State of South Dakota K-12 Data Center

SYMANTEC ENDPOINT PROTECTION MIGRATION INSTRUCTIONS

south dakota
DEPARTMENT OF EDUCATION
Learning. Leadership. Service.

Symantec Endpoint Protection Migration Checklist

Refer to the following checklist for migrating to Symantec Endpoint Protection from either Symantec Antivirus or Symantec Client Security.

- ☐ Install the Symantec Endpoint Protection Manager Console
- ☐ Configure your Symantec Endpoint Protection admin account
- ☐ Configure the general settings for your school
- ☐ Setup location awareness
- ☐ Export Symantec Endpoint Protection client install packages
- ☐ Choose a Windows 2003/2008 server on your network to distribute virus definitions within your school network (this server will be known as the "Group Update Provider")
- ☐ Uninstall all previous versions of Symantec from the Group Update Provider
- ☐ Install the Symantec Endpoint Protection client to the Group Update Provider
- ☐ Configure your school district's policies and settings to utilize the Group Update Provider
- ☐ Disable Windows Firewall through Group Policy
- ☐ Uninstall all previous versions of Symantec from the rest of your school's desktops, laptops/tablets, and servers (except for your original Symantec server and the workstation that has Symantec System Center Console installed)
- ☐ Deploy Symantec Endpoint Protection to your school's desktops, laptops/tablets, and servers (except for the original Symantec server and the Symantec System Center Console workstation)
- ☐ Once Symantec Endpoint Protection has been deployed to the entire school, uninstall all previous versions of Symantec from the original Symantec server and from the Symantec System Center Console workstation
- ☐ Deploy Symantec Endpoint Protection to the original Symantec server and the workstation
- ☐ (Optional) Move the Group Update Provider role to the original Symantec server

Introduction

Overview

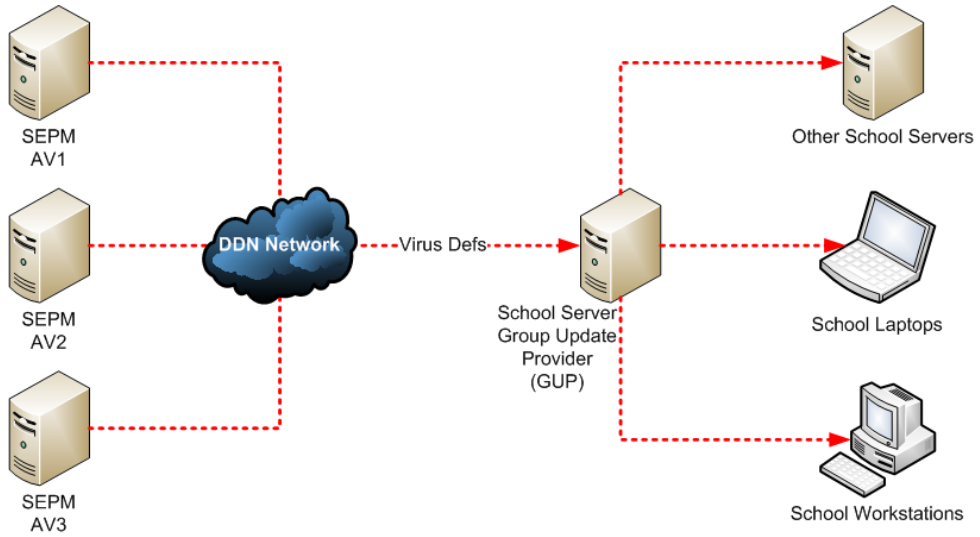
- Symantec Endpoint Protection (SEP) is the next version of Symantec Antivirus
- It has been completely redesigned from top to bottom
- SEP requires dedicated management servers and SQL database servers
- It includes antivirus, antispyware, firewall, intrusion prevention

Centrally Hosted

- SEP Management servers will be hosted at K-12 Data Center
- School districts will no longer have to dedicate a server for Symantec
- Schools have full-control over the policies and settings used in their district through a Java based console

Virus Definition Distribution

- Virus definitions distributed within the school by the Group Update Provider (GUP)
- The GUP can be any Windows Server in your school that is running the Symantec Endpoint Protection client
- The GUP downloads new virus definitions from the SEP Management servers
- The remaining clients in your district download the virus definitions locally from the GUP, reducing the load on your school's bandwidth



Exercise 1: Install the Symantec Endpoint Protection Manager Console

You will be able to manage the Symantec Endpoint Protection settings for your school by installing the Symantec Endpoint Protection Manager (SEPM) Console. This is a Java based application that grants you full control of the clients and settings in your school.

1. The Symantec Endpoint Protection Manager (SEPM) Console specifically requires **Java 6 update 7**. Other versions of Java may not work, including newer versions.

   Note: *This is only required for computers where you install the SEPM Console.*

   a. If necessary, uninstall any other versions of Java from the Tech Coordinator's workstation (or the computer you plan to use in managing Symantec Endpoint Protection).

   b. Install **Java 6 update 7**.

2. Install the SEPM Console:

   a. Launch **Internet Explorer** and browse to: **http://av.k12.sd.us:9090**

   b. Click on the **Click here to download and log in to the Symantec Endpoint Protection Manager** link.

   c. Java will start downloading and installing the SEPM Console.

   d. If prompted, checkmark **Always trust content from this publisher** and click **Run**.

   e. On the Information window, checkmark **Don't show this message again** and click **OK**.

   f. The SEPM Console login window will appear.

   g. Click **Exit**.

      Note: *You must exit the SEPM console window at this time.*

   h. Close **Internet Explorer**.

3. Launch the SEPM Console:

   a. The installer automatically placed an icon named **Symantec Endpoint Protection Mgr** on your desktop.

b. If you're running **Windows XP**, double-click on the icon to launch the SEPM Console.

c. If you're running **Windows Vista**, **Windows 2008**, or **Windows 7**, right-click on the icon and choose **Run as administrator**.

Note: *You must use "Run as administrator" when launching the SEPM console from Windows Vista, Windows 2008, or higher. Otherwise it will not work properly.*

Additional Note: *You cannot change the properties of the icon so it always launches as administrator. The icon is refreshed every time the SEPM Console is launched, so any changes made to the icon's properties are not retained.*

d. User name: **K12-Username** *(must be lowercase – example: ab123)*

e. Password: **symantec**

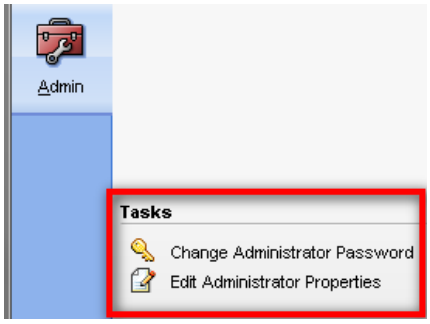
f. Verify that the Server field is set to **av.k12.sd.us:8443**

g. Click **Log On**.

h. If prompted, checkmark **Always trust content from this publisher** and click **Yes**.

4. Configure your SEPM administrator account:

a. Within the SEPM Console, click on the **Admin** icon (bottom-left).



b. In the Tasks area, click **Change Administrator Password**.

c. In the Change Password window, enter and confirm a new password of your choice.

d. Click **OK** to set your new password.

e. Click **Edit Administrator Properties**.

f. In the **Email** field, type in your K-12 e-mail address.

g. Click **OK**.

