
Managed and Unmanaged Clients	3
Section 2: System Requirement and Important Notes	4
System Requirements for Various SCS components	4
Miscellaneous Details.....	5
<i>Details for Districts Planning to Run SCS Management Servers</i>	5
<i>Details for Districts without SCS Management Servers</i>	6
Removing Current Antivirus Software	6
Section 3: Installing Symantec System Center and Snap-ins	6
Section 4: Installing and Configuring SCS Server Software	7
Installing Server Software	7
<i>Installing a Primary Server</i>	7
<i>Making a Server the Primary Server</i>	9
<i>Installing a Secondary Server</i>	9
Configuring Your Definitions Source.....	10
Allowing 10.1 Server to Manage 9.x Clients.....	10
After the server is installed.....	11
<i>Backing up the pki folder</i>	11
Creating an EduTech Login for your Server Group.....	11
Setup and Management of Client Groups	12
Section 5: Firewall and Intrusion Prevention System	12
Planning Firewall Implementation	13
<i>How Many Different Policies Should be Distributed</i>	13
<i>Level of User Customization</i>	13
<i>Policy Maintenance</i>	13
<i>Testing</i>	13
Installing Symantec Client Firewall Administrator	14
<i>Training the firewall</i>	14
<i>Open firewall policy</i>	16
Section 6: Installing Windows Clients	17
Client Installation via CD.....	17
Client Installation via Web Browser.....	18

Section 1: A New Security Application

Introduction

Symantec Client Security (SCS) is the new desktop computer security application purchased by EduTech for distribution to North Dakota's K-12 schools. It includes the Symantec Antivirus application already distributed to most school districts, plus a managed desktop firewall and intrusion prevention and detection system. These three components work together to provide more complete protection from the newest desktop security threats.

Licensing

EduTech has purchased a sufficient number of SCS 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 non-district computers. Computers which are 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 send the latest SCS installation CDs to your district and (if necessary) create components allowing you to perform Web-based installs of the software to your desktop computers.

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

Architecture

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

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

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.

Primary Server and Secondary Servers

If you decide to run your own SCS management servers, you will need to operate a Primary Server and preferably also a Secondary Server.

The **Primary Server** is the machine which will receive antivirus definitions directly from Symantec and deploy them to your school's managed clients (more on those in the next item). Your Primary Server should be running Windows 2000/2003 Server, Windows XP or Netware. Note that your Primary Server can continue to fulfill other functions, such as being a file server.

A **Secondary Server** receives its antivirus definitions from the Primary Server and distributes them to AntiVirus clients. In the past, the main function of a Secondary Server was to manage groups of computers which cannot connect to the primary server via a fast network connection. For example, if you have a facility with many managed computers which is connected to your Primary Server via 56k or similar bandwidth you may wish to set up a Secondary Server in that location. That way you only have to push one set of definitions across the slower connection. The secondary server will distribute the definitions within the facility at much higher LAN speeds.

Changes to the way Symantec distributes definitions have created a new need for Secondary Servers. Because server-to-client communications are now encrypted, if your Primary Server crashes, you may experience significant service interruption unless your clients are aware of another computer which will allow them to receive definitions.

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 Primary (or Secondary) Server whenever new definitions come out. The Primary/Secondary Server can also view information on

managed clients (for example when scans have been done, whether viruses have been found, what action was taken, etc...). The server may also 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 SAVCE or SCS management server.

Section 2: System Requirement and Important Notes

This section includes important information that is critical to the successful implementation of SCS in your district. Further information on these points is available in greater detail on Symantec's website.

System Requirements for Various SCS components

SCS Component	RAM (MB)	Hard Disk (MB)	Operating Systems Supported				IE 5.5 SP2 or later	Additional Notes Below
			2000 Pro	2000 Server	XP Pro	2003 Server		
Symantec System Center (server management tool)	64+	60-700	X	X	X	X	X	X
SCS Client (32-bit firewall/antivirus client)	128+	115	X		X		X	
SCS 64-bit antivirus client	80+	70			64-bit	64-bit	X	X
SCS Server	64+	150	X	X	X	X	X	X
Client Firewall Administrator (firewall policy builder)	80+	130	X	X	X	X	X	

