LiveUpdate™ Administrator's Guide

LiveUpdate™ Administrator's Guide

Documentation version 1.7b

Copyright Notice

Trademarks

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

When contacting the Technical Support group, please be sure to have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (such as features, language availability, dealers in your area)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advise on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1

Overview

This chapter includes the following topics:

About LiveUpdate

LiveUpdate is the Symantec technology that lets installed Symantec products connect to a Symantec server automatically for program and virus definitions updates. The connection is made through an HTTP or an FTP site. Note that while downloading virus definitions and other content updates requires a paid subscription, the updates are included in many corporate contracts.

For corporate sites, Symantec has developed the LiveUpdate Administration Utility (LuAdmin) to address some issues that are unique to corporate environments:

- Security: LiveUpdate establishes an FTP or HTTP connection to a Symantec server. In some cases, this implementation requires modification to firewall software.
- Network traffic: Administrators want to reduce external traffic by having users download updates from an internal site.
- Management: Administrators have no control over the updates that are available to their users.

This guide explains how LiveUpdate works and how you can configure it to suit your environment.

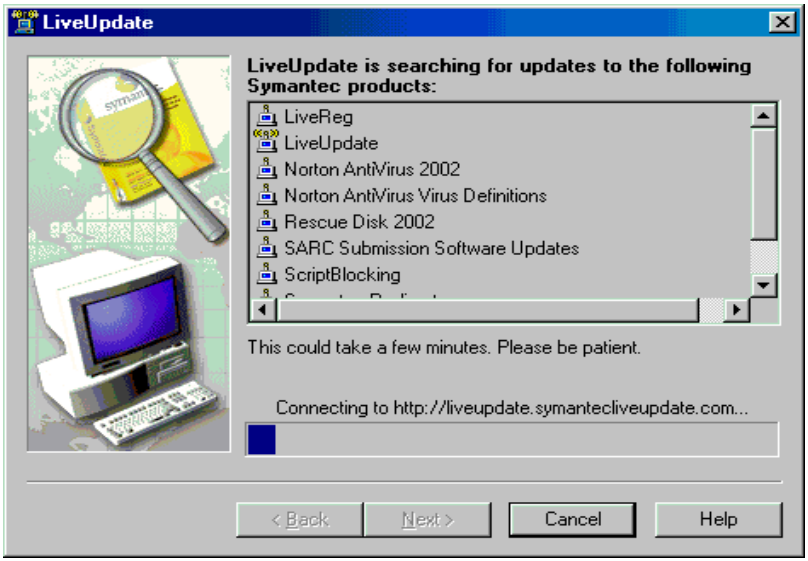
How the LiveUpdate client works

When you start LiveUpdate, it displays a list of the registered Symantec products on the computer and establishes the versions and languages of the products to be updated. LiveUpdate then determines the types of updates that are needed, and the order in which to apply the updates.

LiveUpdate next finds and connects to a LiveUpdate server, either an external Symantec server or an internal server that has been set up by an administrator using the LiveUpdate Administration Utility. LiveUpdate downloads and decompresses a ZIP file named Livetri.zip. LiveUpdate checks the information

within this file (Liveupdt.tri) to see if updates are required (see Figure 1-1). If LiveUpdate determines that updates are available, it downloads and applies them.

Figure 1-1 LiveUpdate product search window



LiveUpdate version 1.6x and later can download updates from the closest external LiveUpdate host server. This typically results in decreased download times. If there is a failure, LiveUpdate automatically uses one of the Symantec LiveUpdate servers.

LiveUpdate version 1.7x performs additional authentication and error checking. Descriptive warnings and error messages assist you in troubleshooting LiveUpdate failures.

See "Understanding LiveUpdate 1.7 package authentication" on page 56.

LiveUpdate client files

Table 1-1 lists the files used by the LiveUpdate client.

Table 1-1 LiveUpdate client files

File	Description
Settings.Default.LiveUpdate	Backup copy of the original default settings for the LiveUpdate client. This is for reference only.
AUPDATE.EXE	Automatic LiveUpdate executable. This program is used to retrieve product or content updates automatically.
LSETUP.EXE	LiveUpdate custom installer application.
LUALL.EXE	Main LiveUpdate executable file that displays all product UI. This file may be run from the command line.
LUALL.HLP	LiveUpdate Help file.
LuComServer.EXE	LiveUpdate engine file.
LuComServerPS.DLL	LiveUpdate engine file.
ludirloc.dat	Configuration file that stores the initial location of the LiveUpdate settings files. This file may be referenced later by LiveUpdate if it cannot find the LiveUpdate settings files.
LUINFO.INF	File used by the LiveUpdate installer. It contains a list of the files installed by LiveUpdate.
LUInit.exe	LiveUpdate installer file.
LUInit.ini	LiveUpdate installer file.
LUINSDLL.DLL	LiveUpdate installer file.
NDETECT.EXE	Automatic LiveUpdate executable. Used to determine the presence of an Internet connection.
NetDetectController.DLL	Automatic LiveUpdate executable.
ProductRegCom.DLL	LiveUpdate engine file.
README.TXT	Updated product information, including recent enhancements, bug fixes, and known issues.
S32LIVE1.DLL	LiveUpdate engine file.

Table 1-1 LiveUpdate client files

File	Description
S32LUCP1.CPL	LiveUpdate control panel file.
S32LUIS1.DLL	LiveUpdate engine file.
S32LUWI1.DLL	LiveUpdate engine file.
SymantecRootInstaller.exe	Program that installs a copy of the Symantec root certificate into the Microsoft certificate store to be used by Internet Explorer.

LiveUpdate client file locations

For LiveUpdate client versions 1.6x and 1.7x, settings are stored as read-only files in the LiveUpdate data folder. The location of the LiveUpdate data folder is dependent upon your operating system.

- In Windows 2000 (a clean installation, not an upgrade), the LiveUpdate folder is located under:
  C:\Documents And Settings\All Users\Application Data\Symantec
- In Windows 95, the LiveUpdate folder is located under:
  C:\Windows\Application Data\Symantec
- In Windows 98, the LiveUpdate folder is located under:
  C:\Windows\All Users\Application Data\Symantec
- In Windows NT 4.0, the LiveUpdate folder is located under:
  C:\WinNT\Profiles\All Users\Application Data\Symantec

If necessary, the folder and path are created during installation. However, if an Application Data folder exists at the time of the installation, the location specified by Shfolder.dll is used.

