



Network Antivirus Training

Setup, Configuration and Troubleshooting

Prepared by Joseph K. Magochi

DRAFT VERSION 2



African Virtual university
Université Virtuelle Africaine
Universidade Virtual Africana

Network Antivirus Training

Setup, Configuration & Troubleshooting

with Joseph K. Magochi

This course is available as an e-learning module.
Log on to the AVU Virtualclass

<http://virtualclass.avu.org>

HOW TO USE THIS MANUAL

This manual was compiled to be used as a reference for the African Virtual University ODeL Centers training.

It covers each topic that shall be discussed in class. This is not a step-by-step tutorial.

Our design ensures that each course is stimulating and customized yet covers the outlined objectives. The left page of your manual is designed for note-taking. That way, you won't have to switch between your notebook and a manual whenever you need to look up how to perform an operation.

Keys and commands that you need to press are displayed as icons such as E or Z.

Each topic starts on a new page, making things easy to find and follow. In addition, topics covering actual commands are divided into two parts, USAGE and MENU. Keyboard shortcuts will be included within TIP boxes or beside a keyboard icon while mouse shortcuts will always include the MOUSE icon.

The next page shows how a typical topic will be discussed and each part found in the manual

TABLE OF CONTENTS

HOW TO USE THIS MANUAL.....	3
INSTALLATION & CONFIGURATION OF SERVER COMPUTER-SYMANTEC ENDPOINT	5
INSTALLING AND CONFIGURING SYMANTEC ENDPOINT PROTECTION 11.0 FOR THE FIRST TIME.....	5
INSTRALLING ON CLIENT COMPUTERS	8
SYMANTEC ENDPOINT PROTECTION-WINDOWS XP	8
PREPARING COMPUTERS THAT RUN WINDOWS VISTA FOR REMOTE CLIENT DEPLOYMENT	10
CARRYING OUT UPDATES.....	12
PROCEDURES INCASE OF INFECTION.....	35
CONTAINMENT PLAN TO RESPOND TO A VIRUS INFECTION	35
TROUBLESHOOTING	38
TROUBLESHOOTING	38
TROUBLESHOOTING CONTENT DELIVERY TO THE SYMANTEC ENDPOINT PROTECTION CLIENT	38
SYMANTEC ENDPOINT PROTECTION CLIENT DEBUG LOGS	41
SYMANTEC ENDPOINT PROTECTION: TROUBLESHOOTING CLIENT/SERVER CONNECTIVITY	43

INSTALLATION & CONFIGURATION OF SERVER COMPUTER-SYMANTEC ENDPOINT

Introduction

This Section describes the procedures for installing Symantec Endpoint Protection 11.0 on a network that has no current Symantec Antivirus software.

SYMANTEC ENDPOINT PROTECTION

Symantec Endpoint Protection 11.0 combines Symantec Antivirus with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops and servers. It seamlessly integrates essential security technologies in a single agent and management console, increasing protection and helping lower total cost of ownership.

INSTALLING AND CONFIGURING SYMANTEC ENDPOINT PROTECTION 11.0 FOR THE FIRST TIME

About installing Symantec Endpoint Protection 11.0

Installing Symantec Endpoint Protection 11.0 includes the installation of three main components: the Symantec Endpoint Protection Manager, a dedicated database, and the Symantec Endpoint Protection clients. Installation begins with the installation and configuration of the Manager and database. Client installation occurs after the manager and database are installed and configured.

Installing and configuring Symantec Endpoint Protection Manager

This is a two-part procedure that installs the Symantec Endpoint Protection Manager (part 1), and configures the Symantec Endpoint Protection Manager and its database (part 2). You can accept all of the default settings for the manager installation. To configure the Symantec Endpoint Protection Manager database you must add at least one custom value, which is a password.

Notes:

- The Symantec Endpoint Protection client installation instructions follow this section.
- Internet Information Services (IIS) must be installed before installation of the Symantec Endpoint Protection Manager.

To install Symantec Endpoint Protection Manager (SEPM)

1. Insert the installation CD and start the installation.
2. In the installation panel, click **Install Symantec Endpoint Protection Manager**.
3. In the Welcome panel, click **next**.

4. In the License Agreement panel, check **I accept the terms in the license agreement**, and then click **next**.
5. In the Destination Folder panel, accept or change the installation folder.
6. Do one of the following:
 - To configure the Symantec Endpoint Protection Manager IIS (Internet Information Service) Web as the only Web server on this computer, check **Create a custom Web site**, and then click **Next**.
 - To let the Symantec Endpoint Protection Manager IIS Web server run with other Web servers on this computer, check **Use the default Web site**, and then click **next**.
7. In the Ready to install panel, click **Install**.
8. When the installation finishes and the Install Wizard Complete panel appears, click **Finish**. Wait for the Management Server Configuration Wizard panel to appear, which can take up to 15 additional seconds.

To configure Symantec Endpoint Protection Manager

1. In the Management Server Configuration Wizard panel, select a configuration type.
 - Note: If you choose the **Simple** configuration type, the password that is specified for the SEPM Administrator account is also the encryption password. If the Administrator password is reset post-installation, the encryption password does not change.
2. Click **Next**.
3. In the Site Type panel, check **Install my first Site**, and then click **next**.
4. In the Server Information panel, accept or change the default values for the following boxes, and then click **Next**:
 - Server Name
 - Server Port
 - Server Data Folder
5. In the Site Name panel, in the Site name box, enter your site name, and then click **next**.
6. In the Encryption Password panel, type a value in both boxes, and then click **next**. Document this password when you install Symantec Endpoint Protection in your production environment. You need it for disaster recovery purposes, and for adding optional Enforcer hardware.
7. In the Database Server Choice panel, check **Embedded Database**, and then click **next**.
8. In the Set User panel, in the Password boxes, type a password to use with the user name Admin to log on to the console, and then click **Next**.

NOTE: In MR3 and higher, the password box will not accept special characters. Previous versions would accept those characters but would not pass them, causing a 'failed to connect to database' error upon completion.

When the installation finishes, you have the option of deploying client software with the Migration and Deployment Wizard. Log on to the console with the user name and password that you entered here.

INSTALLING ON CLIENT COMPUTERS

SYMANTEC ENDPOINT PROTECTION-WINDOWS XP

Configuring and deploying client software on Windows XP

The Migration and Deployment Wizard lets you configure a client software package. The Push Deployment Wizard then optionally appears to let you deploy the client software package. If you do not use the Push Deployment Wizard at that time, you can start it manually by using ClientRemote.exe from the \tomcat\bin folder.

Note: This procedure assumes that you deploy client software to 32-bit computers and not to 64-bit computers. This procedure also has you select a folder in which to place installation files. You may want to create this folder before you start this procedure. Also, you need to authenticate with administrative credentials to the Windows Domain or Workgroup that contain the computers.

Deploying client software to computers that run firewalls, and that run Windows XP or Windows Vista, has special requirements. Firewalls must permit remote deployment over TCP port 139. Computers that are in workgroups and that run Windows XP must disable simple file sharing.

To configure client software

1. In the Management Server Configuration Wizard Finished panel, check **yes**, and then click **Finish**.
2. In the Welcome to the Migration and Deployment Wizard panel, click **next**.
3. In the would you like to do panel, check **Deploy the client**, and then click **Next**.
4. In the next unnamed panel, check **Specify the name of a new group that you wish to deploy clients to**, type a group name in the box, and then click **next**.
5. In the next panel, uncheck any client software that you do not want to install, and then click **next**.
6. In the next panel, check the options that you want for packages, files, and user interaction.
7. Click Browse, locate and select a folder in which to place the installation files, and then click **Open**.
8. Click **Next**.
9. In the next unnamed panel, check **yes**, and then click **Finish**.

Do not check Launch Administrator Console. It can take up to 5 minutes to create and export the installation package for your group before the Push Deployment Wizard appears.

To deploy the client software with the Push Deployment Wizard

1. In the Push Deployment Wizard panel, under Available Computers, expand the trees and select the computers on which to install the client software, and then click **Add**. If you distribute the client to the same computer you work on and Windows Firewall has not been configured to handle Java, it may block this function and pop up a window that asks you to configure it. This window may appear underneath the Push Deployment Wizard, so you may not be able to see it. If the Push Deployment Wizard appears to stop responding, move it to the side to see whether a Windows Firewall window is hidden beneath it.
2. In the Remote Client Authentication dialog box, type a user name and password that can authenticate to the Windows Domain or Workgroup that contains the computers, and then click **OK**.
3. When you have selected all of the computers and they appear in the right pane, click **Finish**.
4. When installation completes, click **done**.

Logging on to and locating your group in the console

your first activity is to log on to the console and locate your group.

Logging on to the management console

the management console lets you manage clients.

To log on to the management console

1. Click **Start> Programs> Symantec Endpoint Protection Manager> Symantec Endpoint Protection Manager Console**.
2. In the Symantec Endpoint Protection Manager Logon prompt, in the User Name box, type **admin**.
3. In the Password box, type the admin password that you created during installation, and then click **Log on**.

About locating your group in the console

After you log on, you should locate the group that you created during installation. Then verify that the client computers to which you deployed software appear in that group.

Enabling Symantec Network Access Control

If you purchased Symantec Endpoint Protection with Symantec Network Access Control, follow these additional steps to enable Symantec Network Access Control.

To enable Symantec Network Access Control

1. If Symantec Endpoint Protection Manager Console is open, close it.
2. Insert the Symantec Network Access Control CD.

3. In the installation panel, click **Install Symantec Network Access Control**.
4. Click **Install Symantec Endpoint Protection Manager**.
5. On the Management Server Upgrade dialog, click **next**.
6. Click **Continue**.
7. When the Server Upgrade Status log shows Upgrade Succeeded, click **next**.
8. Click **Finish**.
9. Log on to the Symantec Endpoint Protection Manager console.
10. On the Policies tab, click **Host Integrity**.
11. In the right pane, click **Host Integrity Policy**.
12. Under Tasks, click **Assign the Policy**.
13. In the Assign Host Integrity Policy window, check the group to which you want to assign the policy.
14. Click **Assign**, and then click **yes** to confirm the change.

Symantec Network Access Control is now enabled in Symantec Endpoint Protection Manager and on the clients in the group that you created.

PREPARING COMPUTERS THAT RUN WINDOWS VISTA FOR REMOTE CLIENT DEPLOYMENT

Symantec Endpoint Protection 11.0 will be deployed to computers that run Microsoft Windows Vista. What preparations must be made on the computers before the client software can be deployed?

Note: Windows Vista provides a highly customizable user interface. The procedures in this section are based on the Windows Classic user interface that can be set for Microsoft Windows Vista.

The Microsoft Windows Vista feature, "User Account Control" (UAC) blocks local administrative accounts from remotely accessing remote administrative shares such as "C\$" and "Admin\$." To use the "Push Deployment Wizard Tool" in this scenario, use a "Domain Administrative" account if the target client computer is part of an "Active Directory" domain. Remote client installation also requires elevated privileges to install.

Administrators of a workgroup will have to decide the best approach for UAC security in their environment. The UAC feature defaults to preventing access to administrative shares through the network for local administrative users in a workgroup environment. Please refer to the UAC

documentation that Microsoft offers on their TechNet and Support websites for further information or workarounds on administration of this feature.