- Symantec System Center (server management interface)
 - Microsoft Management Console version 1.2 or later (installed with SSC if necessary)
- SCS 64-bit antivirus client
 - Intel® processors that support Intel® Extended Memory 64 Technology (Intel® EM64T)
 - AMD 64-bit Opteron™ and Athlon™ processors
- SCS Server
 - 500 MB free disk space needed during install
 - The following versions of NetWare are also supported
 - NetWare 5.1 with Support Pack 8 or higher, or
 - NetWare 6.0 with Support Pack 5 or higher, or
 - NetWare 6.5 with Support Pack 2 or higher
 - A static IP address and 100 Mbps Ethernet recommended (10 Mbps is acceptable)

For a more detailed list of system requirements, refer to www.symantec.com, search for **Document ID: 2006021416560048**, “System requirements for Symantec Client Security 3.1”.

Miscellaneous Details

Details for Districts Planning to Run SCS Management Servers

- A district electing to run a Windows XP Professional system as a Primary Server should contact the EduTech Help Desk for some “hints and tricks”.
- Districts continuing to run SAVCE 9 clients must refer to section “Allowing 10.1 Server to Manage 9.x Clients” in this document for instructions
- If you plan to develop your own firewall policies, make sure you first try everything in a test environment.
- As the software licensee, EduTech will need a login/password to your Symantec Server Group. Please refer to section “Creating an EduTech login in your Server Group”
- Backing up the PKI folder for your Primary Server is an essential step. Please refer to section “After the server is installed” in this document for instructions
- Plan your deployment. Some installation and deployment steps must be completed in specific order. Please read all instructions in this guide.

General steps to be completed are:

1. Plan where you will place SCS management servers based on where your clients are located.
2. Fill out the License Request form located at www.edutech.nodak.edu/antivirus
3. After you receive the install media, install Symantec System Center (SSC) on the system that will be your Primary Server.
 - a. If you are upgrading, uninstall the previous version of SSC from your Primary Server first and then install the new version.
 - b. Repeat this procedure on all systems where you have installed previous versions of SSC.
4. Install/Upgrade SCS Server on the system you will make your Primary management server
5. Unlock the server group and designate the Primary Server (if not already identified as such).
6. Back up the server group root certificate
7. Install additional management servers from Symantec System Center (optional)
8. Configure your server group, adding an account for EduTech
9. Install test SCS clients
10. Install Symantec Client Firewall Administrator on servers

11. Train test client firewalls and develop firewall policies
12. Install SCS client and deploy firewall policies.

More information can be found in the “Symantec Client Security 3.1 installation walk-through” located at www.symantec.com, search for **Document ID:** 2006032313380648.

Details for Districts without SCS Management Servers

- Fill out the License Request form at www.edutech.nodak.edu/antivirus.
- Most installations can be completed via a Web-based install. You will need Internet Explorer 5.5 SP2 or later on desktops where you plan to install the client software via a Web browser.
- If you are unable to use the Web-based install, you may still install Symantec Client Security via CD, however it will be necessary to contact the EduTech Help Desk so they can apply the correct firewall policy and group settings to these machines.

Removing Current Antivirus Software

Before installing SCS 3.1 software on any machine you should uninstall any non-Symantec Corporate Edition antivirus software. Obviously you should attempt to minimize the amount of time your machines are in use without antivirus protection.

Section 3: Installing Symantec System Center and Snap-ins

IMPORTANT: If this is an update to a currently installed Primary Server, you must make a copy of the pki folder and store it in a secure location before modifying any SAVCE or SCS software. It is located in C:\Program Files\SAV\Symantec AntiVirus. Refer to the “After the server is installed” section of this document.

Symantec System Center (SSC) is a module for the Microsoft Management Console. With this program you will interact with and manage your district’s SCS and SAVCE servers and clients. You should install the SSC to your district’s Primary Server first. You may install SSC on additional computers to facilitate management of your Symantec servers and clients.

1. Select a computer which you will use to administer your district’s Primary Server (this can even be the Primary Server itself). Please ensure it meets the system requirements for SSC identified in the previous section. If you have previous versions of Symantec System Center or antivirus software installed, continue with step 2, otherwise skip to step 5.