Exercise 2: Configure Policies and Settings

Symantec Endpoint Protection uses various settings and policies to manage the protection in your district. Your school will already inherit several default policies that should be sufficient for most school districts. However, every school will need to make a few basic customizations before they deploy Symantec Endpoint Protection in their school district.

Configure general settings

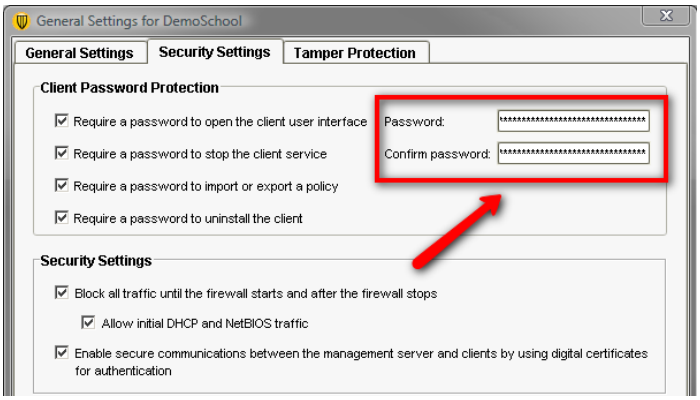
These general settings should only have to be configured once.

1. Login to the SEPM Console.
2. Click on the **Clients** icon.
3. Click on your school district's name in the **View Clients** hierarchy list.
4. Click on the **Policies** tab.
5. Uncheck **Inherit policies and settings from parent group "My Company"**

> **Be careful not to re-checkmark the "Inherit policies" setting. Doing so will reset any changes you make back to the defaults.**

6. Ensure that policy inheritance is **OFF**.
7. In the **Location-independent Policies and Settings** area, click on the **General Settings** link.

8. In the General Settings window, under the General Settings tab:
    a. Uncheck **Remember the last location**.
    b. Checkmark **Enable Location Awareness**.
    c. Choose **Prompt the user to restart the computer**.
9. Under the Security Settings tab:
    a. Enter a new password in the **Password** and **Confirm password** fields. (This prevents end-users from stopping or uninstalling the Symantec client.)



Note: *The default password is set to "symantec" but it's recommended that you change this to something unique.*

b. Checkmark all of the following options:

- **Require a password to open the client user interface.**
- **Require a password to stop the client service.**
- **Require a password to import or export a policy.**
- **Require a password to uninstall the client.**
- **Block all traffic until the firewall starts...**
- **Allow initial DHCP and NetBIOS traffic**
- **Enable secure communications between management server and clients**

c. Click **OK** to close the **General Settings** window.

Create and manage locations

Symantec Endpoint Protection clients have the ability to detect which network location your computers are connected to. This allows you to use different policies on and off the school network.

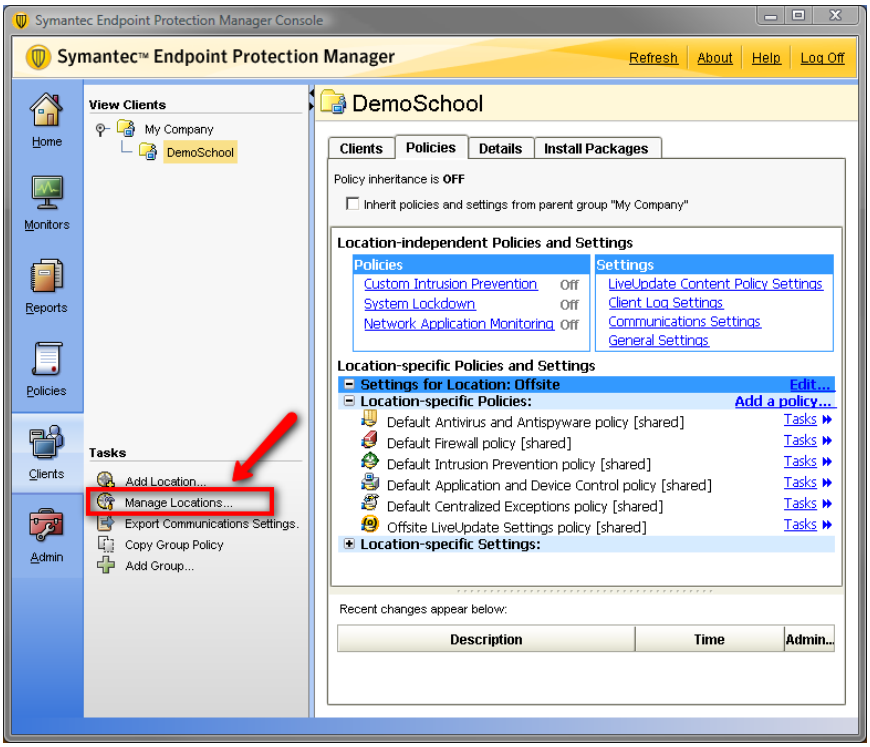
The recommended configuration will be to have two locations: offsite location and school network location.

This section can be confusing unless you follow the instructions precisely. Refer to the screenshots for additional clarification.

1. Login to the SEPM Console.
2. Click on the **Clients** icon.
3. Click on your school district's name in the **View Clients** hierarchy list.

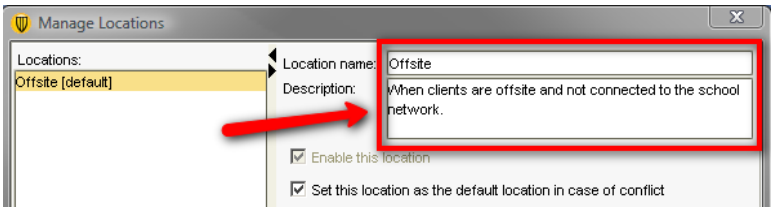
4. Click on the **Policies** tab.

5. Click on **Manage Locations...** in the Tasks area.



6. In the Manage Locations window, verify the Location name field is set to **Offsite**

7. Verify the Description field is set to: **When clients are offsite and not connected to the school network.**

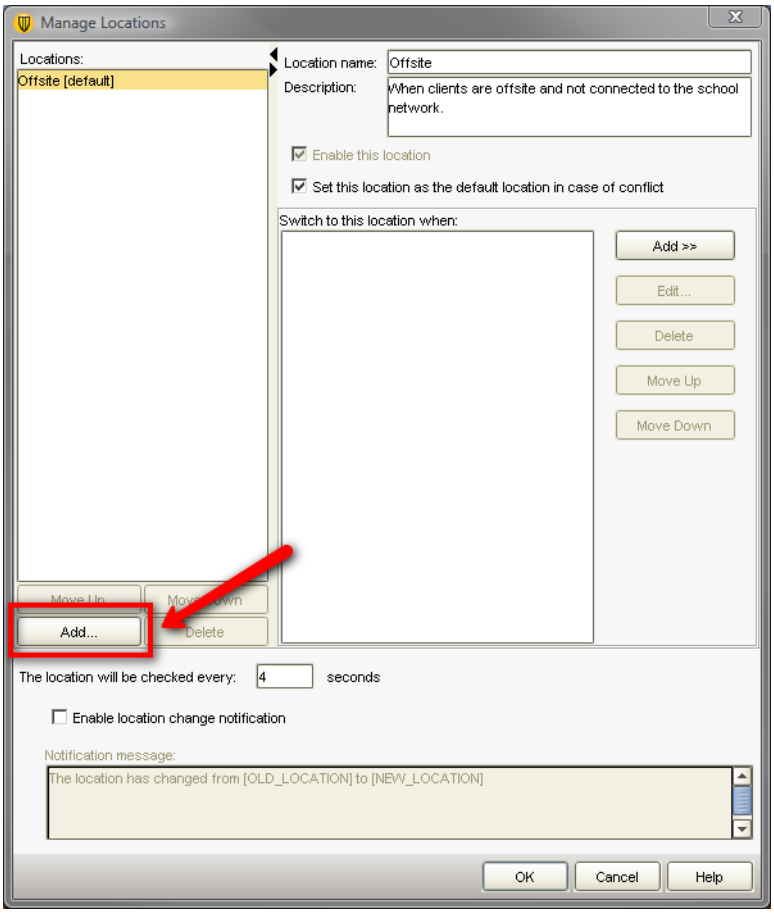


8. Checkmark **Set this location as the default location in case of conflict**.

9. Create the School Network location:

    a. Underneath the Locations area, click the **Add...** button.