Title: Getting Started with User Account Control on Windows Vista

URL: <http://technet.microsoft.com/en-us/library/cc507861.aspx>

Title: Error message when you try to access an administrative share on a Windows Vista-based computer from another Windows Vista-based computer that is a member of a workgroup: "Logon unsuccessful: Windows is unable to log you on"

URL: <http://support.microsoft.com/kb/947232>

To enable remote client software deployment on the computers that run Microsoft Windows Vista, the following must be completed on each client computer:

- Disable the "File Sharing Wizard."
- Enable **Network Discovery** by using the "Network and Sharing center."
- Ensure you are using an Administrative User account.
- Verify that the account has "elevated" privileges.

To disable the "File Sharing Wizard" follow the steps below:

1. Click **Start > Computer**.
2. In the Computer window, click **Organize > Folder and Search Options**.
3. Under the **View** tab, in the **Advanced Settings** section, uncheck **Use Sharing Wizard (Recommended)**.
4. Click **OK**.

If Using Windows Vista in Classic View follow the steps below to disable the "File Sharing Wizard"

1. Display the drives located on the computer.
2. In the "My Computer" window, click **Tools> Folder Options**.
3. Select **View> Advanced Settings**, uncheck **Use Sharing Wizard (Recommended)**
4. Click **OK**.

To enable network discovery

1. Display the computers in the network.
2. In the "Network" window, click **Network and Sharing Center**.
3. Select **Sharing and Discovery**.

4. Click **Network Discovery**.
5. Click **Turn on Network Discovery**
6. Click **Apply**.

Ensure you are using an Administrative User account.

To verify that you have elevated privileges

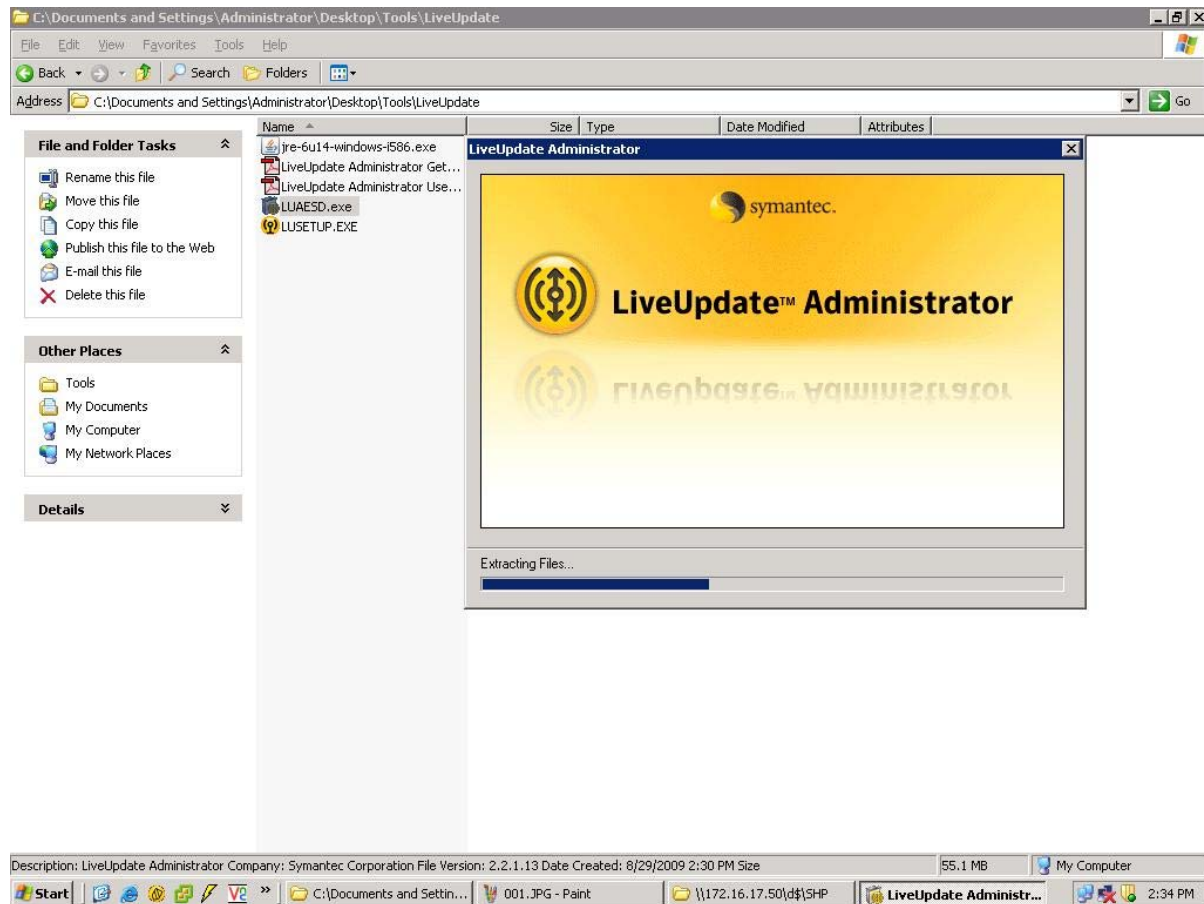
1. Click **Start > Run**.
2. Type \\<target computer name>\C\$.

If you can access and display the "C\$" remote administrative share, then your privileges are elevated. If you cannot access and display this share, you must authenticate with an account that has the required privileges.

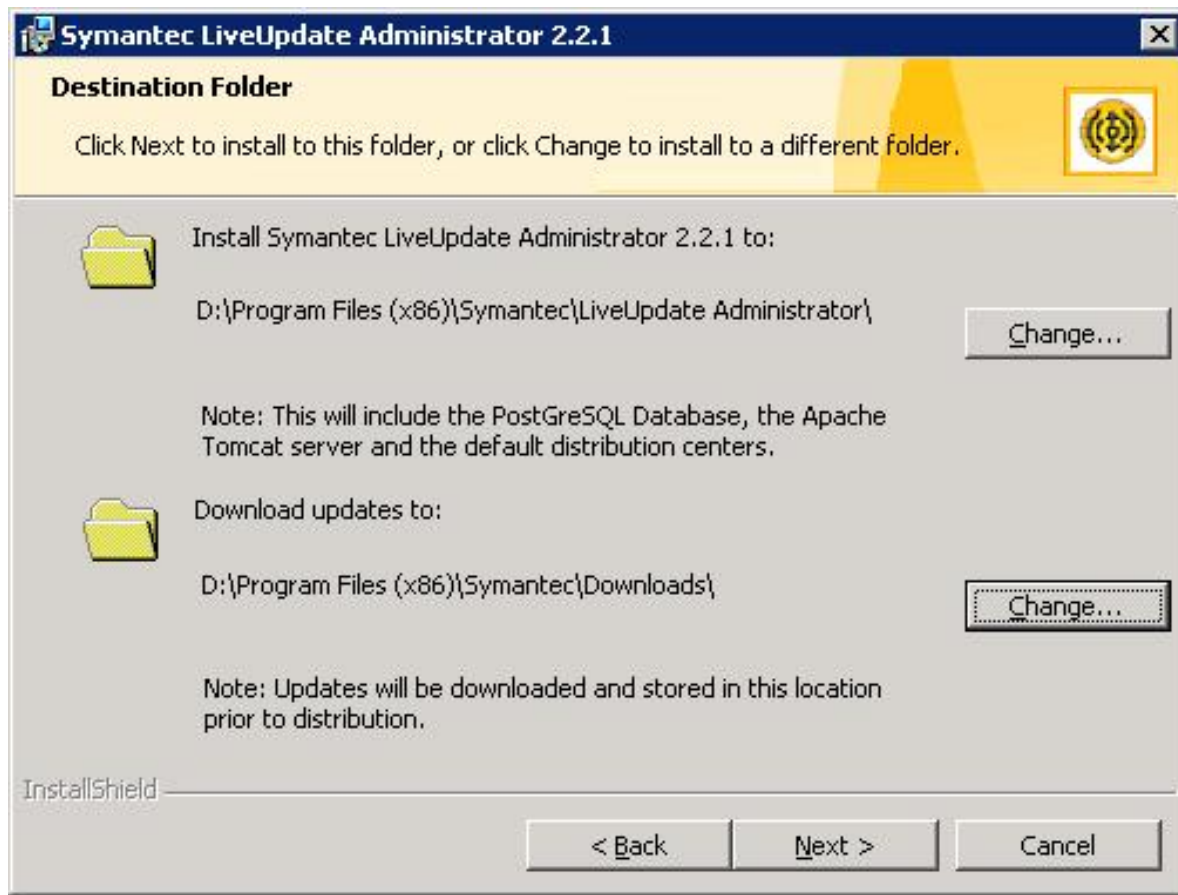
CARRYING OUT UPDATES

The Symantec Live Update Administrator is an enterprise Web application that allows you to manage Symantec updates on multiple internal Central Live Update servers, called Distribution Centers.

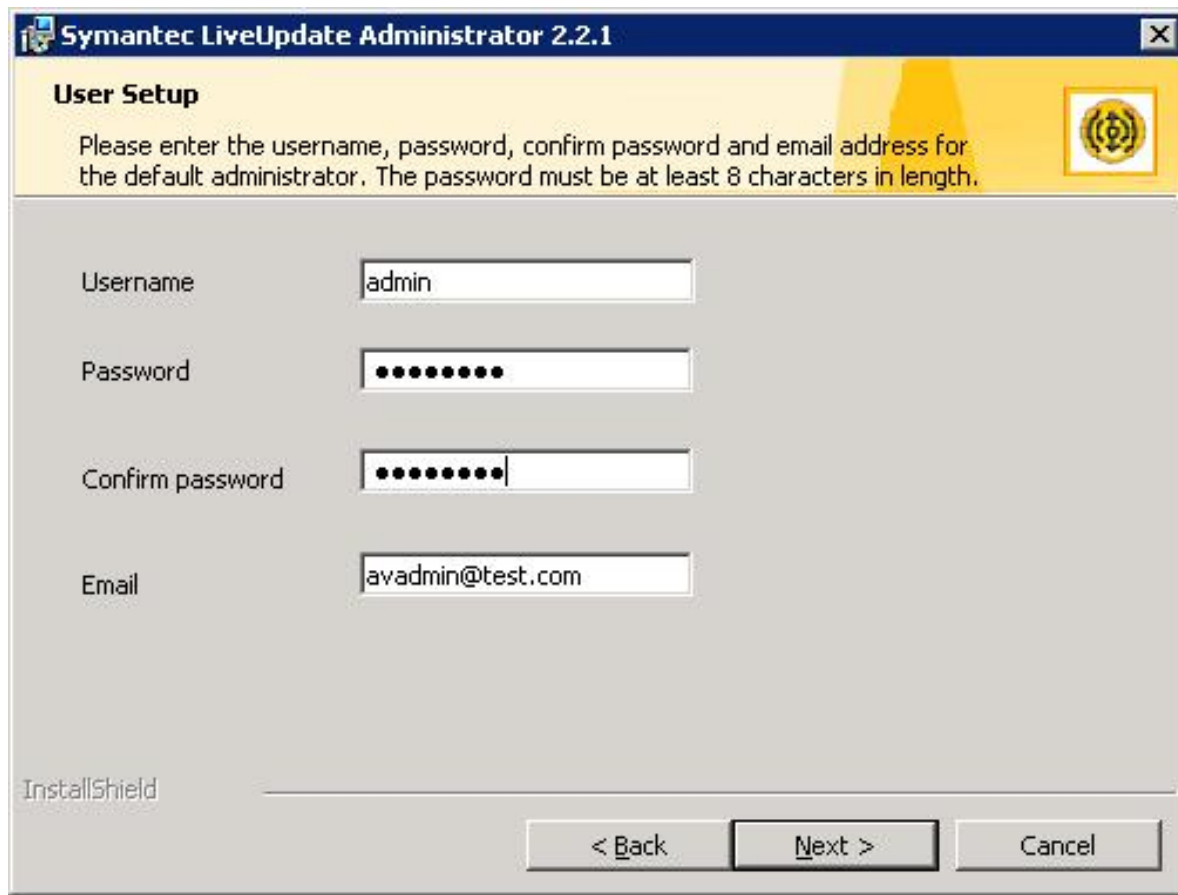
1. Run the live update administrator package from the 2nd CD (Before that install latest version of jre)



2. Choose the folders for LUA and Update download (Note: Select a drive which is having sufficient free space)



3. Give the user account information and finish the installation.



The image shows a screenshot of the Symantec LiveUpdate Administrator 2.2.1 User Setup window. The window has a title bar with the text "Symantec LiveUpdate Administrator 2.2.1" and a close button. Below the title bar is a yellow header area with the text "User Setup" and a small icon of a shield with a dollar sign. The main area of the window is gray and contains four input fields: "Username" with the text "admin", "Password" with eight dots, "Confirm password" with eight dots, and "Email" with the text "avadmin@test.com". At the bottom left of the window is the text "InstallShield". At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

Symantec LiveUpdate Administrator 2.2.1

User Setup

Please enter the username, password, confirm password and email address for the default administrator. The password must be at least 8 characters in length.