Before Proceeding with Uninstall:

- **Write down the Server Group name and IP number of the Primary server. This may be needed later.**
- **Remove older versions of the SSC and install the new version of SSC to the Primary Server first.**

2. To uninstall SSC:
 - a. Click **Start**→**Settings**→**Control Panel**
 - b. Double-Click **Add/Remove Programs**
 - c. Select **Symantec System Center** and click **Remove**
3. You will be prompted to restart your system after it has finished. Click **Yes**.
4. Repeat steps **a & b** above for any of the following that appear in the applications list:
 - LiveUpdate
 - Norton/Symantec Antivirus Add-On for Symantec System Center
 - Any antivirus software other than Symantec Client Security and Symantec Antivirus Corporate Edition
5. (Optional) You may choose to delete the contents of the Temp folder and empty the Recycle Bin to free space on the server.
6. Restart the Server and log in as the local administrator.
7. Insert SCS 3.1 CD Disc 1 (Windows Software) into the CD drive. If the “Symantec Client Security” window does not appear automatically after a few moments, then locate SETUP.EXE on the CD drive’s contents and double-click on it.
8. After the setup interface appears, click **Install Symantec Client Security** followed by **Install Symantec System Center**. Read the instructions on the Welcome screen and click **Next**.
9. Read the license agreement carefully and click **I accept the terms in the license** and then click **Next**.
10. Keep the defaults in the **Select Components** screen. Installation of Alert Management System Console is optional. Click **Next**
11. You are now asked to choose the installation directory; it is recommended you accept the default selection and click **Next**.
12. In the **Ready to Install the Program** screen, click **Install**.
13. When the installation is complete, click **Finish** and then restart the computer

Section 4: Installing and Configuring SCS Server Software

Installing Server Software

Installing a Primary Server

If you have not done so already, choose a single server to act as your district’s Primary Server. Make sure you have installed the SSC as described in the previous section to this system. After SSC has installed successfully, follow these instructions to set up the Symantec Client Security Server software.

When installing the server software to a system with more than one network card, the network interface that communicates with your clients must be first in the binding order.

1. Place SCS 3.1 CD Disc 1 (Windows Software) in the CD tray of the Primary Server (make sure you are logged in with local administrator privileges). If the “Symantec Client Security” window does not appear automatically after a few moments, then locate SETUP.EXE on the CD drive’s contents and double-click on it.
2. Select the menu choice **Install Symantec Client Security Server**.
3. At the Welcome screen, choose **Install** or **Update**, whichever is appropriate and click **Next**.

If you chose *Install* follow these steps. If you chose *Update* skip ahead to step 14.

4. Read the license agreement, select **I Agree** and click **Next**.
5. Select Items screen appears, leave the defaults checked and click **Next**.
6. In the Select Computers window you should see your computer’s name in the left windowpane. Highlight that name and click on the **Add** button and click **Next**.
7. On the Server Summary screen install to the default directory by clicking **Next**.
8. On the **Select Symantec AntiVirus Server Group** screen, the software will ask you for a server group name. If you have already created a server group, select it from the list, if this is the first time you have created a server group, enter a server group name and click **Next**.
9. If you created a new server group, click **Yes** when prompted to create the new group and enter username and password you wish to use for this server group.
10. Select **Automatic Startup** if it isn’t already selected and click **Next**
11. Carefully read the information presented on the successive screens, clicking **Next** to continue to each one. When you click **Finish** the **Setup Progress** screen will display information regarding the install process. This process may take a few minutes.
12. You may get a warning that the definition files are out of date, ignore it for now and click **Close**.
13. If no errors are shown upon completion, click **Close** and reboot the server. If a server had listed errors, click the **View Errors...** button and contact the EduTech Help Desk with the information.

Follow these steps if you chose Update:

14. On the screen **Select Computers** choose the Server on the left then click the **Add** button to move it into the Selected computers box on the right and click **Finish**.
15. Enter the Username and Password that you would use to unlock the Server Group and click **OK**.
16. Click **Finish**.
17. Click **Close** and restart the computer.

Making a Server the Primary Server

After the server has rebooted, you will need to configure the machine to be the Primary Server for the district.