Note: If you have upgraded your operating system from a different version, the correct directory may be one that is listed for the previous operating system.

Shfolder.dll is distributed with Internet Explorer 5.0 and later, and a re-distributable Microsoft updater that installs this file is included with the LiveUpdate installation.

LiveUpdate program files are stored in the following location:
Program Files\Symantec\LiveUpdate

LiveUpdate client configuration files

The configuration information for LiveUpdate clients versions 1.6x and later is in the \Downloads\ folder and in the following files:

- Product.Catalog.LiveUpdate
- Log.LiveUpdate
- Settings.LiveUpdate

These files are found in the Symantec\LiveUpdate folder locations described above. You can view and edit the information in these files with a text editor such as Notepad.

See "Using LiveUpdate client configuration files" on page 46.

How the LiveUpdate Administration Utility works

Using the LiveUpdate Administration Utility (LuAdmin), you can set up an intranet HTTP or FTP server, or a directory on a standard file server to handle all LiveUpdate operations for your network. Users connect to the internal server to retrieve updates instead of connecting to external Symantec servers. By having users connect to a LiveUpdate server on your internal network, you reduce network traffic, increase transfer speed, and limit the size of virus definitions updates that are sent to each client. The LiveUpdate Administration Utility is also useful if you do not have Windows NT computers in your network or if your Windows NT computers do not have Internet connections.

Note: Do not use a UNC location for NT workstations and servers. If you use a scheduling utility, LiveUpdate will not be able to connect to a UNC location unless the LiveUpdate files reside in a shared resource on the NT server that all users are authorized to access (a NULL share).

To use the download and security enhancements in LiveUpdate 1.6x and 1.7x, you must use LiveUpdate Administration Utility version 1.5.3.21 or later. You can download the latest version of LuAdmin, along with supporting documentation, from the Symantec Web site at:

http://www.symantec.com/techsupp/files/lu/lu.html

LiveUpdate Administration Utility files

Table 1-2 lists the files used by the LiveUpdate Administration Utility.

Table 1-2 LiveUpdate Administration Utility files

File	Description
401comup.exe	Common control update (Comctl32.dll) that is required by LuAdmin.exe. The LuAdmin installer detects if you need this update. The installer copies the executable to your LiveUpdate Administration install folder. You must manually install it.
ISLUA.DLL	Custom install and uninstall library.
lua1d5.rtf	File that describes what's new in the latest release of the LiveUpdate Administration Utility.
LuAdmin.exe	LiveUpdate Administration Utility program.
luadmin.hst	Host file that downloads update packages.
Lualog.xml	File that logs messages for events, such as the retrieval process, custom update merging, and host file encryption/decryption. Logs from both the background execution of the application and the execution of the application in user mode. The contents of this file are viewable via the log file viewer within the LiveUpdate Administration Utility.
luaupdat.exe	Executable file. When updating the LiveUpdate Administration Utility, this file launches, closes the LiveUpdate Administration Utility, runs LiveUpdate, then relaunches the LiveUpdate Administration Utility. This process eliminates the need to restart the computer.

Table 1-2 LiveUpdate Administration Utility files

File	Description
products.xml	File that stores a dynamic list of products selected in the Retrieve Updates window. Lets you choose not only multiple languages for multiple product lines, but also the specific products for particular languages within those product lines. Every time that the LiveUpdate Administration Utility downloads from the Symantec servers, the product list is updated as necessary. It also stores your specified LiveUpdate Administration Utility preferences. The contents of this file are viewable via the log file viewer within the LiveUpdate Administration Utility.
README.TXT	Text file that documents the latest changes to the LiveUpdate Administration Utility, as well as any technical issues and late breaking information not included in this document.
S32luhl1.dll	File that is distributed to workstations only if you use a UNC path instead of an FTP server.
SAMPLE.HST	Host file to customize for workstations.
SilntLuA.exe	Silent LiveUpdate Administrator executable file. See "Retrieving packages with Silent LiveUpdate Administrator" on page 31.
SYMZIP.DLL	LiveUpdate ZIP engine/compression library.
Uninst.isu	File that uninstalls the LiveUpdate Administration Utility program.

By default, the LiveUpdate Administration Utility is installed in the Program Files\LiveUpdate Administration folder.

Upgrading LiveUpdate

For versions of LiveUpdate earlier than 1.6x, settings are stored in the registry. When you install LiveUpdate 1.6 or later over an earlier version of LiveUpdate, the settings in the registry are moved to the Settings.LiveUpdate and Product.Catalog.LiveUpdate files. The settings under HKLM\Software\Symantec\LiveUpdate are converted into values in the Settings.LiveUpdate file, with the exception of information regarding registered Symantec products and patches. This information is moved into the Product.Catalog.LiveUpdate file.

The legacy host file, Liveupdt.hst, is converted into the HOSTS\ property tree in the Settings.LiveUpdate file. Before this conversion takes place, the HOSTS\ property tree is deleted so that the contents of the Liveupdt.hst file replace any previous host information. After conversion, the Liveupdt.hst file is deleted.

LiveUpdate Administration Utility and LiveUpdate client compatibility

Because of the changes in configuration file locations in LiveUpdate 1.6x and later, it is important that you use the correct version of the LiveUpdate Administration Utility when managing LiveUpdate client computers. Table 1-3 lists the versions of the LiveUpdate Administration Utility (LuAdmin) that can be used with the versions of the LiveUpdate client.

Table 1-3 LiveUpdate version compatibility

LiveUpdate client	LiveUpdate Administration Utility
LiveUpdate 1.5x	LuAdmin 1.5x
LiveUpdate 1.6x	LuAdmin 1.5.3.18 and later
LiveUpdate 1.7x	LuAdmin 1.5.3.21 and later

To take full advantage of the increased security features in LiveUpdate client 1.7, you must use LuAdmin version 1.5.3.21 or later.