Username: admin

Password:

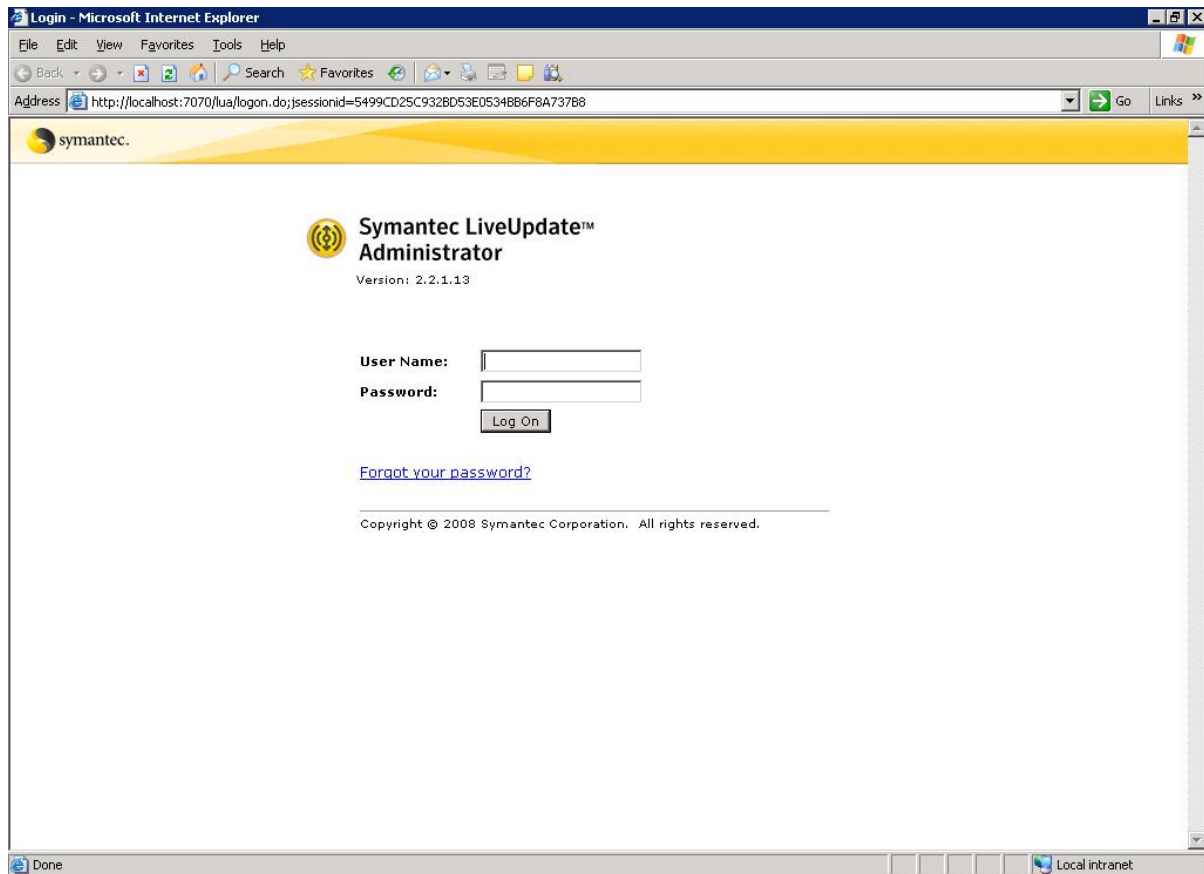
Confirm password:

Email: avadmin@test.com

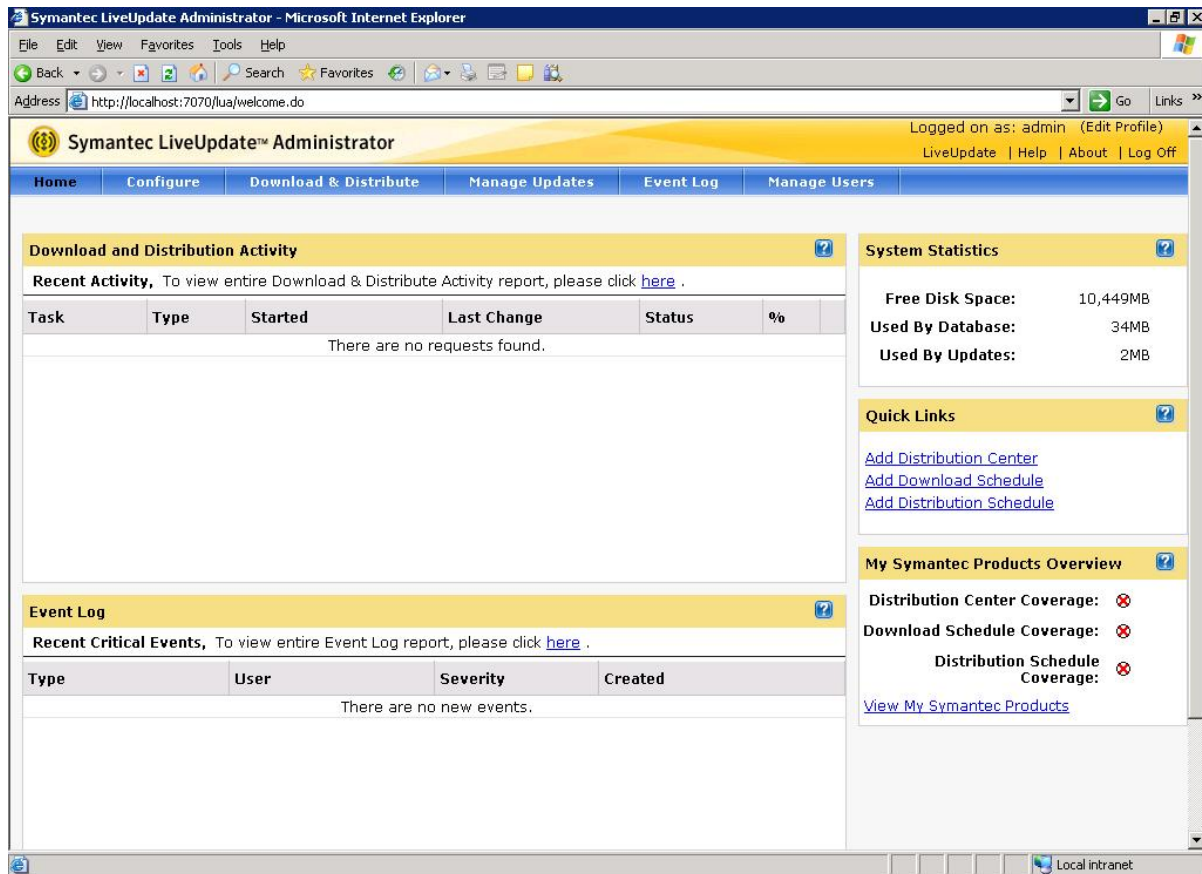
InstallShield

< Back Next > Cancel

4. After installation go to Start---> Programs---> Symantec Live update Administrator--->Live update administrator. You will get a login prompt.



5. After logging into LUA you will get a home page. Home page has lot of information like recent activities, Current critical events, System statistics, etc.



6. By default, updates are downloaded from one of the Symantec Live Update servers. You have to edit this setting to add proxy. (If you are not using proxy go to step 10 (Add proxy information for internet explorer also))

Source Servers

Select All	Name	URL	Status
<input checked="" type="checkbox"/>	Symantec LiveUpdate	http://liveupdate.symantedliveupdate.com:80/	Unreachable

1 - 1 of 1

Symantec LiveUpdate

URL: http://liveupdate.symantedliveupdate.com:80/
 Login:
 Proxy URL: Not used
 Proxy login:
 Status: Unreachable
 Last connection: Never

Failover Servers (ordered list)

Name	URL	Status	Last Connection
Symantec LiveUpdate - HTTP Failover Server	http://liveupdate.symantec.com:80/	Unreachable	Never
Symantec LiveUpdate - FTP Failover Server	ftp://update.symantec.com:21/opt/content/onramp	Unreachable	Never

7. Add the proxy IP address, username password.

Configure - Source Server - Edit Source Server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links >>

Address http://localhost:7070/luu/source-server.do

Home Configure Download & Distribute Manage Updates Event Log Manage Users

My Symantec Products Source Servers Distribution Centers Client Settings Preferences

Source Server Tasks

[Add Source Server](#)
[Add Failover Server](#)
[Reset to defaults](#)

Source servers » Source server

Edit Source Server

Source server name: Symantec LiveUpdate

Priority (from 1 to 5): 1

Hostname/IP address: liveupdate.symantecliveupdate.com

Root directory:

Login id:

Password:

Confirm password:

Protocol: ☒ HTTP ☐ FTP ☐ HTTPS ☐ UNC

Port (if other than default): 80

Use proxy: ☒

Proxy hostname/IP address: 172.16.222.196

Proxy login id: luadmin

Proxy password:

Confirm proxy password:

Local intranet

8. Configure proxy port. You have to set proxy information for failover servers also.

Configure - Source Server - Edit Source Server - Microsoft Internet Explorer

Address <http://localhost:7070/ua/source-server.do?dispatch=back> Go Links >>

Use proxy: ☒

Proxy hostname/IP address:

Proxy login id:

Proxy password:

Confirm proxy password:

Proxy protocol: ☒ HTTP ☐ FTP ☐ HTTPS ☐ UNC

Port (if other than default):

Failover Servers:

Name	URL	Status
Symantec LiveUpdate - HTTP Fail ...	http://liveupdate.symantec.com:80/	Unreachable
Symantec LiveUpdate - FTP Fail ...	ftp://update.symantec.com:21/opt/content ...	Unreachable

Buttons: Move Up, Move Down, Add, Edit, Copy, Delete, Primary, Test

Buttons: OK, Test, Cancel, Apply

symantec.

Done Local intranet

9. Add proxy IP, username, password, port and test the connectivity by clicking "Test" button. If everything is working fine you will get a message "Connection to Symantec Live Update was successful". Save the settings by clicking "OK".