1. Start up the Symantec System Center Console on the Primary Server
2. Expand the System Hierarchy to see your “Server Group”
3. Click once on System Hierarchy and then choose **View** → **Symantec Antivirus** from the menu bar.
4. Right click on your server group name and select **Unlock Server Group**. Enter the username and password for the server group (you created this in the previous section).
5. Right click on your server’s name and select **Make Server a Primary Server**.
6. Read the notes in the dialog box. If making this computer the Primary Server, click **Yes**.
7. In the Reporting Server Options screen enter the Primary Server’s machine name or IP address and click **OK**.

Installing a Secondary Server

1. Start the Symantec System Center console on your Primary Server.
2. Within the left pane of SSC, expand **Symantec System Center**, if necessary, by clicking on the "+" symbol next to it.
3. Select **Tools** → **AntiVirus Server Rollout** from the menu bar.
4. At the Welcome page, click **Install Symantec AntiVirus server**, and click **Next**.
5. Read the License Agreement, click **I agree**, and then click **Next**.
6. On the Select Items page, make sure Server program and Reporting Agents are checked, and click **Next**.
7. In the Select Computers page, locate the system you wish to make a Secondary Server within the Network. Select the computers to which you want to install the server software and click **Add**, followed by **Next**.
8. On the Server Summary page, select your installation path. It is recommended you select the default location. Click **Next**.
9. When prompted, type the user name and password for your server group, and click **OK**.
10. In the Server Startup Options page, click **Automatic startup**, and then click **Next**.
11. In the Using the Symantec System Center Program page, click **Next**.
12. Read the Setup Summary message and then click **Finish**.
13. In the Setup Progress panel, view the status of the server installation, and then click **Close** when the installation is finished.
14. Restart the newly installed server.

Additional instructions related to an SCS deployment on your network can be found at Symantec's website. Go to www.symantec.com and search for **Document ID:2006032313380648**. Click on the first link, "Symantec Client Security 3.1 installation walk-through for...".

Configuring Your Definitions Source

Now you must configure the Primary Server to get its virus definition updates from Symantec Live Update. You would perform similar steps to inform your Secondary Server to get its definitions from your Primary Server.

1. Right click on your primary server and select: **All Tasks** → **Symantec AntiVirus** → **Virus Definition Manager**.
2. Next to **Update only the primary server of this server group** click **Configure**
3. In the window that pops up, click **Source**. Another window will appear.
4. Make sure **Live Update (Win32)/FTP (Netware)** is chosen. Click **OK**.
5. Click **Schedule** (which is below the **Source** button), click **Daily** for frequency and then a time to update. We recommend something between 12:30 AM and 6:30 AM. While still in the **Virus Definition Update Schedule** window, click on **Advanced** and under **Randomization Options** uncheck **Perform update within plus or minus**. Click **OK**.
6. Click **OK** on the Virus Definition Update Schedule screen and on the Configure Primary Server Updates screen, click the **Update Now** button. Click **OK** on the Symantec Antivirus Management Snap-In screen.
7. Click **OK** on the Configure Primary Server Updates screen.
8. Under the **How Clients Retrieve Virus Definitions Updates** section of the Virus Definition Manager screen, make sure **Update virus definitions from parent server** is check marked and **Schedule client for automatic updates using LiveUpdate** is unchecked. Click **OK**.
9. Highlight the server group and from the menu, click on **Action**→**Refresh**. You should see the Definitions date change to a more current definition date.

Allowing 10.1 Server to Manage 9.x Clients

The following steps **must** be performed to allow your SCS 3.1 server to manage SAVCE clients prior to version 10.

1. While still in the SSC, right mouse click on your Primary Server and select: **All Tasks**→**Symantec AntiVirus**→**Server Tuning Options**
2. Click first choice of **Allow this server to manage 9.x and earlier clients and servers (requires reboot to take effect)**. Click **OK**.
3. Restart computer for changes to take effect.

After the server is installed

After you have installed your primary server you **MUST** backup the pki folder. This should be done before you proceed with configuring your server in the event you have a major system crash and have to re-install Symantec Primary Server. Periodically you will want to backup your pki folder to a second location, keeping the original backup untouched. This will allow you to recover to the last backup of the pki structure but retain the original state of the certificates.