Setting up a LiveUpdate intranet server

You must complete the following tasks to set up a LiveUpdate intranet server:

- Install and run the LiveUpdate Administration Utility.
  See "Installing and running the LiveUpdate Administration Utility" on page 19.
- Select languages and products to download, and specify a download directory.
  See "Setting download options" on page 20.
- Create a custom host file (Liveupdt.hst) that points client computers to the internal server using the LiveUpdate Administration Utility (LuAdmin).
  See "Creating a LiveUpdate host file for client workstations" on page 24.
- Distribute the host file (Liveupdt.hst) to all computers that use the LiveUpdate feature using your preferred distribution tool.
- Download update packages from Symantec to the internal server using the LiveUpdate Administration Utility (LuAdmin).
  See "Retrieving update packages" on page 21.
  See "Retrieving packages with Silent LiveUpdate Administrator" on page 31.

Chapter 2

Installing the LiveUpdate Administration Utility

This chapter includes the following topics:

LiveUpdate Administration Utility system requirements

For LiveUpdate Administration Utility 1.5 and later, the system requirements are as follows:

- Windows 95/98/98 SE/Me
- Windows NT 4.0 Workstation/Server/Enterprise Server/Terminal Server
- Windows 2000 Professional/Server/Advanced Server/Data Center
- Windows XP Home/Professional
- Internet Explorer 4.0 or later
- Pentium 100 MHz processor
- 16 MB RAM
- 25 MB hard disk space and up to 500 MB of additional space for LiveUpdate packages

LiveUpdate client system requirements

For LiveUpdate clients 1.5x and later, the requirements are as follows:

- Windows 95/98/98 SE/Me
- Windows NT 4.0 Workstation/Server/Enterprise Server/Terminal Server
- Windows 2000 Professional/Server/Advanced Server/Data Center
- Windows XP Home/Professional
- Pentium 100 MHz processor
- 16 MB RAM
- 10 MB hard disk space and up to 50 MB of additional space for package downloads (depending on the size of the LiveUpdate package)

Installing and running the LiveUpdate Administration Utility

The LiveUpdate Administration Utility is a self-extracting, compressed archive (Luau.exe). It is included with many Symantec products. You can also download the latest version of the LiveUpdate Administration Utility installation file from the Symantec Web site at:

http://www.symantec.com/techsupp/files/lu/lu.html

To install the LiveUpdate Administration Utility

- Launch Luau.exe, then follow the on-screen instructions.

To run the LiveUpdate Administration Utility

- On the Windows taskbar, click **Start** > **Programs** > **LiveUpdate Administration Utility** > **LiveUpdate Administration Utility**.

Understanding the update retrieval process

The list of products that appears in the Retrieve Updates window is dynamically generated from a product list. This list is downloaded automatically from the Symantec LiveUpdate server at the end of every download session. This occurs whether or not updates are retrieved.

The following sequence of events occurs during the update retrieval process:

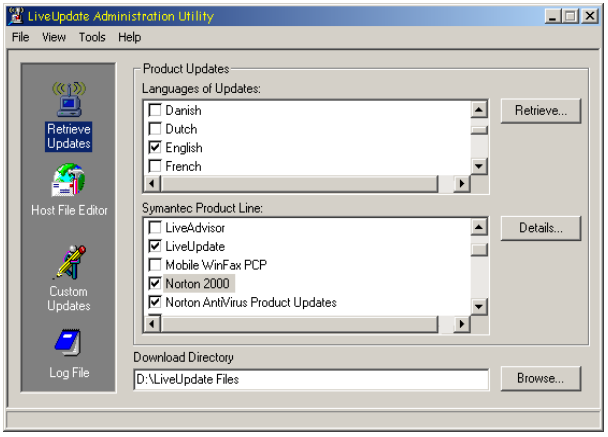
- A temporary download directory is created.
- Any available updates for the product that you chose are retrieved and placed in the temporary download directory.
- The index files are updated. Any incompatible updates are removed.
- All downloaded product updates and updated index files are moved from the temporary directory to your specified download directory.
- The product list is updated.
- Any custom updates are remerged.
- By default, all updates in the index file that weren't downloaded are removed.
- The utility checks for updates to itself.

Setting download options

To set download options, run the LiveUpdate Administration Utility and select the products and languages for which you want to get updates. You also must designate a download directory. This is the location in which the update packages and support files are stored once they are downloaded successfully from Symantec. (Files are first downloaded to a temporary directory that is created by the LiveUpdate Administration Utility. Once the file is downloaded, it is moved to the specified download directory.)

To set download options

1. Run LuAdmin.
2. In the left pane, click **Retrieve Updates**.



3. Under Languages of Updates, select the desired language for download packages.

4 Under Symantec Product Line, do one of the following:

- Check the Symantec product lines for which you want updates.

  Because all installed Symantec products that use LiveUpdate now point to your intranet server, you should download full product lines rather than individual products.
- Select individual product components by checking the appropriate product line check box, then clicking **Details** and checking the Languages and Product Updates to download.

  When you select individual product components to update, you run the risk of missing other available updates. For example, new virus definitions files for Norton AntiVirus may require an engine update that is also available.

5 Under Download Directory, do one of the following:

- Type the path to the directory where you want to download updates.
- Click **Browse** and locate the desired download directory.

The download directory can be any directory on your server, or a directory on your FTP or HTTP server.

In addition to the downloaded packages, LuAdmin retrieves index files called Symtri.zip, Livetri.zip, and Symtri16.zip, as well as Products.xml. These files are required by different versions of LiveUpdate.

Retrieving update packages

After you have selected the product updates and specified the download directory, you can retrieve update packages.

To retrieve update packages

1 Run LuAdmin.

2 In the left pane, click **Retrieve Updates**.

3 Click **Retrieve** to begin downloading update packages.

4 Follow the on-screen instructions.

Note: If the LiveUpdate Administration Utility does not successfully download all of the packages that you selected, then none of the packages appear in your specified download directory. Check the log file for details about the download activity.

The next time that users run LiveUpdate from their workstations, they receive the packages from your internal server, not the Symantec external server.

Handling interrupted downloads

The LiveUpdate Administration Utility knows if a download is interrupted. When you restart the download, assuming that no application settings have changed, the utility continues from where it left off, then integrates all of the packages that were downloaded in both sessions.