LiveUpdate Administrator - Edit Failover Server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links >>

Address <http://localhost:7070/luafailoverserver.do>

[Add Source Server](#)
[Add Failover Server](#)
[Reset to defaults](#)

Edit Failover Server

Source Server: Symantec LiveUpdate

Failover server name: Symantec LiveUpdate - HTTP Failover Server

Hostname/IP address: liveupdate.symantec.com

Root directory:

Login id:

Password:

Confirm password:

Protocol: ☒ HTTP ☐ FTP ☐ HTTPS ☐ UNC

Port (if other than default): 80

Use proxy: ☒

Proxy hostname/IP address: 172.16.222.196

Proxy login id: luadmin

Proxy password:

Confirm proxy password:

Proxy protocol: ☒ HTTP ☐ FTP ☐ HTTPS ☐ UNC

Port (if other than default): 3128

OK Test Cancel

Done Local intranet

10. If all the parameters are configured correctly, you will get a "Ready" message in status column of "Source Server" section.

Configure - Source Servers - Microsoft Internet Explorer

Address: http://localhost:7070/luu/source-servers.do

Symantec LiveUpdate™ Administrator

Logged on as: admin (Edit Profile)

LiveUpdate | Help | About | Log Off

Home | Configure | Download & Distribute | Manage Updates | Event Log | Manage Users

My Symantec Products | Source Servers | Distribution Centers | Client Settings | Preferences

Source Server Tasks

- [Add Source Server](#)
- [Add Failover Server](#)
- [Reset to defaults](#)

Source server Symantec LiveUpdate configuration is saved.

Source Servers

Add Edit Copy Delete

Select All	Name	URL	Status
<input type="checkbox"/>	Symantec LiveUpdate	http://liveupdate.symantecdiveupdate.com:80/	Ready

1 - 1 of 1

Symantec LiveUpdate

URL: http://liveupdate.symantecdiveupdate.com:80/

Login:

Proxy URL: http://172.16.222.196:3128

Proxy login:

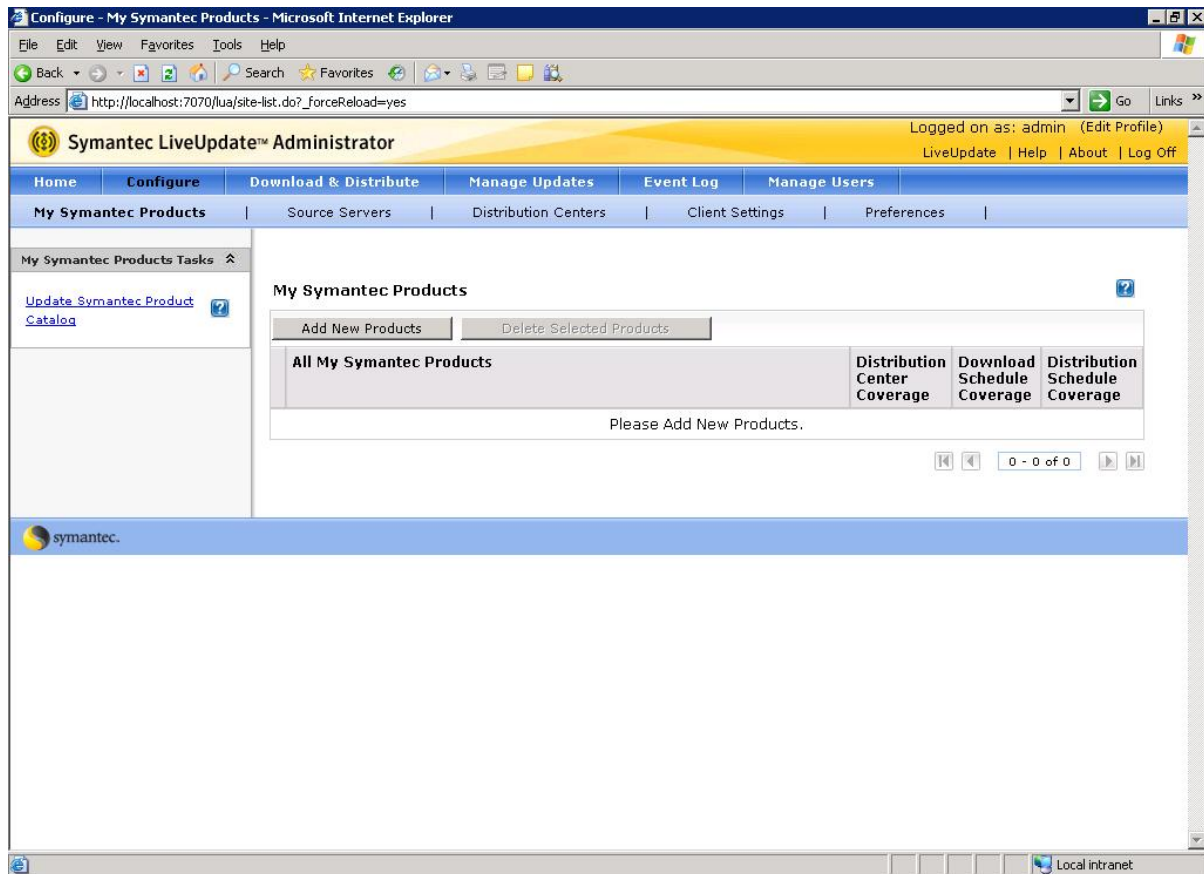
Status: Ready

Last connection: Never

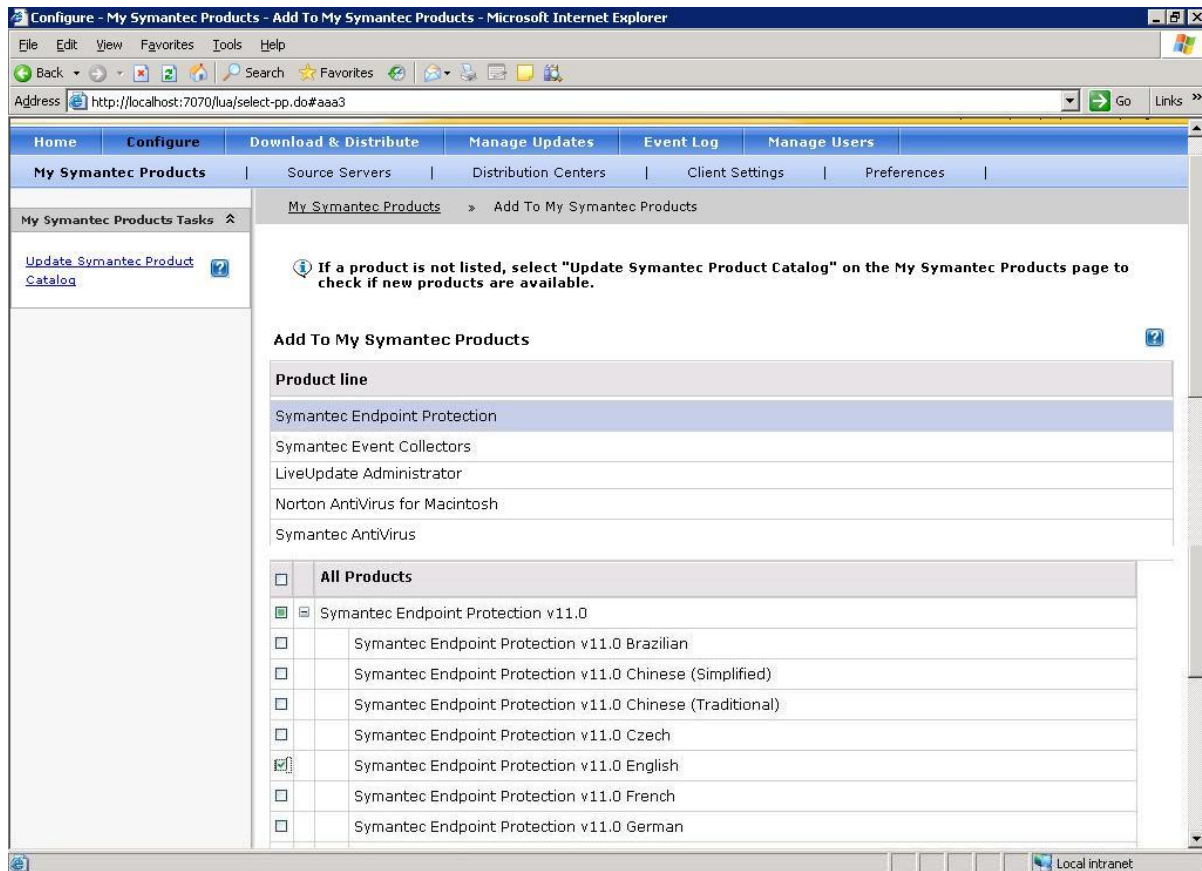
Failover Servers (ordered list)

Name	URL	Status	Last Connection
Symantec LiveUpdate - HTTP Failover Server	http://liveupdate.symantec.com:80/	Ready	Never

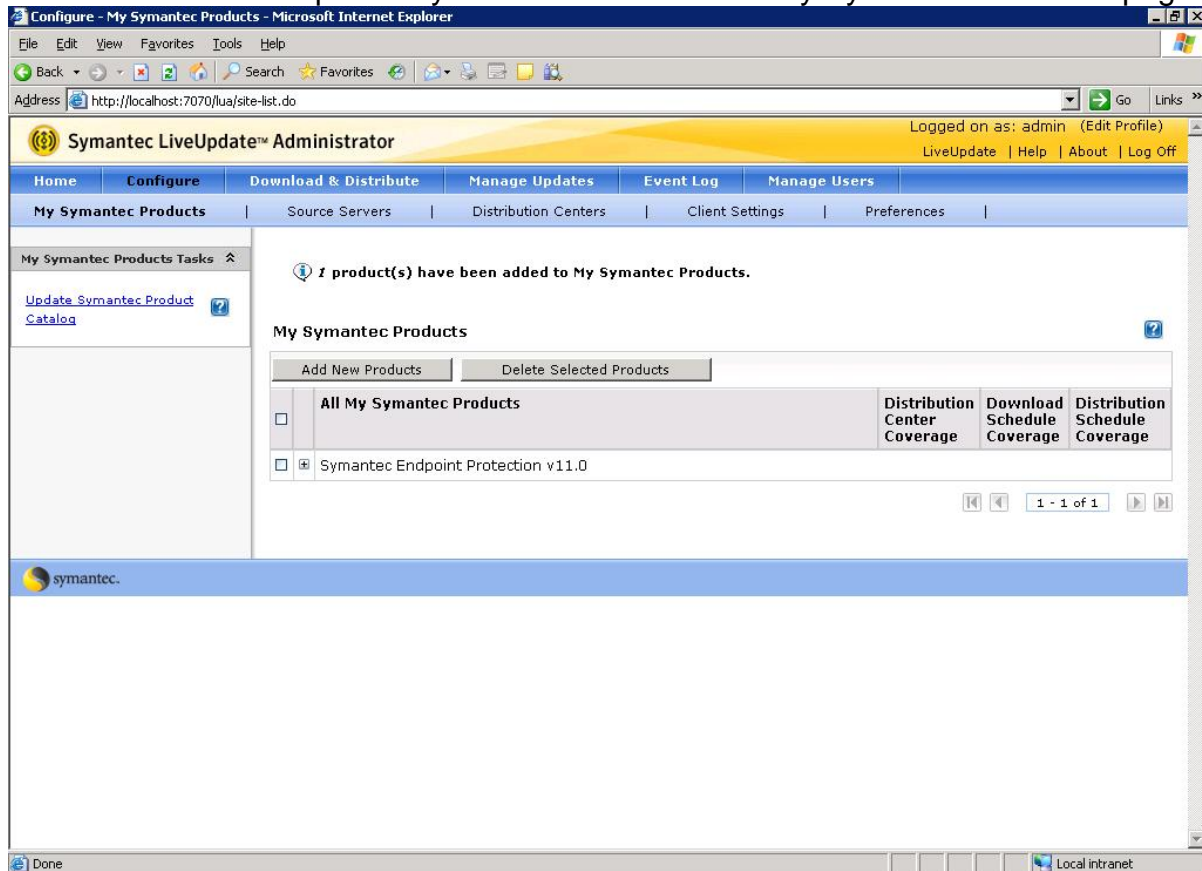
11. Now you can add a product to include in you distribution. Click on "Add new Products"