    Note: *There are two add buttons on the screen. This step uses the one on the bottom left. (Refer to the screenshot below.)*



b. In the Name field type: **School Network**

c. In the Description field type: **When clients are connected to the school network.**

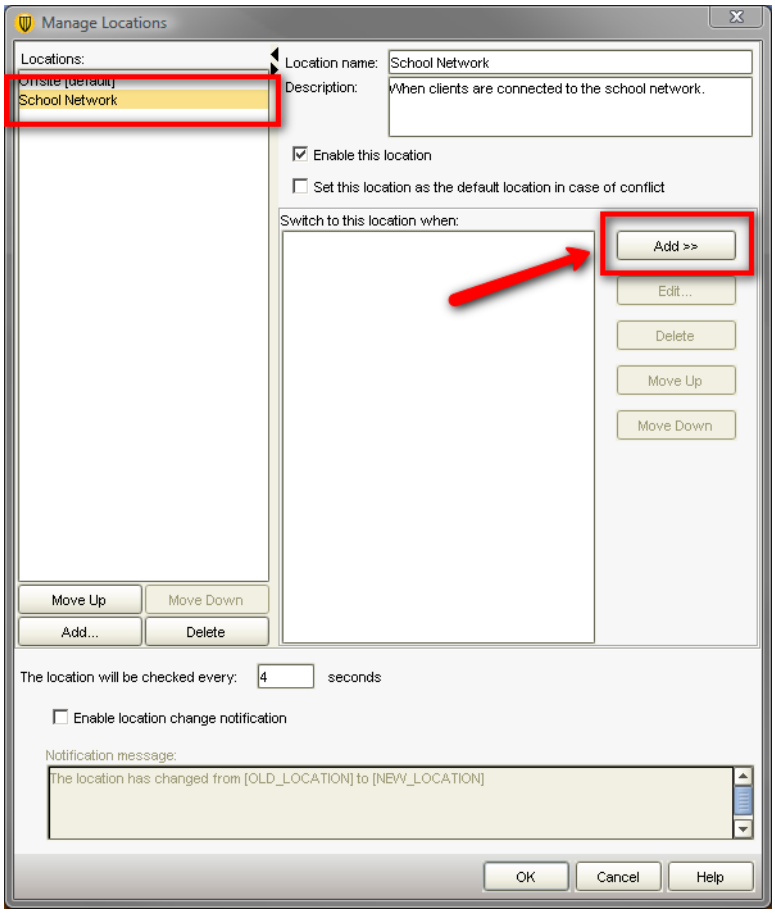
d. Click **OK**.

10. Set the criteria for the School Network:

a. In the Locations area, select **School Network**.

b. In the **Switch to this location when:** area, click the **Add** button.

Note: *There are two add buttons on the screen. This step uses the one on the top right. (Refer to the screenshot below.)*



c. In the Specify Location Criteria window:

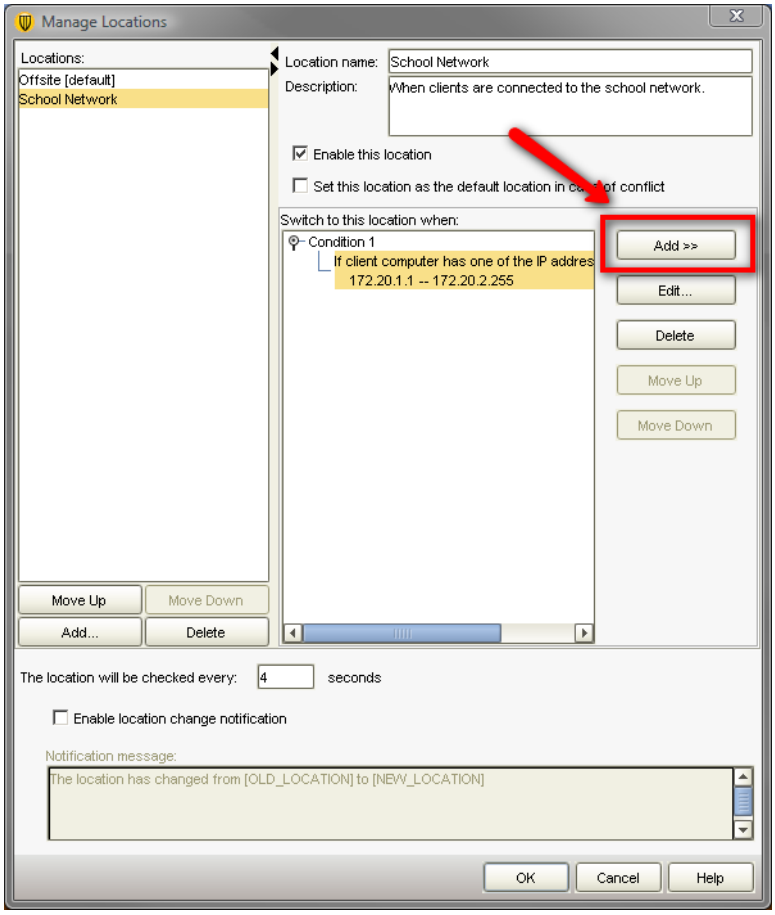
   1. In the Type drop-down menu, choose **Computer IP Address**.
   2. Choose the **If the client computer has one of the IP addresses listed below** radio button.
   3. Click the **Add** button.
   4. In the Address window, in the Type drop-down menu, choose **IP Range**.
   5. Enter the **Start** of your school network's IP address range.
   6. Enter the **End** of your school network's IP address range.
   7. Click **OK**.

      Note: *If your school has multiple IP address ranges, repeat the previous steps until you've added all of your school network's IP ranges.*

   8. Once you've added all of your school network's IP ranges, click **OK** to close the Specify Location Criteria window.

d. Back in the Manage Locations window, in the **Switch to this location when:** area, click the **Add** button again.