If a download is interrupted and you modify application settings (such as changing the product or languages), the utility assumes that the incomplete downloads cached from the preceding interrupted session are part of the current session. To avoid this, you must either restart with the same application settings or remove the cached incomplete downloads from the Program Files\LiveUpdate Administration\TEMP folder.

Chapter 3

Using the LiveUpdate Administration Utility

This chapter includes the following topics:

Creating a LiveUpdate host file for client workstations

Liveupdt.hst is the host file that controls the LiveUpdate operation on client workstations. The location of Liveupdt.hst depends on the version of LiveUpdate that is installed on the client. For LiveUpdate versions earlier than 1.6x, the Liveupdt.hst file is located under C:\Program Files\Symantec\LiveUpdate. For LiveUpdate 1.6x and later, the Liveupdt.hst file is read and then deleted.

You must create a new file that points to an internal server to replace the existing Liveupdt.hst on workstations.

Create a LiveUpdate host file

There are three types of hosts that you can create within host files:

- FTP: If you use an internal FTP server
- HTTP: If you use an internal HTTP server
- LAN: If you use a UNC directory or DOS drive with the full path

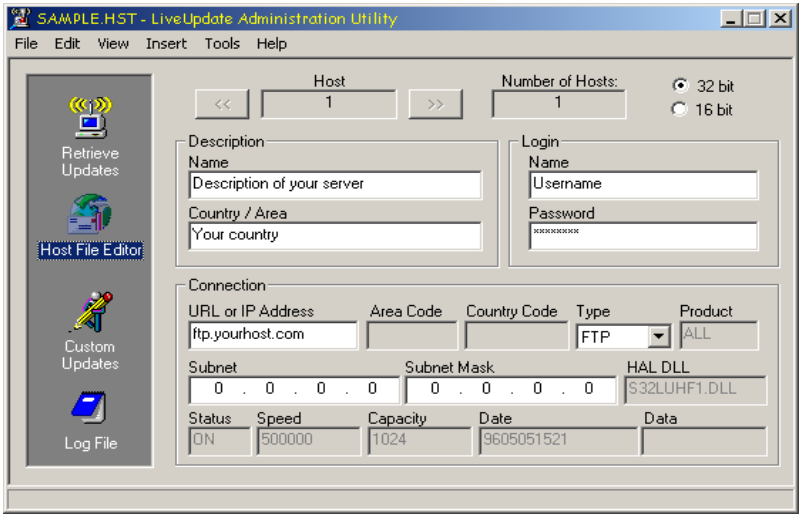
---

Note: For LiveUpdate versions earlier than 1.6x, the order in which the host entries appear in the host file is important if you are supporting both HTTP and FTP. Whichever of these two host types is specified first becomes the default connection type.

To create a LiveUpdate host file for FTP

1. Run LuAdmin.
2. In the left pane, click **Host File Editor**.
3. On the File menu, click **Open**.

4 In the current directory, double-click **SAMPLE.HST**.



5 Under Description, do the following:

- Under Name, type the name that you want to display when users connect to the internal server.
- Under Country / Area, type the country in which your server is located.

6 Under Login, do the following:

- Under Name, type the user name for the FTP server.

  All users use the same name.
- Under Password, type the password for the specified user name.

7 Under Connection, do the following:

- Under URL or IP Address, type the URL for the server or the IP address of the server.
- Under Type, click **FTP**.
- Under Subnet and Subnet Mask, type **0.0.0.0**

  For more information, see "Enabling TCP/IP by location" on page 29.

8 Select one of the following:

- 32 bit: Selected by default. If you install the 32-bit version, the file names start with S32.
- 16 bit: If you are creating a host file for 16-bit LiveUpdate clients, select the 16-bit radio button. If the 16-bit version of LiveUpdate is installed, then the DLLs in the LiveUpdate directory will have names starting with S16.

The 16-bit and 32-bit host files are not compatible with each other.

9 On the File menu, click **Save As**.

10 Save the customized file as Liveupdt.hst.

To create a LiveUpdate host file for HTTP

1 Run LuAdmin.

2 In the left pane, click **Host File Editor**.

3 On the File menu, click **Open**.

4 In the current directory, double-click **SAMPLE.HST**.

The 32-bit radio button is selected by default. HTTP-based hosts are not available to 16-bit clients. If you select 16-bit, you can have the utility convert the host into an FTP host. If you click **Yes**, you will need to review the host and, if necessary, modify it.

5 Under Description, do the following:

- Under Name, type the name that you want to display when users connect to the internal server.
- Under Country / Area, type the country in which your server is located.

6 Under Login, do the following:

- Under Name, type the user name for the HTTP server.

  All users use the same name.
- Under Password, type the password for the specified user name.

7 Under Connection, do the following:

- Under URL or IP Address, type the URL for the server or the IP address of the server.
- Under Type, click **HTTP**.
- Under Subnet and Subnet Mask, type **0.0.0.0**

  For more information, see "Enabling TCP/IP by location" on page 29.

8 On the File menu, click **Save As**.

9 Save the customized file as Liveupdt.hst.

To create a LiveUpdate host file for a UNC directory

1 Run LuAdmin.

2 In the left pane, click **Host File Editor**.

3 On the File menu, click **Open**.

4 In the current directory, double-click **SAMPLE.HST**.

The 32-bit radio button is selected by default. LAN-based hosts are not available to 16-bit clients.

5 Under Description, do the following:

- Under Name, type the name that you want to display when users connect to the internal server.
- Under Country / Area, type the country in which your server is located.

6 Under Login, do the following:

- Under Name, type a user name that has access rights to the server.

  If you leave this field blank, LiveUpdate attempts to connect using the user name logged on to the system.
- Under Password, type the password that corresponds to the user name.

  If you leave this field blank, LiveUpdate uses the password for the user logged on to the system.

7 Under Connection, do the following:

- Under Type, click **LAN**.
- Under Directory, type the UNC path or DOS drive with the full path to the server directory containing the LiveUpdate package.

8 On the File menu, click **Save As**.

9 Save the customized file as Liveupdt.hst.

Note: Modem support has been removed from LiveUpdate, although the option for it remains on the user interface.