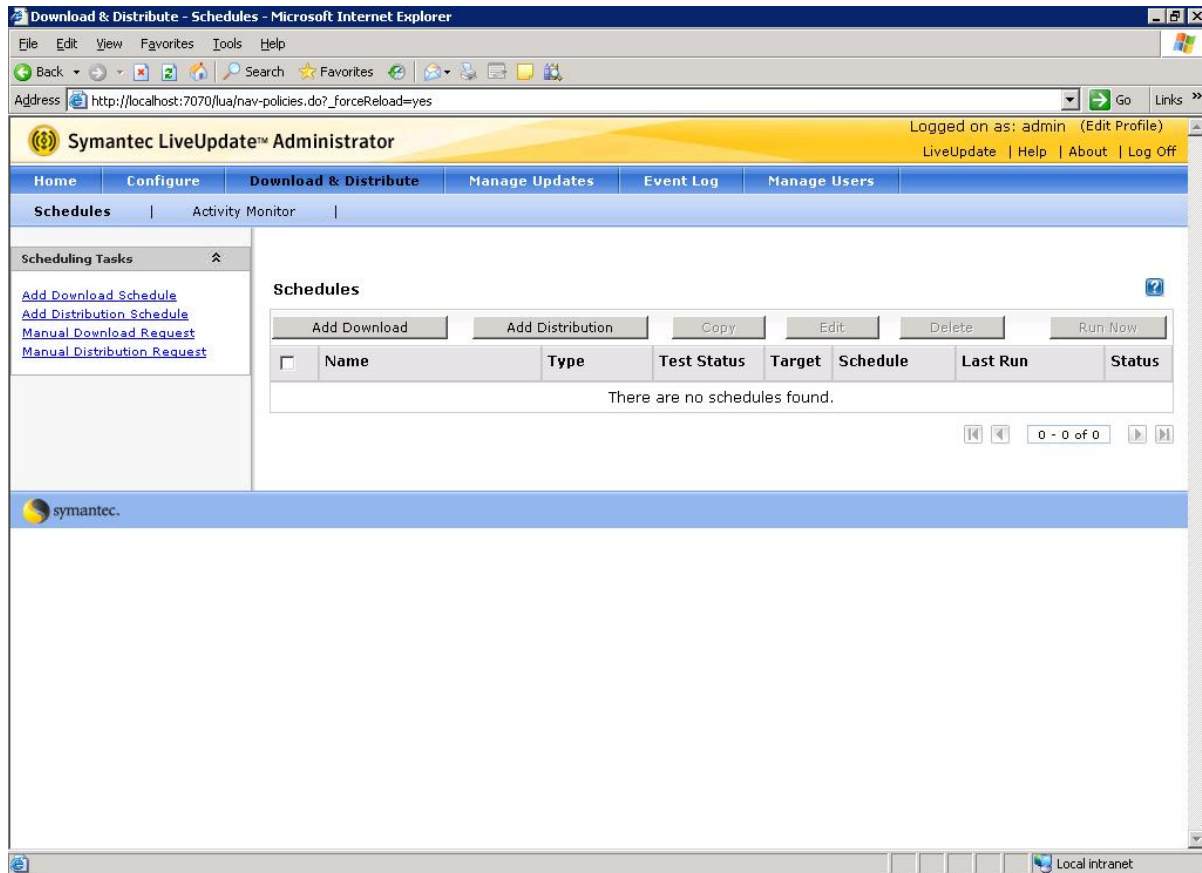
12. You can add any product from the list. I have added only SEP V11 English.



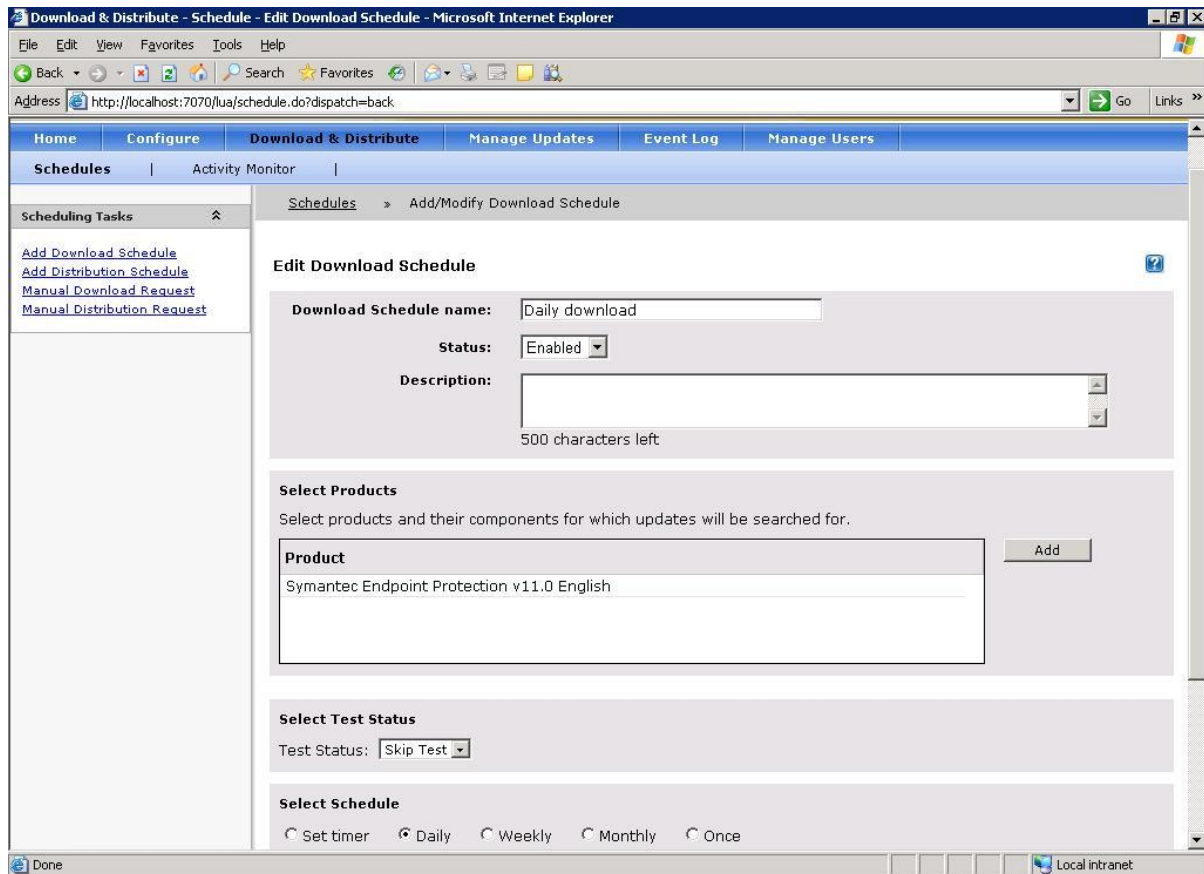
13. Make sure all the product you added are listed in "My Symantec Products" page.



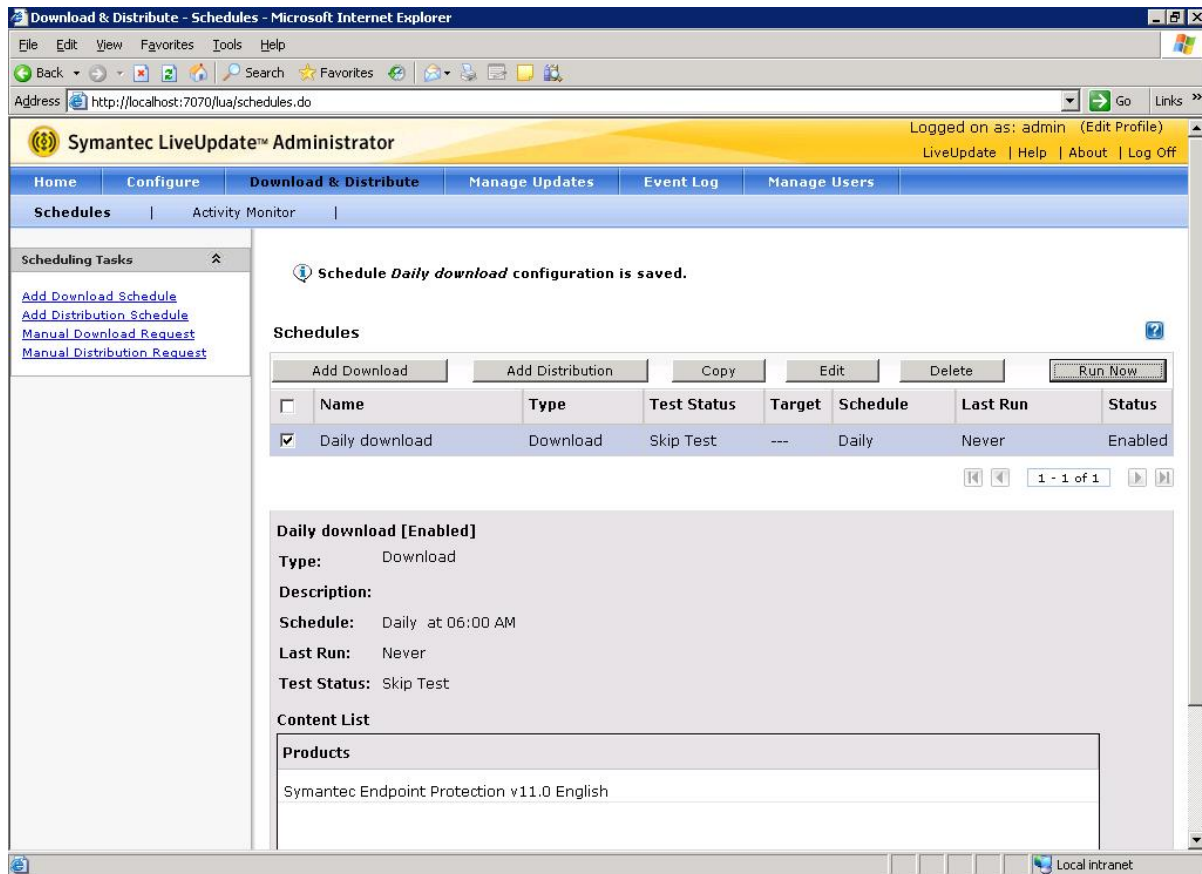
14. Now you have to add Schedules for definition download from Symantec site. Click on “Add Download”