Note: *There are two add buttons on the screen. This step uses the one on the top right. (Refer to the screenshot below.)*

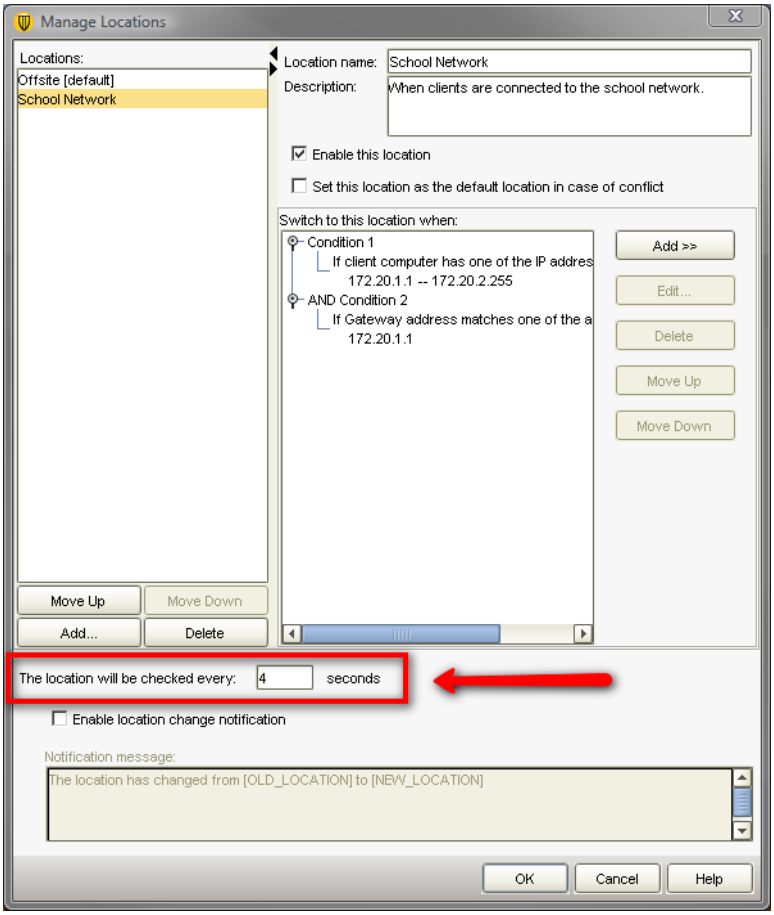


e. Choose **Criteria with AND relationship...**

f. In the Specify Location Criteria window:

   1. In the Type drop-down menu, choose **Gateway Address**.
   2. Choose the **If the Gateway address of the client computer is one of the addresses listed below** radio button.
   3. Click the **Add** button.
   4. In the Address window, in the Type drop-down menu, choose **IP Address**.
   5. Enter the **IP Address** of your school network's gateway.
   6. Click **OK**.
   7. Once you've finished, click **OK** again to close the Specify Location Criteria window.

g. In the Manage Locations window, change the setting **The location will be checked every** to **4** seconds.



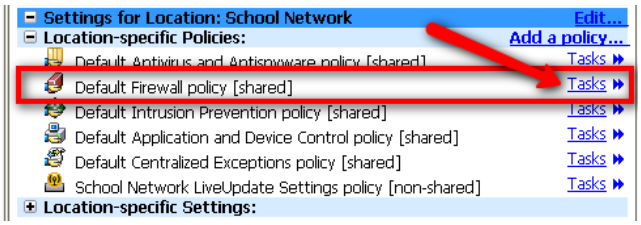
h. Click **OK** to close the **Manage Locations** window.

Configure the School Network location

Configure the policies and settings used in the School Network location.

1. Login to the SEPM Console.
2. Click on the **Clients** icon.
3. Click on your school district's name in the **View Clients** hierarchy list.
4. Click on the **Policies** tab.
5. In the **Settings for Location: School Network → Location-specific Policies** area, withdraw the firewall policy:

    a. Click on the **Tasks** link to the right of **Default Firewall policy [Shared]**.



b. Choose **Withdraw Policy**.

c. In the Withdraw Policy window, verify it says **Firewall Policy** and click **Yes**.

6. Verify that the firewall policy is no longer listed under the School Network policies area.

Exercise 3: Exporting Symantec Client Install Packages

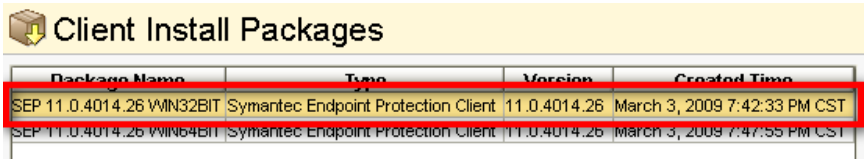
Instead of downloading the installer from the K-12 Data Center's Members web site, with Symantec Endpoint Protection you download the client install packages directly from within the SEPM Console. This allows you to download a package specifically tailored to your school.

In Symantec Endpoint Protection, client install packages are for workstations and servers. In this case, the term "client install package" does not mean it is only for workstations. "Client" indicates it is a SEP client that connects back to the SEP servers hosted at the K-12 Data Center.

Export a client install package for 32-bit (x86) servers

This includes any server running the 32-bit version of Windows 2000, Windows 2003, or Windows 2008.

1. In the SEPM Console, click on the **Admin** icon.
2. Click on **Install Packages**.
3. In the Client Install Packages pane, right-click on **SEP 11.0.4202.75 WIN32BIT**, and choose **Export**.



Note: *A newer build may have been released since these instructions were written, so pick the newest build available.*

4. In the Export Package window:
    a. Set the **Export folder** to a network share.

    Note: *Use a network share that is accessible only by administrators from all computers in your network*

    b. Checkmark **Create a single .EXE file for this package**.

    c. In the Pick the customized installation settings below drop-down menu, choose **DDN Installation Settings**.

    d. In the Select the features you want to use drop-down menu, choose **DDN Default Server Feature Set**.

    Note: *Make sure you choose the **server** feature set.*

    e. Choose **Export a managed client**.

    f. Checkmark **Export packages with policies from the following groups**.

    g. Checkmark your **SchoolName** in the hierarchy list.

h. Checkmark **Add clients automatically to the selected group**.

i. In the Preferred Policy Mode area, choose **Computer mode**.

j. Click **OK** and wait for the installation package to be exported.

5. Click **Close** when the export is complete.

6. Minimize the SEPM Console window.

7. Rename the exported client installation package:

   a. Browse to the network share.

   b. Within a folder named **My Company_SchoolName** *(example: "My Company_Madison" or something similar)*

   c. Rename **setup.exe** to instead be **SEP_11.0.4202.75_WIN32BIT_servers.exe**

      Note: *A newer build may have been released since these instructions were written, so use the name of build you picked.*

   d. After renaming the client installation package, you may choose to move it out of the **My Company_SchoolName** folder.

   e. You may then delete the empty **My Company_SchoolName** folder.

Important consideration for renaming the client installation packages:

Build Number: give them the same name as the build from the SEPM Console. This way when new builds are released, you'll know which version the exported package is.

Server/Workstation: designate whether the install package is for servers or workstations, because they use a different feature set.

Underscores: use underscores instead of spaces so it's easier to deploy with tools such as Altiris.

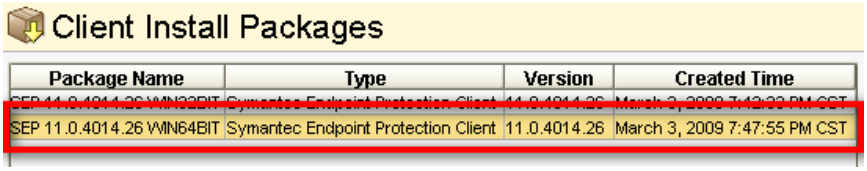
Export a client install package for 64-bit (x64) servers

This includes any server running the 64-bit version of Windows 2003 or Windows 2008.