Configuring LiveUpdate UNC support (LAN transport)

LiveUpdate supports the downloading of packages from an internal server via UNC support without the need for an HTTP or FTP server. The UNC support consists of two components:

- A LiveUpdate DLL that supports UNC download (S32luhl1.dll).
- A customized host file created by the LiveUpdate Administration Utility that points to the internal server.

By default, the UNC DLL becomes the exclusive transport when it is present. This prevents users from using FTP when the administrator has determined that it is better to use a UNC path.

On Windows 95/98/NT 4.0, LiveUpdate 1.4x and later can have Network as one of the connection options in the LiveUpdate Wizard.

To make Network a connection option

- Under HKEY_LOCAL_MACHINE\Software\Symantec\LiveUpdate\Preference, add the following registry entry:
  Name: All Transports Available
  Type: DWORD

If this entry is nonzero and S32luhl1.dll is present in the LiveUpdate directory, Network is an available connection option.

You could use this feature, for example, to have host files contain entries for an internal UNC location as well as for the Symantec FTP and HTTP servers. This is an ideal setup for laptop users.

Note: UNC support is only available with the 32-bit version of LiveUpdate. You can also specify a DOS drive with the full path instead of UNC.

Implementing LiveUpdate UNC support

After you create the host file, copy it and the UNC DLL (S32luhl1.dll) to the LiveUpdate directories on the client computers. The default LiveUpdate directory is \Program Files\Symantec\LiveUpdate.

To implement LiveUpdate UNC support

1. Create and distribute a new Liveupdt.hst file.
2. Distribute S32luhl1.dll to the workstations.
   This file is in the LuAdmin folder.
3. Create the update retrieval folder.
   See "Retrieving packages with Silent LiveUpdate Administrator" on page 31.

An issue exists for Windows 95/98 computers connecting to a Windows NT server. Windows 95/98 users must have access rights to the resource. It is not recommended that you use a UNC location for NT workstations and servers.

On LAN connections, LiveUpdate ignores user names and passwords supplied in the host file. The solution is to create a shared resource on a server that all users are authorized to access.

If you have workstations connecting to a UNC network location, the user logged on to the network must have access rights to the network resource. The user name and password supplied in the host file are ignored. With a Windows NT server, one option is to create a shared resource that all users are authorized to access (a NULL share). For information about creating a NULL share, refer to your Microsoft Windows NT server documentation.

Enabling TCP/IP by location

If you include more than one host entry in a single host file, or if you want client computers to log on to different servers based on their IP addresses, you must enable TCP/IP by location within the host file. To do this, you must type both a valid subnet and subnet mask. Otherwise, type all zeros for these settings.

LiveUpdate applies the subnet mask of the host entry to the IP address of the client workstation and then tries to match the resulting IP address with the subnet of the same host entry. If the masked IP address and subnet match, LiveUpdate uses that host to access the LiveUpdate server defined within the host.

If the IP address with the subnet mask applied does not match the subnet defined within the same host entry, LiveUpdate proceeds to the next host entry and repeats the process.

Sample host configuration

Table 3-1 shows a sample host configuration for a client workstation.

Table 3-1 Sample host configuration

Option	Entry
Host entry URL/IP	myserver.liveupdate.com
Host entry subnet	155.64.159.0
Host entry subnet mask	255.255.255.0
IP address of client workstation	155.64.159.20

The IP address of the client workstation with the above subnet mask applied is 155.64.159.0. This is matched with the subnet of the host entry. Since these IP addresses are identical, LiveUpdate uses this host to connect to the specified LiveUpdate server.

If the client workstation IP address is 155.64.155.80 and the above subnet mask is applied (resulting in 155.64.155.0), the subnet and resulting masked IP address do not match and LiveUpdate proceeds to the next host entry and repeats the process. If no matching host entries are found, the LiveUpdate session fails. You should have a default host entry that does not contain either subnet or subnet mask information as the last entry in the host file.

Making all connection options available

Normally, when S32luhl1.dll is placed in the LiveUpdate folder on the workstations, Network is the only connection option available. In the current version of LiveUpdate, you can make all of the connection options available. This may be practical for laptop users. For example, the host file on the laptop might contain an entry for an internal UNC location as well as the Symantec FTP and modem servers.

To make all connection options available

- Under HKEY_LOCAL_MACHINE\Software\Symantec\LiveUpdate\Preference, add the following registry entry:
  Name: All Transports Available
  Type: DWORD

When this entry is set to zero and S32luhl1.dll is present in the LiveUpdate directory, only the Network option is available.

When this entry is nonzero and S32luhl1.dll is present in the LiveUpdate directory, all connection options are available.

If S32luhl1.dll is not present in the LiveUpdate folder, only the Internet option is available.

Retrieving packages with Silent LiveUpdate Administrator

Silent LiveUpdate Administrator lets scheduled LiveUpdate Administration Utility sessions automatically retrieve all of the packages that you need without user intervention.

Before you run Silent LiveUpdate Administrator, you must run LiveUpdate Administration Utility to select the products to support, the language, and the download location. Once Silent LiveUpdate Administrator exits, the settings are saved and Silent LiveUpdate Administrator uses them every time it runs.

To retrieve packages automatically with Silent LiveUpdate Administrator

- Do one of the following:
  - Run SilntLuA.exe.

    By default, this program resides under \Program Files\ LiveUpdate Administration\.
  - Run LuAdmin.exe /SILENT.

Updating the LiveUpdate Administration Utility

The LiveUpdate Administration Utility can update itself. When the LiveUpdate Administration Utility finishes downloading packages, it automatically checks for new LiveUpdate Administration Utility updates.

To update the LiveUpdate Administration Utility

1. Run LuAdmin.
2. On the Tools menu, click **Update LiveUpdate Administration Utility**.
3. Click **Next** to see what updates are available.
4. Click **Finish** to complete the update.

Note: The LiveUpdate Administration Utility temporarily quits while retrieving and installing updates for itself.

Updating the LiveUpdate client

You can download the latest LiveUpdate client setup file using either of the following methods:

- Download Lusetup.exe from the Symantec Web site at:
  http://www.symantec.com/techsupp/files/lu/lu.html
- Download the client using the LiveUpdate Administration Utility.
  This lets your LiveUpdate clients update their workstations directly from your internal server.