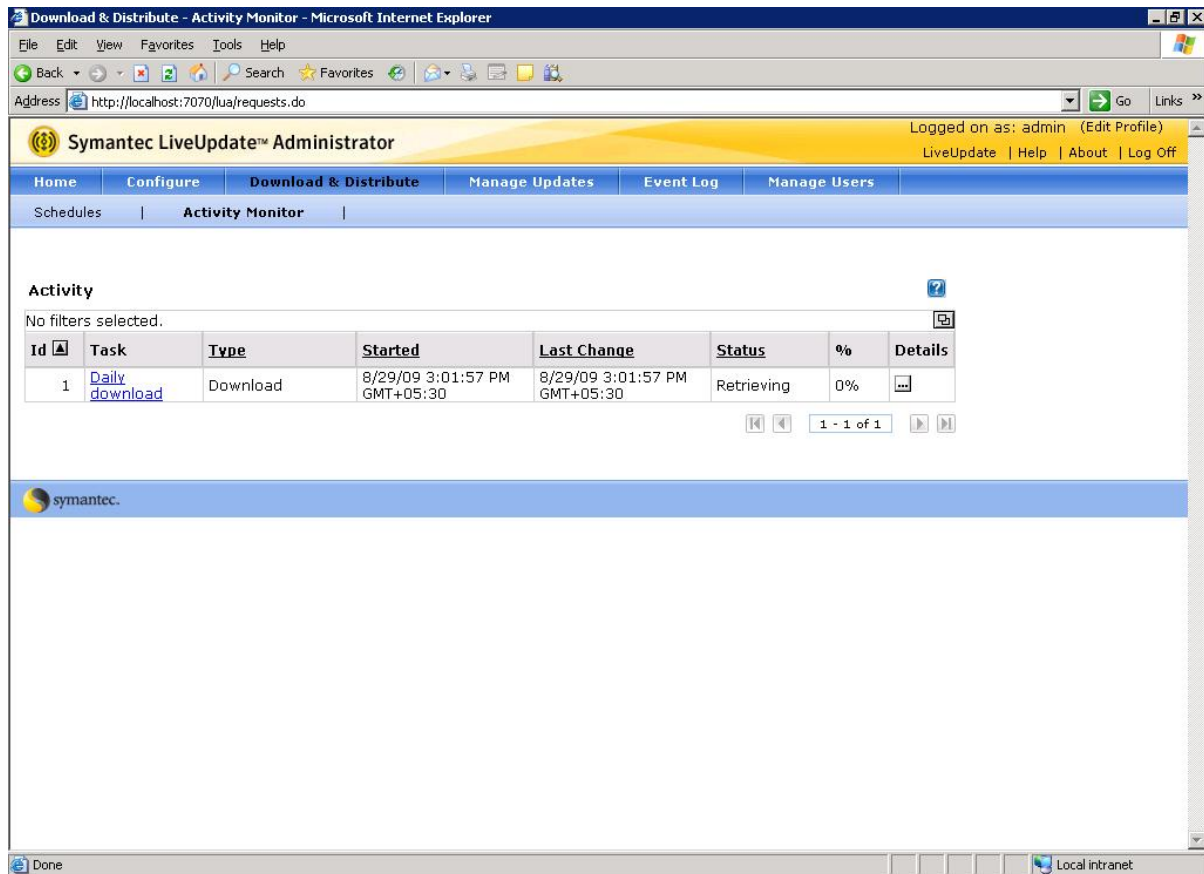
15. Give a Schedule name, add the products and set schedule time.



16. Once you add schedule u can run it on demand by clicking on "Run Now" button.



17. Activities of Schedules can be monitored from "Activity Monitor" tab.



18. If you click on "Details" you will get more information about the request.

The screenshot shows the Symantec LiveUpdate Administrator web interface in a Microsoft Internet Explorer browser window. The address bar shows the URL: http://localhost:7070/lua/view-request.do?requestId=1. The user is logged in as 'admin'. The interface has a navigation bar with tabs: Home, Configure, Download & Distribute (selected), Manage Updates, Event Log, and Manage Users. Under 'Download & Distribute', there are sub-tabs: Schedules and Activity Monitor (selected). The 'Request Details' section shows the following information:

- Request Status:** Retrieving updates
- Request started by:** admin
- Description:** [Daily download](#)
- Request type:** Download
- Test Requirement:** Skip Test
- Completed:** [Progress bar]
- Total size of files in Request:** 1,026,623 KB
- Request started at:** 8/29/09 3:01:57 PM GMT+05:30
- Request elapsed time:** 50 seconds

Below this information is a table showing the details of the files being downloaded:

Status	Server	Product	Component	File Name
Downloading	Symantec LiveUpdate	Symantec Endpoint Protection v11.0 English	Decomposer 1.0.0	1203515784jtun_the_...
Downloading	Symantec LiveUpdate	Symantec Endpoint Protection v11.0 English	SEP PTS Content 6.1.0	1223494762jtun_the_...
Downloading	Symantec LiveUpdate	Symantec Endpoint Protection v11.0 English	SEP PTS Engine Win32 6.1.0	1223493964jtun_the_...
Downloading	Symantec LiveUpdate	Symantec Endpoint Protection v11.0 English	SEP PTS Engine Win64 6.1.0	1223494646jtun_the_...
Downloading	Symantec LiveUpdate	Symantec Endpoint Protection v11.0 English	SESC IPS Signatures Win32 11.0	1251222158jtun_sesc...

19. Once the download of definition is complete, u can distribute these updates to Distribution centers. By default there will be two distribution centers. You have to edit them to add products.

Symantec LiveUpdate™ Administrator

Logged on as: admin (Edit Profile)

LiveUpdate | Help | About | Log Off

Configure | Distribution Centers

Distribution Centers

Add | Edit | Copy | Delete

Select All	Name	Type
<input type="checkbox"/>	Default Production Distribution Center	Production
<input type="checkbox"/>	Default Testing Distribution Center	Testing

1 - 2 of 2

Default Production Distribution Center [Server View](#)

Description: This is the default production distribution center installed by the Symantec LiveUpdate Administrator application.

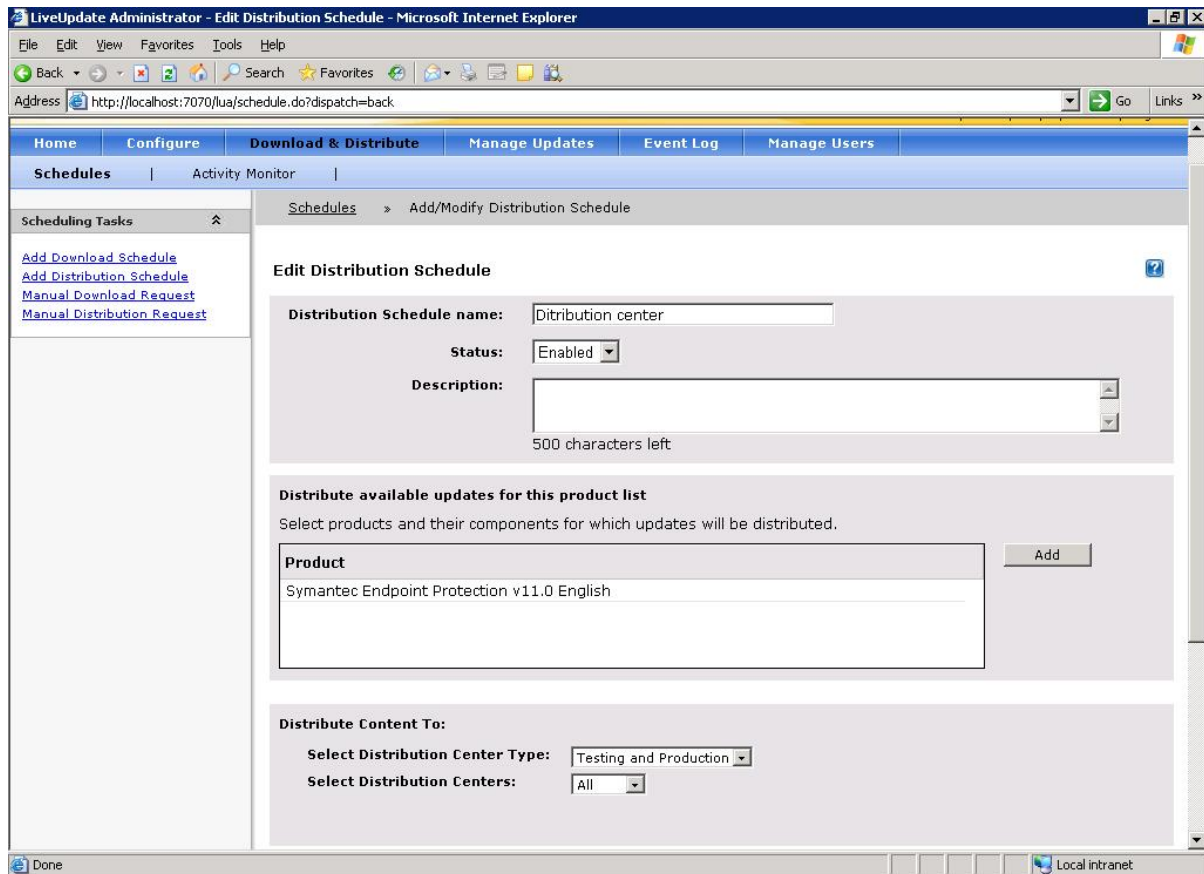
Type: Production

Location List

Name	URL	Status	Last Connection
Default Production Distribution Center	http://CANARA-SEPM:7070/clu-prod	Ready	Never

Note: Max 20 Locations. for complete list of available locations, visit details page.

20. Once you do the modification in Distribution centers configuration, you have to add a schedule for Distribution. Click "New Distribution" button under "Schedules" tab. Give a name, add the product and set the time for schedule.



21. You can run the schedule on demand by clicking on "Run Now".

Symantec LiveUpdate™ Administrator

Logged on as: admin (Edit Profile)
LiveUpdate | Help | About | Log Off

Schedules | Activity Monitor

Scheduling Tasks

- [Add Download Schedule](#)
- [Add Distribution Schedule](#)
- [Manual Download Request](#)
- [Manual Distribution Request](#)

Schedules

<input type="checkbox"/>	Name	Type	Test Status	Target	Schedule	Last Run	Status
<input type="checkbox"/>	Daily download	Download	Skip Test	---	Daily	8/29/09 2:59:36 PM GMT+05:30	Enabled
<input checked="" type="checkbox"/>	Distribution schedule	Distribution		All	Daily	Never	Enabled

1 - 2 of 2

Distribution schedule [Enabled]

Type: Distribution

Description:

Schedule: Daily at 06:00 AM

Last Run: Never

Content List

Products

Symantec Endpoint Protection v11.0 English

22. All event logs will be available under "Event Log" tab.

Event Log - Microsoft Internet Explorer

Address: http://localhost:7070/lu/nav-reports.do?_forceReload=yes

Symantec LiveUpdate™ Administrator

Logged on as: admin (Edit Profile)

LiveUpdate | Help | About | Log Off

Home | Configure | Download & Distribute | Manage Updates | **Event Log** | Manage Users

Event Log

No filters selected. [Select Filter:](#)

Delete

Select All	Created	Event Type	Severity	User	Description
<input type="checkbox"/>	8/29/09 3:09:48 PM GMT+05:30	Schedule	informational	admin	Successfully saved schedule information for <i>Distribution schedule</i> .
<input type="checkbox"/>	8/29/09 3:07:10 PM GMT+05:30	Server	informational	admin	Successfully updated server group information for <i>Default Production Distribution Center</i> .
<input type="checkbox"/>	8/29/09 3:06:10 PM GMT+05:30	Server	informational	admin	Successfully updated server group information for <i>Default Production Distribution Center</i> .
<input type="checkbox"/>	8/29/09 3:01:57 PM GMT+05:30	Download	informational	admin	Started download of content for request id 1 started by user <i>admin</i> .
<input type="checkbox"/>	8/29/09 2:59:36 PM GMT+05:30	Schedule	informational	admin	Download schedule <i>Daily download</i> started.
<input type="checkbox"/>	8/29/09 2:59:26 PM GMT+05:30	Login/Log Off	informational	admin	User <i>admin</i> logged in successfully.
<input type="checkbox"/>	8/29/09 2:56:39 PM GMT+05:30	Schedule	informational	admin	Download schedule <i>Daily download</i> started.
<input type="checkbox"/>	8/29/09 2:56:06 PM GMT+05:30	Schedule	informational	admin	Successfully saved schedule information for <i>Daily download</i> .
<input type="checkbox"/>	8/29/09 2:45:33 PM GMT+05:30	Server	informational	admin	Successfully updated server information for <i>Symantec LiveUpdate</i> .
<input type="checkbox"/>	8/29/09 2:45:05 PM GMT+05:30	Server	informational	admin	Successfully updated server information for <i>Symantec LiveUpdate</i> .
<input type="checkbox"/>	8/29/09 2:45:00 PM GMT+05:30	Server	informational	admin	Successfully updated server information for <i>Symantec LiveUpdate</i> .
<input type="checkbox"/>	8/29/09 2:39:28 PM GMT+05:30	Login/Log Off	informational	admin	User <i>admin</i> logged in successfully.