1. In the SEPM Console, click on the **Admin** icon.

2. Click on **Install Packages**.

3. In the Client Install Packages pane, right-click on **SEP 11.0.4202.75 WIN64BIT**, and choose **Export**.



Note: *A newer build may have been released since these instructions were written, so pick the newest build available.*

4. In the Export Package window:

    a. Set the **Export folder** to a network share.

    Note: *Use a network share that is accessible only by administrators from all computers in your network*

    b. Checkmark **Create a single .EXE file for this package**.

    c. In the Pick the customized installation settings below drop-down menu, choose **DDN Installation Settings**.

    d. In the Select the features you want to use drop-down menu, choose **DDN Default Server Feature Set**.

    Note: *Make sure you choose the **server** feature set.*

    e. Choose **Export a managed client**.

    f. Checkmark **Export packages with policies from the following groups**.

    g. Checkmark your **SchoolName** in the hierarchy list.

    h. Checkmark **Add clients automatically to the selected group**.

    i. In the Preferred Policy Mode area, choose **Computer mode**.

    j. Click **OK** and wait for the installation package to be exported.

5. Click **Close** when the export is complete.

6. Minimize the SEPM Console window.

7. Rename the exported client installation package:

    a. Browse to the network share.

    b. Within a folder named **My Company_SchoolName** *(example: "My Company_Madison" or something similar)*

    f. Rename **setup.exe** to instead be **SEP_11.0.4202.75_WIN64BIT_servers.exe**

    Note: *A newer build may have been released since these instructions were written, so use the name of build you picked.*

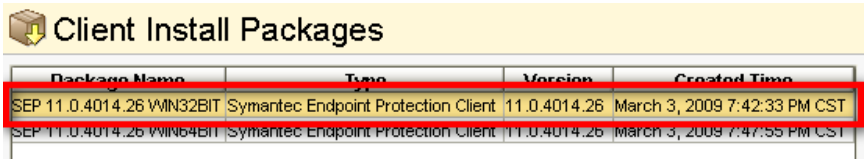
g. After renaming the client installation package, you may choose to move it out of the **My Company_SchoolName** folder.

h. You may then delete the empty **My Company_SchoolName** folder.

Export a client install package for 32-bit (x86) workstations

This includes any workstation, desktop, laptop, or tablet pc running the 32-bit version of Windows XP, Windows Vista, or Windows 7.

1. In the SEPM Console, click on the **Admin** icon.
2. Click on **Install Packages**.
3. In the Client Install Packages pane (top-right), right-click on **SEP 11.0.4202.75 WIN32BIT**, and choose **Export**.



Note: *A newer build may have been released since these instructions were written, so pick the newest build available.*

4. In the Export Package window:

   a. Set the **Export folder** to a network share.

      Note: *Use a network share that is accessible only by administrators from all computers in your network*

   b. Checkmark **Create a single .EXE file for this package**.

   c. In the Pick the customized installation settings below drop-down menu, choose **DDN Installation Settings**.

   d. In the Select the features you want to use drop-down menu, choose **DDN Default Workstation Feature Set**.

      Note: *Make sure you choose the **workstation** feature set.*

   e. Choose **Export a managed client**.

   f. Checkmark **Export packages with policies from the following groups**.

   g. Checkmark your **SchoolName** in the hierarchy list.

   h. Checkmark **Add clients automatically to the selected group**.

   i. In the Preferred Policy Mode area, choose **Computer mode**.

   j. Click **OK** and wait for the installation package to be exported.

5. Click **Close** when the export is complete.

6. Minimize the SEPM Console window.

7. Rename the exported client installation package:

    a. Browse to the network share.

    b. Within a folder named **My Company_SchoolName** *(example: "My Company_Madison" or something similar)*

    i. Rename **setup.exe** to instead be **SEP_11.0.4202.75_WIN32BIT_workstations.exe**

    Note: *A newer build may have been released since these instructions were written, so use the name of build you picked.*

    j. After renaming the client installation package, you may choose to move it out of the **My Company_SchoolName** folder.

    k. You may then delete the empty **My Company_SchoolName** folder.

Note: If you have 64-bit workstations, repeat the previous steps, but export the WIN64BIT version of the SEP client instead.

Exercise 4: Deploy the SEP Client to the Group Update Provider (GUP)

The Group Update Provider (otherwise known as "GUP") is a role you will designate to a server in your school district's network. The function of the GUP is to download new virus definitions from the servers at the K-12 Data Center and then redistribute those definitions within your school network. This reduces the bandwidth required to keep all of your computers up-to-date.

Note: The GUP does not require a special client or installation package. Any server running the Symantec Endpoint Protection client can be designated as the GUP. You can even change which server has the GUP role at any time by updating your policies.

Choose the GUP

Refer to the following criteria when choosing the server that will function as your school's Group Update Provider. See the important note below if you have a WAN or multiple FortiGates in your district.

1. The Group Update Provider (GUP) must be a Windows 2003 or Windows 2008 server.
2. It can be either a physical server or a virtual machine (e.g. VMSECURITY).
3. The GUP has to be on the same subnet as the clients that download virus definitions from it.
4. A single GUP can only provide updates for approximately 1,000 clients. (If you have additional clients, you would need additional GUPs.)
5. **Important:** Do not choose your existing Symantec Antivirus 10 server. If you want to use your existing Symantec server, temporarily choose a different server to be the GUP, and then change it back to your Symantec server once the entire district has been migrated to Symantec Endpoint Protection.

   Note: *Your existing Symantec server should be the very last computer to migrate to Symantec Endpoint Protection, because it needs to be available to provide updates until all of your other computers have been migrated.*
6. The Group Update Provider must have a static IP address.
7. There are special considerations for schools with multiple FortiGates or a WAN:

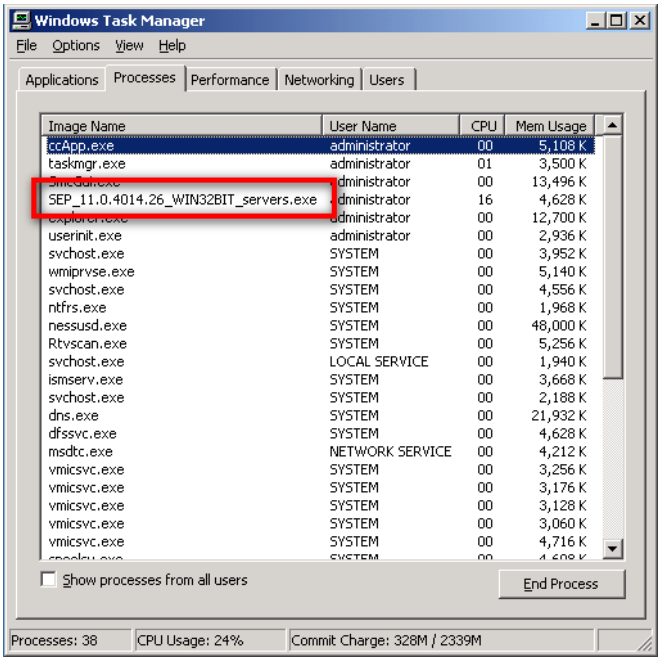
   a. **Schools with more than one FortiGate:**
   Designate a GUP behind each of the FortiGates. For example, if your elementary building and high school buildings each have their own FortiGate, you would have two GUPs—one in the elementary and one in the high school.

   b. **Schools with a Wide Area Network (WAN):**
   To reduce the bandwidth on the WAN links, place a GUP in each location or building on the WAN. For example, if you have two elementary buildings and one high school building connected by a WAN, you would have three GUPs—one in each elementary building and one in the high school building.