When you run the installer manually, it can be run silently. To implement this functionality, use the command-line switch Lusetup /s /a /q

---

Note: To run the LiveUpdate installer silently for versions earlier than 1.6x, use the command Lusetup /s

---

To create a log file of the Lusetup installation, use the command-line switch Lusetup /a /log. This creates a log file named Luinstall.log in the Windows folder.

You can check the version of LiveUpdate contained in the installer by checking the date displayed in Lusetup.txt, which is available at:

http://www.symantec.com/techsupp/files/lu/lu.html

Using custom LiveUpdate packages

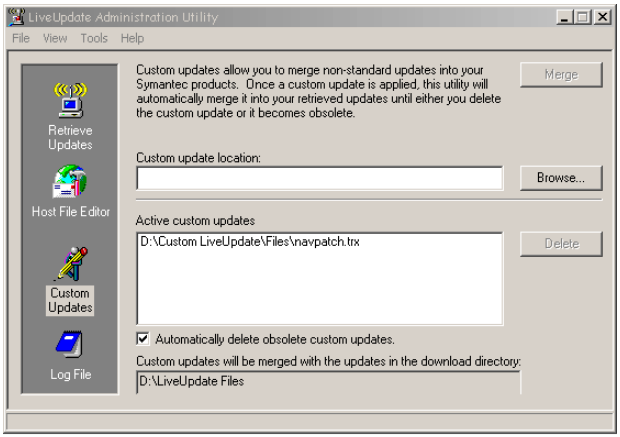
Symantec Security Response, formerly known as Symantec AntiVirus Research Center (SARC), or Symantec Technical Support supplies custom updates to customers on an as-needed basis. These updates, which have a .trx file extension,

are typically used to address unique situations or other specific Symantec customer needs. For example, an update may include virus definitions, not yet available from a LiveUpdate production server, that detect and remove a new virus.

Copy the .trx file onto a computer on which LiveUpdate Administration Utility is installed. When you receive a custom update, merge it with the most recent LiveUpdate definitions update. The merged update is delivered the next time that the client runs LiveUpdate.

To use custom LiveUpdate packages

1. Run LuAdmin.
2. In the left pane, click **Custom Updates**.
3. In the Custom update location text box, type the location in which the custom updates that you receive from Symantec are located on your computer.



4. Click **Merge**.

   LiveUpdate Administration Utility compares the dates of the custom update and your most recent LiveUpdate virus definitions and merges the files as appropriate. The Active custom updates box lists the current custom updates that are being applied by LiveUpdate Administration Utility.
5. If you want custom updates to be deleted automatically when they are no longer needed, check **Automatically delete obsolete custom updates.**

   LiveUpdate Administration Utility compares the dates and deletes obsolete custom update packages when you download LiveUpdate virus definitions files from a LiveUpdate server.

Using the LiveUpdate Administration Utility log file

The LiveUpdate Administration Utility includes an event log. This log may include events such as:

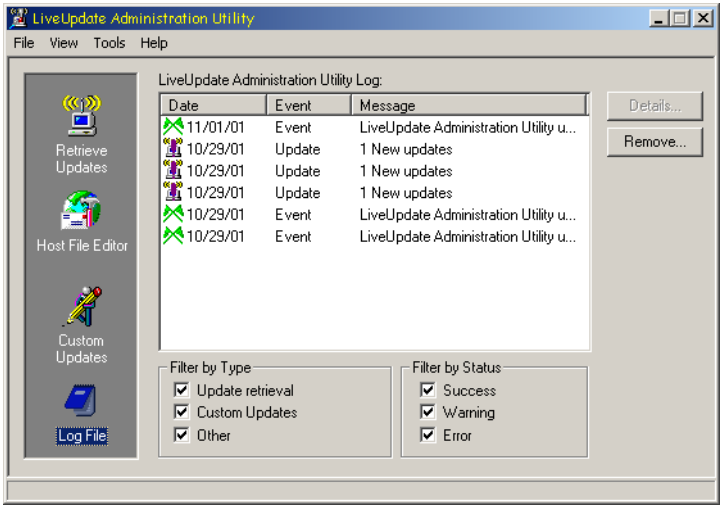
- The retrieval process, including silent updates
- Custom update merging
- Host file encryption and decryption

Use the LiveUpdate Administration Utility log file

You can view or remove events in the log file.

To view events in the LiveUpdate Administration Utility log file

1. Run LuAdmin.
2. In the left pane, click **Log File**.



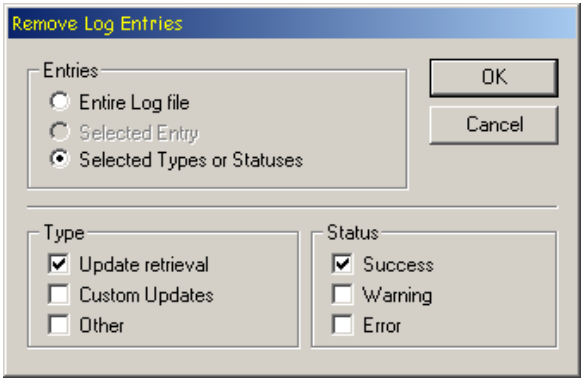
3. Under Filter by Type and Filter by Status, check the appropriate boxes to filter events.

To remove events from the LiveUpdate Administration Utility log file

1. Run LuAdmin.
2. In the left pane, click **Log File**.
3. In the right pane, do one of the following:
   - Under LiveUpdate Administration Utility Log, select one or more events that you want to remove, click **Remove**, then click **OK**.
   - Click **Remove**, remove all events or events based on the type or status, then click **OK**.

To remove events based upon type or status

1. Run LuAdmin.
2. In the left pane, click **Log File**.
3. In the right pane, click **Remove**.
4. In the Remove Log Entries window, click **Selected Types or Statuses**.
5. Select the type and/or status of the entries to remove.



6. Click **OK**.

Chapter 4

Using the LiveUpdate Administration Utility with the Symantec System Center

This chapter includes the following topics:

Configuring a host file for use with the Symantec System Center

Managed clients and Symantec AntiVirus NT servers can automatically receive LiveUpdate settings configured from the Symantec System Center. This lets them connect to your internal LiveUpdate server to download updates. For computers that are running Symantec AntiVirus 8.0, you can designate multiple LiveUpdate servers to provide fail-over capability.