1 - 12 of 12

Local intranet

23. You can use "Client Settings" tab to export the client settings host file, Settings. Hosts. Live Update, used by Windows Live Update clients to download updates from the Distribution Center, or export a liveupdt.hst file, used by Java Live Update clients.

Export Client Settings - Microsoft Internet Explorer

Address: http://localhost:7070/lu/generate-host-file.do?_forceReload=yes

Symantec LiveUpdate™ Administrator Logged on as: admin (Edit Profile)

LiveUpdate | Help | About | Log Off

Home | Configure | Download & Distribute | Manage Updates | Event Log | Manage Users

My Symantec Products | Source Servers | Distribution Centers | **Client Settings** | Preferences

Export Client Settings

[Create New Client Settings](#)
[Reset to defaults](#)

Client Settings

To export Windows LiveUpdate client settings, select the corresponding row and click Export Windows Settings.
To export Java LiveUpdate client settings, click Export Java Settings.

Export Windows Settings | Export Java Settings | Add | Edit | Copy | Delete

Select	Name	Description
<input type="checkbox"/>	Default client settings for production environment	These are the Default client settings for connecting LiveUpdate clients to the Default Production Distribution Center.
<input type="checkbox"/>	Default client settings for testing environment	These are the Default client settings for connecting LiveUpdate clients to the Default Testing Distribution Center.

1 - 2 of 2

Name: Default client settings for production environment

Description: These are the Default client settings for connecting LiveUpdate clients to the Default Production Distribution Center.

Server List

Name	Protocol	URL
Default Production Distribution Center	HTTP	http://CANARA-SEPM:7070/du-prod
Symantec LiveUpdate	HTTP	http://liveupdate.symantecliveupdate.com:80/
Symantec LiveUpdate - HTTP Failover Server	HTTP	http://liveupdate.symantec.com:80/

You then copy the exported file to the \Program Files\Symantec\LiveUpdate directory on the Live Update client computers. When the Live Update client runs, it will use the host file for information on where to download updates.

PROCEDURES INCASE OF INFECTION

CONTAINMENT PLAN TO RESPOND TO A VIRUS INFECTION

Issue:

You need a plan of action in the event of a virus infection, such as a computer worm.

Solution:

As users begin reporting virus symptoms spreading through your network, check your Antivirus logs for information. If you can identify the infection, then use the [Symantec Security Response Virus Encyclopedia](#) to gather information on viral characteristics, payload, and removal instructions.

If you cannot identify the infection, then follow this procedure.

To identify the infection

1. Browse to <http://securityresponse.symantec.com> and look at the Latest Virus Threats and Security Advisories areas for news.
2. Ensure that the latest Antivirus definitions have been applied to the infected computers.
3. If scanning with the latest virus definitions does not identify the infection, and if you cannot find relevant information at <http://securityresponse.symantec.com>, then submit any suspicious files to Symantec Security Response for analysis.

Note: You may want to designate one computer that is connected to the Internet, but not networked or shared with any other systems on your LAN, to download updated virus definitions or submit suspect files to Symantec Security Response.

4. Regularly visit <http://securityresponse.symantec.com> for updates.

When responding to infection by computer worms, it sometimes becomes critical to isolate the infected computers by disconnecting them from the network. Many worms can transfer through shared resources without user interaction. Familiarize yourself with the mechanisms by which these worms operate by carefully reading the virus write-ups available at <http://securityresponse.symantec.com>.

Once you understand the virus threat, implement an emergency plan based on the guidelines in this article.

Understanding Network Topology

Fundamental to containing a virus infection understands the topology of your network. As a preliminary action, create a map, or use a map that you currently have, to section off your network client systems in a way that will allow you to systematically isolate and clean the

computers in each section before reconnecting them to your local network. Your map should contain the following information:

- Servers - name and address
- Clients - name and address
- Network protocols
- Shared resources

Understanding Security Solutions

In addition to understanding your network topology, you need to understand how anti-virus and security products are implemented to protect your network and distribute virus definitions and security updates. Consider the following information:

- What security programs are protecting servers and clients.
- What is the plan for checking, testing, and installing operating system and network updates.
- What is the schedule for updating virus definitions.
- What alternative methods of obtaining updates are available if the normal channels are under attack.
- What log files are available to administrators.

Understanding Backup Solutions

It is imperative that you have critical system information backed up. In the event of a catastrophic virus infection, it may be necessary to restore servers and clients to be sure that your network has not been compromised. Having a backup plan in place with procedures to backup and restore critical systems is essential.

To combat worms that spread across network resources

1. Disconnect your local network from incoming transfers.
2. Run Live Update and ensure that the latest definitions have been distributed throughout your network.

Note: Many times during a virus outbreak emergency, it may be difficult to retrieve definitions through the Live Update process. If Live Update is unavailable, then download and run the manual updater from the Symantec Web Site.

3. Isolate any systems displaying virus-, Trojan-, or worm-like activity by disconnecting them from the internal network.

4. Run a complete scan, scanning all file types, on all computers that are suspected of infection.
5. In the event that a virus is found and is cleaned or quarantined, go through any manual disinfection routines on those computers that have been isolated.
6. Visit <http://securityresponse.symantec.com> to see whether a removal tool is available for this infection.
7. Repeat steps 1 through 6 on all computers that are suspected of infection and do not reconnect any computers to the network until your entire LAN is disinfected.

TROUBLESHOOTING

TROUBLESHOOTING CONTENT DELIVERY TO THE SYMANTEC ENDPOINT PROTECTION CLIENT

Symantec Endpoint Protection supports updates to its data and engines in the field. These updates are collectively referred to as "content".

Content reaches the Symantec Endpoint Protection client via 4 possible channels:

- Distributed by the Symantec Endpoint Protection Manager Symantec Endpoint Protection Manager
- Downloaded from a Live Update server (internal or external)
- Distributed by the Group Update Provider (GUP)
- Distributed by a third-party management system (TPM)

Content Flow

This is the general flow of content packages to Symantec Endpoint Protection clients for each channel.

Distributed by the Symantec Endpoint Protection Manager

Internal or External Live Update Server > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Client

Downloaded from a Live Update server (internal or external)

Internal or External Live Update Server > Symantec Endpoint Protection Client

Distributed by the Group Update Provider (GUP)

Internal or External Live Update Server > Symantec Endpoint Protection Manager > GUP Host > Symantec Endpoint Protection Client

Distributed by a third-party management system (TPM)

Internal or External Live Update Server > Symantec Endpoint Protection Manager > Third Party Management System > Symantec Endpoint Protection Client

Enabling or disabling each of these channels is done in the Symantec Endpoint Protection Manager Console under Policies > Live Update. There are two policies: Live Update Settings and Live Update Content. Live Update Settings policy controls which channels are enabled and other settings, such as scheduling. Live Update Content policy controls which content types are enabled and which sequence number of each content type to use. Live Update Settings is a location-specific policy, while Live Update Content is a location-independent policy.

SescLu.exe is the executable responsible for processing Live Update policies and orchestrating content management on the Symantec Endpoint Protection Client. LuAll.exe (owned by the Live Update team) is used both when downloading content directly from a Live

Update server and as a tool for installing some content types distributed by other channels.

Symantec Endpoint Protection identifies each content type using a "moniker". A moniker is a GUID that uniquely identifies a combination of content's product, platform and language. For instance, SESC Virus Definitions Win32 v11 on Win32 in All Languages is identified by the moniker {C60DC234-65F9-4674-94AE-62158EFCA433}. Each revision of a content type is identified by a "sequence number". The Virus Definitions released today will have a higher sequence number than the ones released yesterday.

Troubleshooting

If the Symantec Endpoint Protection client reports that its content is out of date and you can't figure out why, here are some things to try. When troubleshooting, keep these questions in mind:

- Which update channels do I have enabled?
- Do I have the content I'm expecting enabled in the Live Update Content policy?
- Do I have the content I'm expecting set to **latest revision** or a **specific revision** in the Live Update Content policy?
- If I am expecting content to come down via the Symantec Endpoint Protection Manager, does the Symantec Endpoint Protection Manager itself have the content?
- If I am expecting content to come down via a Live Update server, do I have Live Update enabled in the Live Update Settings policy?

Log. LiveUpdate

The main Live Update executable is LuAll.exe. It is typically located in C:\Program Files\Symantec\Live Update. When you click "Live Update" on the Symantec Endpoint Protection Client UI, when you send down an "Update Content" command from the Symantec Endpoint Protection Manager Console or when a scheduled Live Update is run, LuAll.exe will be launched. LuAll.exe is also launched when installing content updates (**except** for AV Definitions and IPS Signatures) distributed to the Symantec Endpoint Protection client via the Symantec Endpoint Protection Manager or other channels. AV and IPS content that arrives from Symantec Endpoint Protection Manager, GUP or TPM are not installed using LuAll.exe.

LuAll.exe outputs to a debug log (Log.LiveUpdate) every time it runs. This log is typically located at C:\Documents and Settings\All Users\Application Data\Symantec\Live Update (c:\ProgramData\Symantec\LiveUpdate on Vista or newer).

If a content update package arrives on the client but fails to install, there is usually good related information in the Log.LiveUpdate, though it is typically buried under a mountain of extraneous log lines. A good strategy is to start looking for lines that contain "Start of New LU

Session" and then examining the subsequent lines to determine if the session relates to the content you are interested in. Searching for the product name or the moniker associated with your content is also helpful. You should eventually be able to find the exact failure.

Content Cache Directory

Content that arrives on the Symantec Endpoint Protection Client is cached on disk. The default number of cached revisions is either 3 or 5 depending on your Symantec Endpoint Protection version. AV and IPS content is always cached, no matter what channel it used to get there. Other content types are cached for all channels except the Live Update server channel. The cache directories are as follows:

- Symantec Endpoint Protection 11.0.1 or older
 - All content is typically under c:\Program Files\Symantec\Symantec Endpoint Protection\Content Cache
- Symantec Endpoint Protection 11.0.2 or newer
 - AV content: C:\Program Files\Common Files\Symantec Shared\VirusDefs
 - IPS content: C:\Program Files\Common Files\Symantec Shared\SymcData\cndcipsdefs
 - All other content is typically under c:\Program Files\Symantec\Symantec Endpoint Protection\ContentCache

If you are unsure if new content has made it to the client and been installed, check the cache. Content that arrives but fails to install will not be cached.