Install the SEP client to the GUP

The Symantec Endpoint Protection client install package build may be different than the one listed in this section. Always use the latest available build.

1. Logon to the server you've chosen to be the GUP.
2. Uninstall any/all previous versions of Symantec already installed on the GUP server, such as:
    - Symantec Antivirus
    - Symantec Client Security
    - LiveUpdate
    - Symantec System Center Console
    - Any other Symantec administration tools
3. Reboot the server after uninstalling all previous versions of Symantec.
4. Once the server has restarted, logon and install the Symantec Endpoint Protection client. *(Make sure to use the correct version of the client—either x86 or x64.)*
5. Launch Task Manager on the server. A process named **SEP_11.0.4202.75_WIN32BIT_servers.exe** (or something similar) will appear while the installer is running.



6. Once the installer has finished, the process will no longer appear in Task Manager, and the client software will appear in **Start menu → All Programs → Symantec Endpoint Protection → Symantec Endpoint Protection**.
7. Reboot the server.

8. Login to the GUP server.

9. Launch the SEP client from **Start menu → All Programs → Symantec Endpoint Protection → Symantec Endpoint Protection**.

10. When prompted, type the **password** you chose when configuring the General Settings policies (in the *Configure Policies and Settings → Configure General Settings* section of this document).

11. Click the **LiveUpdate** button.

12. Wait for LiveUpdate to finish.

13. Close out of the Symantec Endpoint Protection window.

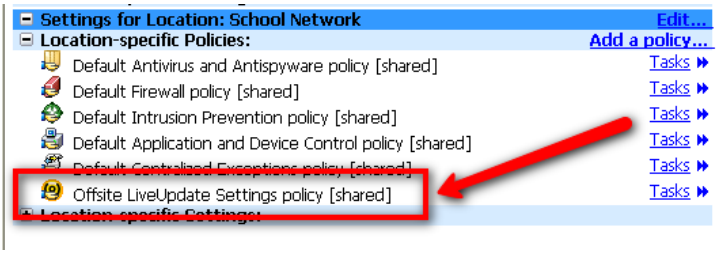
14. Log off from the GUP server.

Exercise 5: Configure the School Network location to use the GUP

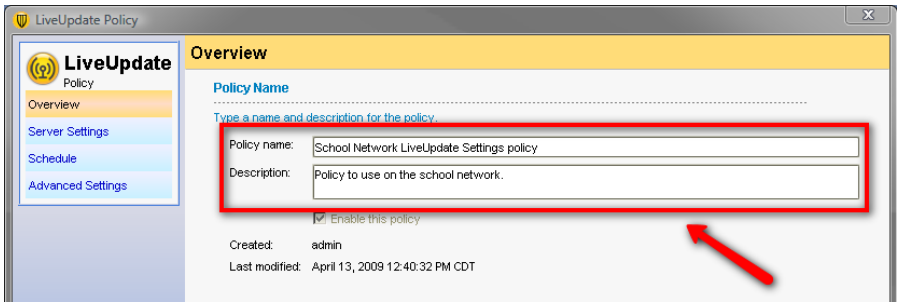
Once the Symantec Endpoint Protection client is installed on the GUP server, and you've done a manual LiveUpdate, you're ready to configure your School Network location to use the GUP.

Note: You can repeat these steps later on to move the GUP role to another server.

1. Login to the SEPM Console.
2. Click on the **Clients** icon.
3. Click on your school district's name in the **View Clients** hierarchy list.
4. Click on the **Policies** tab.
5. In the Settings for Location: School Network → Location-specific Policies area, left-click on **Offsite LiveUpdate Settings policy [shared]**.

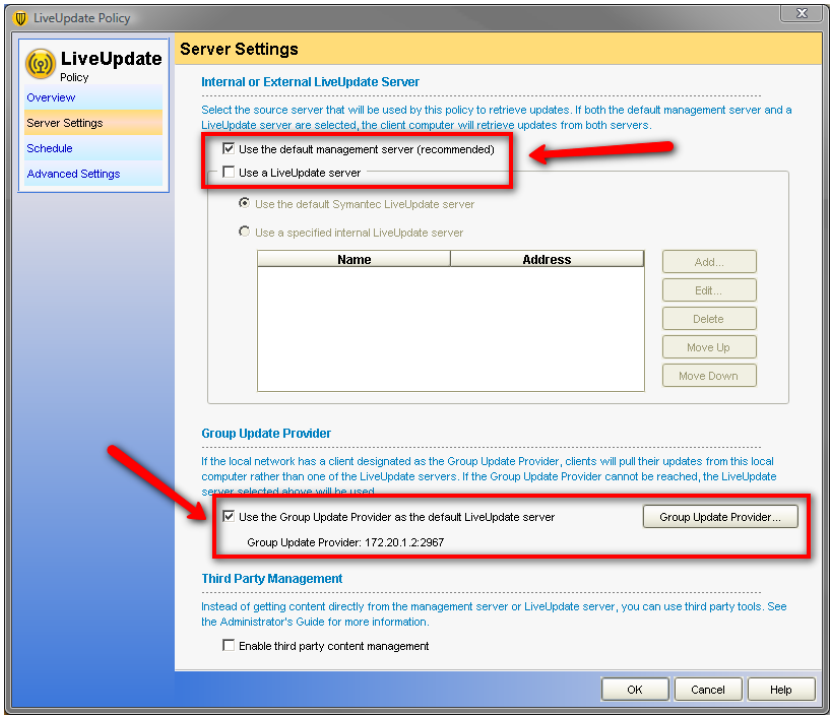


6. Choose **Create Non-Shared Policy From Copy**.
7. In the LiveUpdate Policy window:
    a. Click **Overview** from the list on the top-left.
        1. Change the Policy name field to: **School Network LiveUpdate Settings policy**
        2. Change the Description field to: **Policy to use on the school network.**

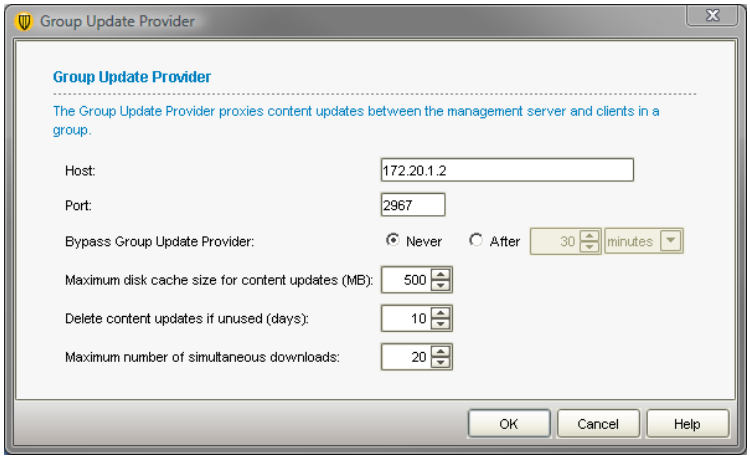


    b. Click **Server Settings** from the list on the top-left.
        1. Checkmark **Use the default management server (recommended)**
        2. Uncheck **Use a LiveUpdate server**

3. Checkmark **Use the Group Update Provider as the default LiveUpdate server**.



4. Click the **Group Update Provider...** button.
    a. In the Host field, type the **IP address of the GUP server**.
    b. Leave the Port field set to **2967**.
    c. For Bypass Group Update Provider, choose **Never**.
    d. Leave the Maximum disk cache size… set to: **500** (MB)
    e. Change Delete content updates if unused (days) to: **10**
    f. Change Maximum number of simultaneous downloads to: **20**.