After you've configured a host file, you must generate a new Grc.dat and enable LiveUpdate to perform scheduled updates.

To configure a host file for use with the Symantec System Center

1. Open the Symantec System Center.
2. In the Symantec System Center console, in the left pane, do one of the following:
   - Right-click the server group folder, then click **All Tasks** > **LiveUpdate** > **Configure**.

     When you make configuration changes at the server group level, all servers and all clients are affected, including Client Groups. This configures a host file for all servers and clients in the server group and lets them share the same settings.
   - Right-click the server or parent server, then click **All Tasks** > **LiveUpdate** > **Configure**.
3. In the Configure LiveUpdate dialog box, on the LiveUpdate tab, click **Internal LiveUpdate Server**.
4. Under Description, do the following:
   - In the Name text box, type the name of the server.
   - In the Location text box, type the location of the server.

   These text boxes are optional.
5. If you are using an FTP or HTTP server instead of a shared directory, under Login, do the following:
   - In the Name text box, type the name of the FTP or HTTP server.
   - In the Password text box, type the password for the FTP or HTTP server.
6. Under Connection, in the URL or IP Address text box, type the UNC path to your shared directory, or the URL or IP address for your HTTP or FTP server.

7. In the Type text box, select one of the following:
   - FTP
   - HTTP
   - LAN
8. In the Subnet and Subnet Mask text boxes, enter valid subnet and subnet mask addresses. Otherwise, leave these text boxes blank.
9. Check **Store passwords in encrypted form**.
10. Check **Apply settings to clients not in Groups**.
11. Click **Apply**.
12. Click **OK**.
13. If you want to configure multiple internal LiveUpdate servers, click **New** and repeat steps 1 - 12.
14. If you have multiple parent servers, repeat steps 1 - 13 for each parent server in order for all clients and servers to receive the changes, unless the steps are performed at the server group level.

Scheduling the retrieval of LiveUpdate packages

If the server you are configuring is also running the LiveUpdate Administration Utility, you have the option of scheduling the retrieval of LiveUpdate packages.

To schedule the retrieval of LiveUpdate packages

1. On the LiveUpdate Administrator tab, check **Schedule retrieval of LiveUpdate packages.**
   If the server is not running the LiveUpdate Administration Utility, this tab will not appear.
2. Under Frequency, select one of the following:
   - Daily: Set LiveUpdate Administrator to retrieve packages once a day.
   - Weekly: Set LiveUpdate Administrator to retrieve packages once a week.
   - Monthly: Set LiveUpdate Administrator to retrieve packages once a month.

3. Under When, do any of the following:
   - In the Time of Day box, select the time of day for the package retrieval.
   - In the Day of week box, select the day of the week for the package retrieval.
   - In the Day of month box, select the day of the month for the package retrieval.
4. Click **Apply**.
5. Click **OK**.

Generating a new Grc.dat file

You must generate a new version of the settings file (Grc.dat) before clients receive the changes.

To generate a new Grc.dat file

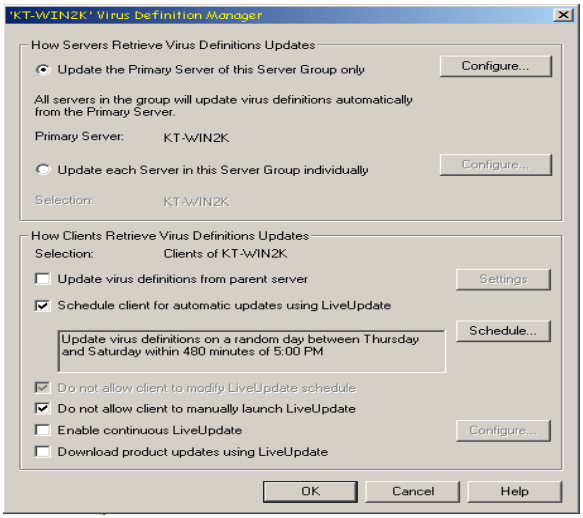
- Do one of the following:
  - Within the Symantec System Center, change an option within Client Realtime Protection Options, then click **Reset all**. You can immediately go back and change the option to the original setting.
  - Update the server's virus definitions.
  - Stop and then restart the Symantec AntiVirus Server service on the parent server. For NetWare servers, unload and then reload Vpstart.nlm.

Enabling and scheduling client updates from the Symantec System Center

After you have created a new host file and generated a new Grc.dat, you must enable LiveUpdate to perform scheduled updates of the clients.

To enable and schedule client updates from the Symantec System Center

1. Open the Symantec System Center.
2. In the Symantec System Center console, in the left pane, right-click the parent server, then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.



3. In the Virus Definition Manager dialog box, under How Clients Retrieve Virus Definitions Updates, uncheck **Update virus definitions from parent server.**
4. Check **Schedule client for automatic updates using LiveUpdate.**
5. Click **Schedule** to specify the frequency and time.
6. Click **OK** to save the changes and exit the Virus Definition Manager.

Configuring NetWare servers from the Symantec System Center

The LiveUpdate Administration Utility will not retrieve updates for NetWare Symantec AntiVirus servers. You can download these updates to your FTP server from the following FTP sites:

ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/vpcur.lst

ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/navup.exe

To configure NetWare servers from the Symantec System Center

1. Open the Symantec System Center.
2. In the Symantec System Center console, in the left pane, right-click the NetWare server, then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
3. In the Virus Definition Manager dialog box, under How Servers Retrieve Virus Definitions Updates, click **Configure**.
4. In the Configure Primary Server Updates dialog box, click **Source**.
5. In the Setup Connection dialog box, click **LiveUpdate (Win32) / FTP (NetWare)**.
6. Click **Configure**.
7. In the Configure FTP dialog box, type the FTP information needed to access the internal LiveUpdate server.

   Changes made here only apply to NetWare servers.
8. Click **OK** to save the changes and exit the Virus Definition Manager.

Note: In order for the NetWare server to download definitions from the internal LiveUpdate server, you must configure it to use TCP/IP and FTP correctly.