Event ID 13: LiveUpdate returned a non- critical error. Available content updates may have failed to install

This event shows up in the Symantec Endpoint Protection client's Windows Event Log. It indicates that a 20010007 (see DbgView section above) has occurred. This error condition should be resolved as soon as new sequence number for that content becomes available. To figure out which content package is failing, look at the DbgView output and Log.LiveUpdate. If the Symantec Endpoint Protection client in question receives new content via Symantec Endpoint Protection Manager, TPM or GUP and you are sure that a new, corrected content packages is available, but are still seeing the error, some things you might try:

- Verify that the new content package has been downloaded to Symantec Endpoint Protection Manager by checking that it is listed under the LiveUpdate Content policy
- Verify that you have the content type in question set to "use latest available" in the LiveUpdate Content policy

- Verify that intermediate steps in the content flow are up and running (the GUP, an internal LiveUpdate server, Third Party Management software)
- If the content type that is failing is not AV Definitions or IPS Signatures, try deleting the cached revisions of that content under c:\Program Files\Symantec\Symantec Endpoint Protection\ContentCache. This will force a full package to come down via your enabled content channel(s) rather than a delta package.

SYMANTEC ENDPOINT PROTECTION CLIENT DEBUG LOGS

- What different kind of debug logging is available for the Symantec Endpoint Protection client?
- How to turn on debug logging?
- Where do I find detailed logs for debugging in Symantec Endpoint Protection?
- What are the different types of debug logs?

There are several different debug logs for the different client components.

RtvScan

RtvScan is the AntiVirus/Antispyware scanning process. Its log is in the product install directory and is named vpdebug.log	HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\ProductControl
Registry Key:	
Registry Value:	Debug (string)

Sylink

Sylink handles the client-side communication between the client and the Symantec Endpoint Protection Manager. Once you set the registry values below, you will have to restart the smc service to start writing the log.

Registry Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink
Registry Value:	DumpSylink (string)
Set To:	Complete path to the log file (i.e. c:\sylink.log)

Registry Value:	DumpSymlinkLevel (DWORD)
Set To:	1, 2, 3 or 4. If you don't set this value, the default is 3.

Please note: The behavior of Symlink debug logging has changed in MR3. Prior to MR3, SMC debug value doesn't need to be set to 1 for symlink activities to be logged in the log file. With MR3, the SMC debug value has to be set to 1

Registry Key:	HKLM\Software\Symantec\Symantec Endpoint Protection\SMC
Registry Value:	smc_debuglog_on = 1

SMC

SMC is the agent process that hosts plug-ins that implement all other functionality. Its log is in the product install directory and is named debug.log

Registry Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC
Registry Value:	smc_debuglog_on (DWORD)
Set To:	1

Registry Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\Log
Registry Value:	debug_log_filesize (DWORD)
Set To:	The maximum log size in bytes before it rolls over. For example, 0000c350 lets the log grow to 50MB.

SescLu

SescLu handles client content updates that come via Symantec Endpoint Protection Manager (SEPM), Third Party Management (TPM) or Group Update Provider (GUP).

LiveUpdate

LiveUpdate handles client content updates that come via an internal or external LiveUpdate server. It is also used as a local content install tool by SescLu for some content types. The LiveUpdate log is always on and does not need to be enabled.

Directory:	C:\Documents and Settings\All Users\Application Data\Symantec\LiveUpdate
File:	Log.LiveUpdate

SepLuCallback

SepLuCallback is Symantec Endpoint Protection's custom LiveUpdate callback that handles client AntiVirus Definitions and IPS Signature content that come via an internal or external LiveUpdate server. Like SescLu's debug output, SepLuCallback's debug output can be viewed using DbgView. SepLuCallback does not write a log file to disk.

The DbgView tool can be downloaded from the Microsoft website:

<http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx> . This tool will allow you to save a log containing the SepLuCallback information.

DefUtils

DefUtils is the library that handles all direct interaction with AntiVirus Definitions and other DefUtils managed content (such as IPS Signatures). Products like Symantec Endpoint Protection make requests of DefUtils and DefUtils handles all the details, shielding Symantec Endpoint Protection from needing AntiVirus Definition-specific know-how.

DefUtils has a log that can be enabled. It is useful for tracking down AntiVirus Definition errors, such as definition corruption or failure to authenticate.

To enable the log:

- Create a text file called symc-defutils.conf
- Inside the file, put the following 2 lines:

```
[defutillog]
```

```
defutillog_name=defutils.log
```

- Copy symc-defutils.conf to the following locations:

```
C:\Program Files\Common Files\Symantec Shared\
```

```
C:\Program Files\Common Files\Symantec Shared\VirusDefs
```

Now whenever the DefUtils library is invoked, debug output will be written to defutils.log in the VirusDefs directory.

SYMANTEC ENDPOINT PROTECTION: TROUBLESHOOTING CLIENT/SERVER CONNECTIVITY

How to troubleshoot client to manager connectivity issues.

Symptoms:

- Client not getting definition updates.
- Client not getting policy updates.
- Client not showing green dot in taskbar.
- Client not showing green dot in the Symantec Endpoint Protection Manager console.

Solution:**About communication problems**

Check network connectivity before you call Symantec Technical Support. Once that has been verified, check the communication between the client and the server. For example, the client may not be receiving Policy updates or it may not be receiving Content updates. It is important to gather as much information as possible about which communications are working and which are not.

About checking the communication between the client and the management server

If you have trouble with the client and the server communication, you should first check to make sure that there are no network problems. You can test the communication between the client and the management server in several ways.

Table 2-1 describes the steps that you can take to check the communication between the client computer and the management server.

Table 2-1 Checking the communication between the management server and the client










What to check	Description
Check the client status icon.	You can check the status icon in the client and in the management console.
Check the policy serial number in the client and in the management console.	<p>The serial number should match if the client can communicate with the server and receives regular policy updates.</p> <p>You can perform a manual policy update and then check the policy serial numbers against each other.</p>
Test the connectivity between the client and the management server.	<p>You can issue several commands on the client to test the connectivity to the management server.</p> <p>You can do the following tests:</p> <ul style="list-style-type: none"> ■ Ping the management server from the client computer. ■ Telnet to the management server from the client computer. ■ Use a Web browser on the client computer to connect to the management server.
Check for any network problems.	<p>You should verify that there are no network problems by checking the following items:</p> <ul style="list-style-type: none"> ■ Test the connectivity between the client and management server first. If the client computer cannot ping or Telnet to the management server, you should verify the DNS service for the client. ■ Check the client's routing path. ■ Check that the management server does not have a network problem. ■ Check that the Symantec Endpoint Protection firewall (or any third-party firewall) does not cause any network problems.
Check the IIS logs on the management server.	You can check the IIS logs on the management server. The logs can help you to determine whether the client can communicate with the IIS server on the management server computer.
Check the debug logs on the client.	You can use the debug log on the client to determine if the client has communication problems.

Viewing the client status in the management console

You can check the client status icon in the management console as well as on the client directly to determine client status.

Table 2-3 shows the various icons that might appear in the management console for the client status.

Table 2-3 Client status icons in the management console

Icon	Description
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	<p>This icon indicates the following status:</p> <ul style="list-style-type: none"> ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in user mode.

To view the client status in the management console:

- In the management console, on the **Clients** page, under "View Clients", select the group in which the client belongs.
- Look on the **Clients** tab.

The client name should appear in the list next to an icon that shows the client status.

About the client status icon on the client

You can find the client status icon in the notification area of the taskbar on the client computer. The icon appears as a yellow shield icon with a green dot when the client can communicate with the management server.

Viewing the policy serial number

You should check the policy serial number on the client to see if it matches the serial number that appears in the management console. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

If the policy serial numbers do not match, you can try to manually update the policies on the client computer and check the troubleshooting logs.

To view the policy serial number in the management console

1. In the management console, click **Clients**.
2. Under "View Clients", select the relevant group, and then select the **Details** tab.

The policy serial number and the policy date appear at the bottom of the details list.

To view the policy serial number on the client

- On the client computer, in the client user interface, click on the **Help and Support** button, select **Troubleshooting**.
- In the **Management** section, look at the policy serial number.

The serial number should match the serial number of the policy that the management server pushes to the client.

About performing a manual policy update to check the policy serial number

You can perform a manual policy update to check whether or not the client receives the latest policy update. If the client does not receive the update, there might be a problem with the client and server communication.

You can try a manual policy update by doing any of the following actions:

- In the client click on the **Help and Support** button, click **Troubleshooting**. Under Policy Profile, click **Update**. You can use this method if you want to perform a manual update on a particular client.

- For the clients that are configured for pull mode, the management server downloads policies to the client at regular intervals (heartbeat). You can change the heartbeat interval so that policies are downloaded to the client group more quickly. After the heartbeat interval, you can check to see if the policy serial numbers match. (For the clients that are configured for push mode, the clients receive any policy updates immediately.)

After you run a manual policy update, make sure that the policy serial number that appears in the client matches the serial number that appears in the management console.

Using the ping command to test the connectivity to the management server

You can try to ping the management server from the client computer to test connectivity.

To use the ping command to test the connectivity to the management server

1. On the client, open a command prompt.

2. Type the ping command. For example:

ping name

3. Where name is the computer name of the management server. You can use the server IP address in place of the computer name. In either case, the command should return the server's correct IP address.

If the ping command does not return the correct address, verify the DNS service for the client and check its routing path.

Using a browser to test the connectivity to the management server

You can use a Web browser to test the connectivity to the management server.

To use a browser to test the connectivity to the management server:

1. On the client computer open a Web browser, such as Internet Explorer.
2. In the browser command line, type a command that is similar to either of the following commands:

- `http://<management server IP address>/reporting/index.php`

If the reporting log-on Web page appears, the client can communicate with the management server.

- `http://<management server name>:9090`

If the Symantec Endpoint Protection Manager Console page appears, the client can communicate with the management server.

3. If a Web page does not appear, check for any network problems. Verify the DNS service for the client and check its routing path.

Using Telnet to test the connectivity to the management server

You can use Telnet to test the connectivity to the IIS server on the management server. If the client can Telnet to the management server's HTTP or HTTPS port, the client and the server can communicate. The default HTTP port is 8014 (80 for the earlier builds of SEP); the default HTTPS port is 443.

Note: You might need to adjust your firewall rules so that the client computers can Telnet into the management server.

For more information about the firewall, see the Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control.

To use Telnet to test the connectivity to the management server

1. On the client computer, make sure the Telnet service is enabled and started.
2. Open a command prompt and enter the Telnet command. For example:

```
telnet ip address 8014
```

where ip address is the IP address of the management server.

If the Telnet connection fails, verify the client's DNS service and check its routing path.

Checking the IIS logs on the management server

You can check the IIS logs on the management server. The logs show GET and POST commands when the client and the server communicate.

To enable logging in IIS:

1. In the IIS manager, right click each site where you wish to have the logs (such as Reporting, Secars, etc.) and select **Properties**
2. On the **Virtual Directory** tab: ensure a check in the box that corresponds to **Log visits**.
3. Click **OK**.

To check the IIS logs on the management server:

4. On the management server, go to the IIS log files directory. A typical path to the directory is:

\\WINDOWS\system32\LogFiles\W3SVC1

5. Open the most recent log file with a text application such as Notepad.
For example, the log file name might be ex070924.log.
6. Review the log messages.

The file should include both GET and POST messages.