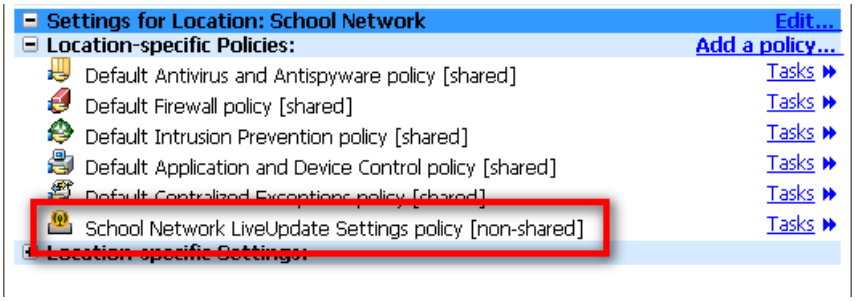


g. Click **OK** to close the Group Update Provider window.

5. Uncheck **Enable third party content management**.

c. Click **OK** to close the LiveUpdate Policy window.

8. In the Location: School Network → Location-specific Policies area, verify the policy name is **School Network LiveUpdate Settings policy [non-shared]**.



9. Your School Network location will now use the GUP to distribute virus definitions within your network.

10. There are special considerations for schools with multiple GUPs (e.g. schools with multiple FortiGates or a WAN):

a. You will need to create a location for each GUP.

b. For example: if you have a GUP for your elementary building and another GUP for your high school building, you would create a location for each building. Instead of "School Network" you might call one location "Elementary Network" and the other location "High School Network" etc.

Exercise 6: Uninstall Previous Versions of Symantec

It is important to uninstall previous versions of Symantec before deploying the new SEP client. While upgrading is possible, Symantec advises against this. In our testing, when we upgraded, we experienced problems and bugs.

There are three main ways to uninstall previous versions of Symantec that we will cover in this document. If you prefer other methods, please make sure to do a complete uninstall and reboot the computer before installing the SEP client.

Uninstall Previous Versions with Altiris

1. Launch the Symantec System Center Console.
2. Click the **View menu → Symantec AntiVirus**.
3. Look at the View column in the client list and make note of which version(s) of Symantec you have installed. Make a list of the versions, and which computers are running each version.
4. Obtain the GUID for the version(s) of Symantec installed in your school:
    a. Login to a workstation running a previous version of Symantec.
    b. Launch **REGEDIT**.
    c. Browse to the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall**
    d. Browse through each of the listed GUIDs until you find the one for Symantec. It will be obvious which one is for Symantec, as it will be listed in the information in the right-pane of the window.
    e. Once you have located the one for Symantec, write down the complete GUID. It will look something like this: **{2085C617-589C-40F8-BE40-EDBC9E2CA2EB}**
    f. Repeat this process for each version of Symantec you are running in your school.
        - So if you are only running one version of Symantec, you will only have one GUID and will create one Altiris job to uninstall Symantec.
        - If you are running two version of Symantec, you will have to find two GUIDs and will create two separate Altiris jobs.
        - Etc…
5. Create a separate Altiris job to remove each version of Symantec running in your school:
    a. Within the Altiris Deployment Console, create a new job called **Uninstall Symantec [version-number-here]**. *(So for example, if you were uninstalling Symantec Antivirus 10.1.7.7000, you would name the job **Uninstall Symantec 10.1.7.7000**, etc.)*

b. In the new Uninstall Symantec job, click **Add → Run Script**.

c. In the Run Script window, select **Run this script**.

d. In the Run this script field, type the following as one single line:
```
reg add HKLM\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AdministratorOnly\Security /v UseVPUninstallPassword /t REG_DWORD /d 0 /f
```

e. Press **Enter** to start a new line, and type the following as one single line:
```
msiexec.exe /norestart /q /x {GUID-HERE} remove=all
```

Note: *Replace GUID-HERE with the actual GUID obtained in the previous step.*

f. Press **Enter** to start a new line, and type the following as one single line:
```
shutdown /r /f /t 0
```

g. Configure the job to run as the **ServiceAltiris** account (or whatever account you use for Altiris jobs).

h. Repeat these steps to create a new Altiris job for each version of Symantec you need to uninstall from your school network.

1. Run the newly created Altiris job(s) to perform the uninstall:

   a. Make sure the target computers are running and connected to the school network.

   b. Run each Uninstall Symantec job against the computers running that specific version of Symantec.

   c. Do not use Altiris to uninstall Symantec from servers, or from workstations that have the Symantec System Center Console installed. They should be uninstalled manually instead.

Uninstall Previous Versions Manually

This method is labor intensive but straightforward. You will need to visit each workstation to perform the uninstall and reboot after each step. This is the preferred method for servers and the Symantec System Center Console workstation.

1. Do not uninstall from your previous Symantec server. You will perform that task last. However you can uninstall from other servers at this time.
2. Uninstall Symantec AntiVirus or Symantec Client Security.
3. Reboot the computer.

Exercise 7: Deploy the Symantec Endpoint Protection Client

It is important to perform a clean install of the SEP client. Make sure to uninstall all previous versions of Symantec before proceeding. We will demonstrate how to deploy the client through Altiris to workstations, laptops, and tablets. We will also demonstrate how to deploy the client manually to servers or workstations.

Deploy to Workstations with Altiris

This method is for workstations (i.e. desktops, laptops, tablets). Do not use this method for servers.

1. If you have installed any other software or Windows updates before deploying the SEP client, make sure to reboot the computers before proceeding, otherwise the SEP install will fail.

2. Create an Altiris job:

    a. Within the Altiris Deployment Console, create a new job called **Deploy Symantec Endpoint Protection**.

    b. In the new Deploy Symantec Endpoint Protection job, click **Add → Run Script**.

    c. In the Run Script window, select **Run this script**.

    d. In the Run this script field, type the following as one single line:
    `\\UNC-Share-Path-Here\SEP-Client-Install-Package-Here.exe`

    Note: *Replace UNC-Share-Path-Here with the actual share and path you used when exporting the SEP Client Installation packages. Replace SEP-Client-Install-Package-Here with the actual file name of the SEP Client Installation Package*.

    Additional Note*: If you have workstations running the 64-bit version of Windows, you will need to have two Altiris deployment jobs. One for the 32-bit clients and another for the 64-bit clients. Make sure to use the proper SEP Client Install Package for each.*

    e. Press **Enter** to start a new line, and type the following as one single line:
    `shutdown /r /f /t 0`

    f. Configure the job to run as the **ServiceAltiris** account (or whatever account you use for Altiris jobs).

3. Run the Altiris job:

    a. Make sure your desktop, laptop, and tablet computers are running and connected to the school network.

    b. Make sure all previous versions of Symantec have been uninstalled from them.

    c. Run the Deploy Symantec Endpoint Protection job against the desktops, laptops, and tablets in your school.

4. Verify the clients appear in the SEPM Console:

a. Wait for the Altiris job to complete.

b. Login to the SEPM Console.

c. Click on the **Clients** icon.

d. Click on your school district's name in the **View Clients** hierarchy list.

e. Click on the **Clients** tab.

f. Verify that all of the computers you just installed SEP onto appear in the list. You may have to wait a few minutes for all of them to appear. (Click the **Refresh** link in the top-right of the window if needed.)