The antivirus server component of SCS 3.1 and SAVCE 10 uses encryption to secure communication with their managed clients. If the certificates used to encrypt/decrypt the communication are lost (due to hardware failure or system migration) the relationship between the server and managed clients will be broken and you may need to re-install all clients! Therefore we recommend backing up the folder on the server where these certificates are stored. This will minimize recovery time in the event of a Primary Server failure.

Backing up the pki folder

The pki folder is located in the primary server's Symantec AntiVirus program folder. The default location depends on your operating system and whether you installed Symantec AntiVirus or Symantec Client Security:

- When Symantec AntiVirus Corporate Edition server is installed on Windows, the default program folder is <OS drive>:\Program Files\SAV.
 - When Symantec Client Security server is installed on Windows, the default program folder is <OS drive>:\Program Files\SAV\Symantec AntiVirus.
- For help with this, read the "To find the Symantec AntiVirus program folder" section in the Technical Information section of this document.

After you locate the pki folder, make a copy of it and secure it in a safe location such as a removable hard drive in a vault or alternate location.

For more on backing up the pki folder and restore communication of your primary server using the backup of the pki folder, go to www.symantec.com and search for **Document ID:2005040513373748**. Click on the first link, "Steps to minimize recovery time in the event of a server failure".

Creating an EduTech Login for your Server Group

For EduTech to better assist you in troubleshooting your Symantec installation, we need a login to the Symantec portion of that server. The access can be read-only. To create the login/password on that server, do the following:

1. Start up the Symantec System Center Console on the Primary Server
2. Expand the System Hierarchy to see your "Server Group"

3. Click once on System Hierarchy and then choose **View** → **Symantec Antivirus** from the menu bar.
4. Right click on your server group name and select **Unlock Server Group**. Enter the username and password for the server group.
5. Highlight the server group and right mouse click. Click on **Account Management...**
6. On the Configure Server Group Accounts window, click the **Add...** button.
7. On the Account Setup window, enter **EduTech** for the username and create a password. Once you have created the username and password for the EduTech account, send this information along with the server name and server IP number to the EduTech Help Desk at sendit.helpdesk@sendit.nodak.edu.
8. Under the Account Type in the same window, make sure the Read-only account line is checked. Click **OK**.
9. Click **Finished**.

After you have created the login/password, please notify sendit.helpdesk@sendit.nodak.edu with that information to include your name, district, email address, telephone number and the password you created.

Setup and Management of Client Groups

Once you have your primary server installed and before you install the clients, you may wish to setup client groups for different collections of computers. The real benefit is for applying different firewall policies and antivirus settings to different groups of computers. Not all of your clients may require the same settings, so by creating client groups and collecting similar clients in those groups you'll be able to apply settings and policies to just those clients.

For example, computers in a particular computer lab may require more restrictive firewall policies than individual teacher computers. You can create client groups called "TeacherSystems" and "LabComputers" and move computers into the corresponding group. Antivirus settings can be configured separately for each client group and different firewall policies can be applied to each set of computers.

You may find it beneficial to put all the Windows 98 users in their own client group. Since they will not use the Symantec Firewall, this will allow you to avoid pushing any firewall policies to them.

For a detailed explanation of creating and managing client groups, go to www.symantec.com and search for **Document ID:2005041618530548**. Click on the first link, "Creating and managing client groups in Symantec Client Security 3...".

Section 5: Firewall and Intrusion Prevention System

Symantec Client Firewall and the Intrusion Prevention System (IPS) protect client computers and data by monitoring connections with the Internet and between networks.

The centralized security management capabilities of SCS allow you to customize your firewall and IPS protection without requiring per-machine maintenance.

Different firewall configurations are achieved by pushing out client firewall policies. These policies are sets of firewall rules and configuration options that control the client firewall's operation.

Planning Firewall Implementation

We strongly encourage you to read Symantec Document 2005041718372548, “Creating a custom policy for Symantec Client Firewall 8.x...”. and Chapter 3 of the SCS Administrators Guide if you plan to customize the firewall. Developing firewall rules that do not interfere with legitimate user activity while reducing or eliminating the number of prompts users see is the most challenging part of managing SCS within an organization.