Manually Deploy to Workstations or Servers

1. Login to the target server or workstation.
2. Verify that all previous versions of Symantec have been uninstalled.
3. Browse to the network share where you previously exported the SEP Client Installation packages.
4. Select the appropriate SEP Client Installation package for the computer you're on, which will either be:

    a. 32-bit server

    b. 64-bit server

    c. 32-bit workstation

5. Launch the installer. There will not be any windows or prompts, so you will have to wait for the SEP icon to appear in the taskbar's system tray.

    Note: *You can also launch Task Manager and look for a process with the same name as the install package (e.g. SEP_11.0.4202.75_WIN32BIT_servers.exe). As long as that process appears in the Task Manager, the installer is still running.*

6. Once the installer has finished, reboot the computer.
7. Login to the SEPM Console.
8. Click on the **Clients** icon.
9. Click on your school district's name in the **View Clients** hierarchy list.
10. Click on the **Clients** tab.
11. Verify that the computer you just installed SEP onto appears in the list. You may have to wait a few minutes for it to appear. (Click the **Refresh** link in the top-right of the window if needed.)

Exercise 8: Deploy to the Old Symantec Server

Wait until the rest of your district has been migrated to SEP before migrating your old Symantec server or your Symantec System Center Console workstation.

1. Ensure previous versions of Symantec have been uninstalled from ALL other computers in your school district.
2. Perform these steps on your old Symantec server (and if needed, from the workstation used for the Symantec System Center Console).
3. Uninstall the Symantec System Center Console.
4. Reboot the computer.
5. Uninstall previous version of Symantec AntiVirus or Symantec Client Security.
6. Reboot the computer.
7. Browse to the network share where you previously exported the SEP Client Installation packages.
8. Select the appropriate SEP Client Installation package for the computer you're on, which will either be:
    - 32-bit server
    - 64-bit server
    - 32-bit workstation
9. Launch the installer. There will not be any windows or prompts, so you will have to wait for the SEP icon to appear in the taskbar's system tray.

    Note: *You can also launch Task Manager and look for a process with the same name as the install package (e.g. SEP_11.0.4202.75_WIN32BIT_servers.exe). As long as that process appears in the Task Manager, the installer is still running.*
10. Once the installer has finished, reboot the computer.
11. Login to the SEPM Console.
12. Click on the Clients icon.
13. Click on your school district's name in the View Clients hierarchy list.
14. Click on the Clients tab.
15. Verify that the computer you just installed SEP onto appears in the list. You may have to wait a few minutes for it to appear. (Click the Refresh link in the top-right of the window if needed.)

Exercise 9: Including the SEP Client in an Image

The Symantec Endpoint Protection client uses a HardwareID to distinguish between different clients. This HardwareID values are located in the registry. You will have to remove these values from the imaging computer before creating the image.

Note: *In these instructions "Base Image PC" refers to the computer you're using to build your image. Sometimes this is refered to as the Base Computer, Base Image PC, Gold Computer, etc.*

1. You must delete the following registry values from the **Base Image PC** before creating the image:

    - **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink\HardwareID**
    - **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink\SySoftk**

    Warning: *in order for this to work, you must immediately grab the image without rebooting back into Windows.*

Exercise 10: Disable the Windows Firewall through Group Policy

Since the Symantec Endpoint Protection client includes a firewall component, you need to disable the built-in Windows Firewall so there are no conflicts. (You should never run two firewalls simultaneously.) The best way to disable the Windows Firewall is through a Group Policy Object (GPO).

Critical Warning: once the Windows Firewall is disabled, do not allow mobile devices to leave your school network until they have SEP installed, otherwise they will not be protected by a firewall.

Create a Domain-Level GPO to Disable the Windows Firewall

Warning: once you disable the Windows Firewall, the computers in your network will not be protected by a firewall until you install the Symantec Endpoint Protection client on them.

It's important that you do not allow mobile devices to leave your school network until you have installed the SEP client on them. Please plan ahead accordingly, and do not proceed with these steps until you are prepared to migrate your mobile devices to Symantec Endpoint Protection.

4. Open a remote desktop connection to a domain controller on your network.
5. Launch the **Group Policy Management** tool (located under Administrative Tools).
6. In the Group Policy Management window, in the left pane, expand until you see your school's domain listed. (*Make sure you create the policy at the domain level.*)
    a. For example: **Group Policy Mangement → Forest: Madison → Domains → Madison**.
7. Right-click on your school's domain and choose **Create and Link a GPO Here**.
8. Name the new GPO **Disable Windows Firewall** and click **OK**.
9. Right-click the newly created **Disable Windows Firewall** GPO and choose **Edit**.
10. Disable the Windows Firewall while connected to the school network:
    d. In the Group Policy Object Editor window, expand **Computer Configuration → Administrative Templates → Network → Network Connections → Windows Firewall → Domain Profile**.
    e. Double-click **Windows Firewall: Protect all network connections** and choose **Disabled**.
    f. Click **OK**.
11. Disable the Windows Firewall while connected to an off-site network:
    g. In the Group Policy Object Editor window, expand **Computer Configuration → Administrative Templates → Network → Network Connections → Windows Firewall → Standard Profile**.

h. Double-click **Windows Firewall: Protect all network connections** and choose **Disabled**.

i. Click **OK**.

12. Close the Group Policy Object Editor window.

13. In the Group Policy Management window, with the **Disable Windows Firewall** GPO selected, click the **Settings** tab.

14. Click the **Show All** link and verify the Windows Firewall is set to **Disabled** for both the Domain Profile and the Standard Profile.

15. Close the Group Policy Management window.

(If Needed) Modify Existing GPO's that Enable the Windows Firewall

If you currently have the Windows Firewall configured to turn on when laptops are not on the domain, you will need to modify those GPOs so the firewall always remains disabled. The following steps demonstrate how to do this for any school that has followed the Classroom Connections documentation. You may have to adapt these steps if you have setup your GPOs differently.

If you have not previously enabled the Windows Firewall through Group Policy, you can skip the rest of this section.

1. Open a remote desktop connection to a domain controller on your network.

2. Launch the **Group Policy Management** tool.

3. In the Group Policy Management window, in the left pane, expand until you see the **Tablets** OU.

4. Right-click on the **Tablet Computer Policy** and choose **Edit**.

Note: *If you did not follow the Classroom Connections instructions, or if you enabled the Windows Firewall in a different Group Policy Object than the one listed here, you'll have to locate and edit that policy instead.*

5. Disable the Windows Firewall while connected to the school network:

j. In the Group Policy Object Editor window, expand **Computer Configuration → Administrative Templates → Network → Network Connections → Windows Firewall → Domain Profile**.

k. Double-click **Windows Firewall: Protect all network connections** and choose **Disabled**.

l. Click **OK**.

6. Disable the Windows Firewall while connected to an off-site network:

m. In the Group Policy Object Editor window, expand **Computer Configuration → Administrative Templates → Network → Network Connections → Windows Firewall → Standard Profile**.

n. Double-click **Windows Firewall: Protect all network connections** and choose **Disabled**.

o. Click **OK**.

7. Close the Group Policy Object Editor window.

8. In the Group Policy Management window, with the **Tablet Computer Policy** GPO selected, click the **Settings** tab.

9. Click the **Show All** link and verify the Windows Firewall is set to **Disabled** for both the Domain Profile and the Standard Profile.

10. Close the Group Policy Management window.