Your implementation of the Symantec Client Firewall will be much more effective if you begin by developing a plan for creating firewall policies and distributing them. A well thought out plan will maintain the firewall's effectiveness without preventing users within your district from completing their necessary computing tasks. The following points should be considered:

How Many Different Policies Should be Distributed

Your district size and the needs of different client groups will be guiding factors in deciding how many different firewall policies you should develop. Another significant point is how much time you and your technology staff can spend developing and troubleshooting different firewall policies.

Level of User Customization

You have the ability to set which features users can configure or view in the firewall. Blocked features are grayed-out or removed from the firewall user interface.

Policy Maintenance

Once your firewall policies have been developed and deployed, there is still maintenance to be performed on each policy. You will need to update firewall policies as new applications are installed (or existing applications are updated) and as new network attacks threats are identified. An essential component of a successful firewall implementation plan will include a description of how you will regularly update your firewall policies and distribute updates to your clients.

Testing

Before they are distributed, all rules and firewall settings should be thoroughly tested on computers with similar setup, software and configuration to those used by your users. The goal is to develop rules and policies that provide maximum protection and allow users to perform all necessary computing tasks while reducing or eliminating the number of warnings/alerts asking for end-user intervention.

Installing Symantec Client Firewall Administrator

1. Insert the Symantec Client Security CD into the CD-ROM drive. If your computer is not set to run a CD automatically, you must manually run Setup.exe.
2. In the Symantec Client Security panel, click **Install Symantec Client Security → Install Symantec Client Firewall Administrator**.
3. In the Welcome panel, click **Next**.
4. In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.
5. In the Destination Folder panel, do one of the following:
 - a. To accept the default installation folder, click **Next**.
 - b. To specify a custom folder, click **Change**, locate and select a destination folder, click **OK**, and then click **Next**.
6. In the Ready to Install the Program panel, check **Add Symantec Client Firewall Administrator shortcut on your desktop**, if necessary.
7. Click **Install** to begin the installation.
The InstallShield Wizard installs all of the necessary files onto the computer.
8. Click **Finish**.
 - For information on best practices for creating a Symantec Client Firewall policy file, go to www.symantec.com and search for **Document ID:** 2005100315004748. Click on the first link, “Best practices for creating a Symantec Client Firewall policy file”.
 - For detailed information on creating a custom policy for Symantec Client Firewall or Symantec Client Security 3.x go to www.symantec.com and search for **Document ID:** 2005041718372548. Click on the first link, “Creating a custom policy for Symantec Client Firewall 8.x...”.

Training the firewall

To prepare your client machines for using the firewall and a given policy you set, you first need to train a client to “behave” in a given manner when accessing the internet, network or programs that access the internet. It is best to carry this out in multiple stages.

First, install the SCS client and the Symantec Client Firewall Administrator to a test or prototype computer that best reflects the majority of computers in your district. You’ll then want to change the Access Control Alert switch so you can see the prompts; Permit, Block, Permit Once, Block Once, etc. To do this:

1. Click **Start→All Programs→Symantec Client Security→Symantec Client Firewall**.
2. Once the firewall has opened, click on **Client Firewall** and on the bottom right and click on **Configure**.
3. With the **Firewall** tab chosen, click on **Custom Level**.
4. Near the bottom of the Firewall window, there is a choice for **Enable Access Control Alerts**. Check that box and click **OK**.

5. Click **OK** on next window and the **X** in the upper right corner to close the Symantec Client Firewall window.

Now you begin training the firewall to distinguish between acceptable and unacceptable network applications by using the prototype computer as if you were a typical user. Access programs, internet sites, and perform day-to-day activities, etc. While carrying out these actions you will see Security Alert screens prompting you to make choices for: Permit Always, Block Always, etc. As you answer these questions, you are developing rules that instruct the firewall on how it can respond to future activity.

After you are satisfied that you have trained the firewall to understand most of the situations your users are likely to experience, you will export these rules from the SCS client, copy them to the server where the Firewall Administrator is installed, import the rules into the firewall administrator and create a policy.

1. To export the ruleset in an XML format, open the Symantec Client Firewall on the client
2. On the top menu, click on **Options**
3. Select the Settings Manager tab and click **Export Settings**
4. Select a location and choose a filename and click **Save**
5. A Confirm Import/Export window will appear, click **Yes**
6. To import the ruleset (the XML file you exported from the client) into the Firewall Administrator application, copy the XML file to your primary server
7. Once on your primary server, open the Symantec Client Firewall Administrator
8. On the menu bar, click **File→Import**
9. Click **OK** on the File Import Data Selection window
10. Navigate to where you stored the XML file you copied from the client
11. Change the Files of Type to .xml, select the XML file and click **Import**
12. Click **OK** on the IPS Signatures and Settings Read Warning window
13. Now you can make any changes (or not) to that policy. When finished, click on the menu bar and click **File→Save As**
14. Click **OK** on the File Save Data Selection window
15. Select a location, fill in a filename, make sure the file type is .cfp and click **Save**.
16. You have now created a firewall policy that can be distributed to desktop clients.

You can now distribute the newly created firewall policy to a second set of test computers on which you have installed SCS. Repeat your tests on these new computers.

1. Open Symantec System Center on your primary server
2. Unlock the server group and change the view you are in by clicking on the menu bar and choosing **View→Symantec Client Firewall**
3. Highlight the client group you wish to push the newly created policy too

4. Right mouse click that client group and choose **All Tasks**→**Symantec Client Firewall**→**Update Client Policy Now**
5. In the Open window, find the location where you stored the policy you created, select that file and click **Open**
6. A Symantec Client Firewall Management Snap-In window will appear, click **OK**

During this next phase of testing, you will most likely encounter new situations that will generate new prompts that will create additional rules. After everything appears to be running smoothly within that test group, export the policy from each client and merge them into the Firewall Administrator. Once merged, use the Firewall administrator to edit the rules as necessary.

1. To merge multiple policies, you should first have the policies from the clients stored on your primary server in a .cfp format as explained in the last section.
2. Open the Symantec Client Firewall Administrator on your primary server
3. Click **File**→**Open** and locate the first file and click **Open**
4. To merge the next file click **File**→**Merge** and locate the file to be merged and click **Open**
5. A Merge Options window will appear and select **All Rules**
6. The first policy should now contain the Rules and pRules from both policies
7. Repeat steps 3 – 5 for other policies you wish to merge

Repeat the cycle of refining, distributing and merging rule sets as necessary until you are satisfied with the rules you have created. At that point you can push the policy to the appropriate client groups using the Symantec System Center.

Keep in mind that you may need to make minor modifications to your firewall policies as the software in use on client machines is updated (for example, moving from Internet Explorer 6 to Internet Explorer 7).

Open firewall policy

It would be impossible for EduTech to develop firewall policies that are trained to reflect the many unique environments present in the districts connecting directly to our SCS management servers. Therefore we use what we call an “open firewall policy” for those clients. That doesn’t mean the firewall is left wide open for attacks, it simply means that many prompts and notifications are disabled and most user initiated network activity is allowed by default.

Our firewall policy allows the computer to accept Internet traffic the user instigates without prompting the user to make decisions. Even with this level of openness, there may be instances where a user identifies that the firewall is blocking some activity or function from working. Therefore the open policy provides users with the ability to add programs or IP addresses to their list of trusted programs/sites. Schools operating their own SCS management servers may contact the EduTech Help Desk if they wish to obtain a copy of this firewall policy for their own use.

Note: If the Symantec Client Firewall were completely turned off, the computer would still be protected from most Internet attacks by the IPS. The IPS monitors incoming/outgoing traffic and compares the activity to known exploits, hacks and suspicious behaviors. It works in conjunction

with the firewall and antivirus components of SCS to take appropriate action when suspicious activity is detected.

Section 6: Installing Windows Clients

Before installing any client software, remember to uninstall any anti-virus software that is currently installed unless this is an upgrade to a current Symantec AntiVirus Corporate Edition installation.

There are several ways to install the client software. Two of the more common are via a Web-based install or using the application CD. If EduTech will be managing your client(s), the easiest method is to use the Web-based installer. This requires the desktop to be running Internet Explorer 5.5 SP2 or later. If you are setting up your own definition server or running a browser other than Internet Explorer, you may elect to use the application CD for installation.

If EduTech will be managing your clients and you must use the CD for installation, please contact the EduTech Help Desk at sendit.helpdesk@sendit.nodak.edu with the following information:

- Your name
- School/district name
- Computer name(s) of the client machines

EduTech will need to make sure the appropriate management policy is applied to these machines.

Client Installation via CD

1. 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 the installation.
2. At each machine[†], insert SCS 3.1 CD Disc 1 (Windows Software). If the “Symantec Client Security” window does not appear automatically after a few moments, then locate SETUP.EXE on the CD drive’s contents and double-click on it.
3. Choose **Install Symantec Client Security** → **Install Symantec Client Security Client** from the Install Menu.
4. At the Welcome screen, click **Next**. Read and accept the terms of the license agreement and click **Next**.
5. On the Symantec Client Security InstallShield Wizard window, make sure the **Complete** radio button is chosen and click **Next**.
6. If you are running your own Primary Server or you are unable to use the web installer, select **Managed**.
7. The next screen asks for the server name. Enter the IP address or name of your Primary Server or the name of the EduTech Primary Server by clicking **Browse** → **Find Computer**

[†] For information on performing alternate installation methods that do not require you to visit each machine, refer to Chapter 7 in the SAVCE Installation Guide (/Docs/savinst.pdf on Disc 1 of the SAVCE 10 media pack)

and in **Search For** type scs.sendit.nodak.edu after which click **Find**. Finish by clicking **OK** and **Next**.

8. Next click **Install**.
9. After the client install is completed, click **Finish**.
10. You'll see a prompt for restarting your computer, click **Yes** to restart now or **No** for later. We recommend clicking **Yes**.
11. After a restart you'll see a prompt informing you the Windows Firewall is disabled. When the Symantec firewall is installed it disables the windows firewall. Click **OK**.
12. **NOTE: You are strongly encouraged to go to www.edutech.nodak.edu/support/antivirus/ and install any patches to keep your installation current and protected.**

Client Installation via Web Browser

1. 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.
2. Open Internet Explorer (IE) and go to www.edutech.nodak.edu/support/scswebinstall
3. Next the Symantec Client Security Web Install webpage will be displayed showing the City, Client Group and the District the client will be installed too.

NOTE: Before proceeding to the appropriate web install link, you'll want to uninstall Symantec Live Update and AntiVirus on any definition server you are currently running and run the web install link for AntiVirus Client for Servers. After that is completed you can then precede to the clients/workstations.

- a. If these are correct, click on the **SCS 3.1** link for Windows 2000/XP/2003, **Symantec AntiVirus for Vista** link Windows Vista, **Symantec AntiVirus V9** link for Windows 98 or **AntiVirus Client for Servers** link for Windows Server 2000/2003 depending on the computer's operating system.
 - b. If the district, city, etc... are incorrect, please contact the EduTech Help Desk at sendit.helpdesk@sendit.nodak.edu.
4. The web installation requires ActiveX controls. If ActiveX is not installed, you may see a prompt for doing so.
 5. Click on **Install Now**.
 6. Skip to step 10 if not using the Vista installation.
 7. Vista users will see a dialog box for User Account Control, click **Continue**.
 8. Vista users will also see a dialog box for installing the web installer, click **Install**.
 9. Vista user, a dialog box for User Control for Symantec AntiVirus for 10.2, click **Continue**.
 10. When the Symantec Client Security InstallShield Wizard window appears, click **Next**.
 11. Click the radio button **I accept the terms in the license agreement** and then click **Next**.

12. Make sure the radio button for **Complete** is checked and click **Next**.
13. On the next window click the **Install** button.
14. You may encounter two windows: Old Definition Files and a scan window, click **Close** on both.
15. The LiveUpdate screen may appear, if so click **Next**.
16. After it completes click **Finish**.
17. Before going onto the next step, make certain the LiveUpdate Updating Virus Protection Files window has completed it's task.
18. Next click **Finish** on the InstallShield Wizard Completed screen.
19. Skip to next step if not installation the Vista version of Symantec AntiVirus.
20. You'll see a prompt for restarting your computer, click **Yes** to restart now or **No** for later. We recommend clicking **Yes**.
21. After a restart you'll see a prompt informing you the Windows Firewall is disabled. When the Symantec firewall is installed it disables the windows firewall. Click **OK**. You won't see this screen if installing to Windows 98 or Windows Servers 2000/2003 as clients.