Configuring a host file for unmanaged clients

If you have unmanaged clients or are not using the Symantec System Center, you must create a new host file and distribute it to your clients.

To configure a host file for unmanaged clients

1. Run LuAdmin.
2. In the LiveUpdate Administrator dialog box, in the left pane, click **Host File Editor**.
3. On the File menu, click **New** > **Host File**.
4. Under Description, do the following:
   - In the Name text box, type the name of the server.
   - In the Location text box, type the location of the server.

   These text boxes are optional.
5. If you are using an FTP or HTTP server instead of a shared directory, under Login, do the following:
   - In the Name text box, type the name of the FTP or HTTP server.
   - In the Password text box, type the password for the FTP or HTTP server.
6. Under Connection, in the URL or IP Address text box, type the UNC path to your shared directory, or the URL or IP address for your FTP or HTTP server.
7. In the Type text box, select one of the following:
   - LAN
   - FTP
   - HTTP
8. On the File menu, click **Save As**.
9. In the Save As dialog box, type **Liveupdt.hst** for the file name.

   Save the file to the Desktop or some place where you can easily locate it.

   Do not save the Liveupdt.hst file to the \Programs\Symantec\LiveUpdate folder on the LuAdmin computer.

10 Copy the Liveupdt.hst file that you created to the C:\Program Files\Symantec\LiveUpdate folder on each client.

11 Copy the S32luhl1.dll file to the same directory on all clients if it does not already exist.

This file is in the C:\Program Files\LiveUpdate Administration Utility folder on the computer on which the LiveUpdate Administration Utility folder is installed.

When LiveUpdate is started on the client computer, it retrieves updates from the local LiveUpdate server.

Running LiveUpdate from a command line or scheduler

You can run a silent LiveUpdate session for Symantec AntiVirus 8.x clients from a command line or a scheduler.

To run LiveUpdate from a command line or scheduler

- Type **vpdn_lu.exe** with the following parameters:
  - /s: Retrieves definitions and product updates in silent mode
  - /fUpdate: Filters out product updates
  - /fVirusdef: Filters out definitions updates

For example, you would type:

- vpdn_lu.exe /fUpdate /s
  to retrieve virus definitions silently.
- vpdn_lu.exe /fVirusdef /s
  to retrieve product updates silently.
- vpdn_lu.exe /s
  to retrieve product updates and definitions silently.

Note: LiveUpdate does not display error messages when it runs in silent mode. If LiveUpdate fails, you are not notified.

Chapter 5

Troubleshooting the LiveUpdate Administration Utility

This chapter includes the following topics:

Using LiveUpdate client configuration files

The configuration information for LiveUpdate clients version 1.6x and later is in the \Downloads\ folder and in the following files:

- Product.Catalog.LiveUpdate
- Log.LiveUpdate
- Settings.LiveUpdate

Up to ten copies are kept of the Product.Catalog.LiveUpdate, Log.LiveUpdate, and Settings.LiveUpdate files. As each of these files is overwritten, the previous version is saved with a prefix indicating the backup number. For example, 2.Settings.LiveUpdate indicates that this is the second backup of the Settings.LiveUpdate file. When the number of backups reaches ten, the oldest is deleted. The number of backups that are kept is configurable under the Preferences section of the Settings.LiveUpdate file.

You may use the information within these files to determine the causes of LiveUpdate download failures and to verify LiveUpdate client settings.

{LiveUpdate Data}\Downloads\

The {LiveUpdate Data}\Downloads\ directory contains downloaded LiveUpdate packages, which are decompressed into separate folders and applied. With the exception of Livetri.zip and partial downloads, this directory is cleared at the end of each successful LiveUpdate session.

If the LiveUpdate session was not completed successfully, and your LiveUpdate connection uses HTTP, the information in this directory is used to attempt to resume the download.

Product.Catalog.LiveUpdate

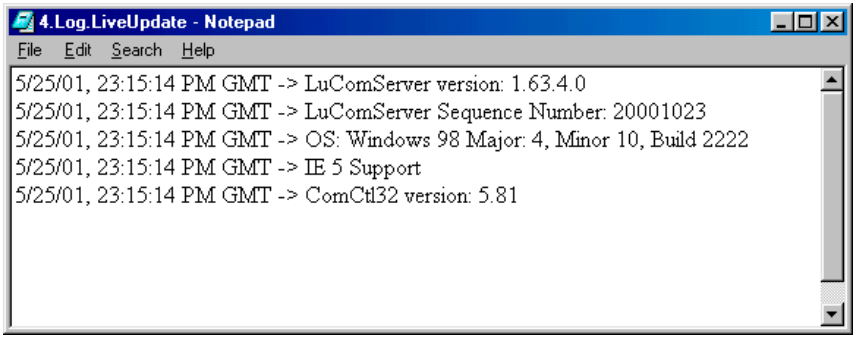
The Product.Catalog.LiveUpdate file is used internally by LiveUpdate to list the Symantec products that are installed on the computer and the current patch level of each product. It should not be edited.

Log.LiveUpdate

LiveUpdate creates a log file, Log.LiveUpdate, each time it runs. Up to ten copies of the log are kept to assist in troubleshooting. The log file is located in the Application Data\Symantec\LiveUpdate folder. At the beginning of each log is information about the version of LiveUpdate that is running, and information

about the computer on which it is running. Logging is enabled by default. You can open the log file using a text editor such as Notepad as shown in Figure 5-1.

Figure 5-1 Log.LiveUpdate file



Settings.LiveUpdate

Settings.LiveUpdate contains all of the LiveUpdate configurations, including download resumption information, host entries, LiveUpdate settings, and merge indicators. Table 5-1 lists the possible settings and describes how they are used.

Table 5-1 Settings.LiveUpdate settings

Setting	Description
INSTALL_FOLDER	This setting shows where LiveUpdate is installed.
SETTINGS_FILE	The settings file contains the full path to the Settings.LiveUpdate file (by default, in the \Symantec\LiveUpdate folder).

Table 5-1 Settings.LiveUpdate settings

Setting	Description
MERGE_FILE_LOCATION	This setting contains the full path to the location to search for a LiveUpdate.Settings.Merge file. This setting can contain a folder to look for the LiveUpdate.Settings.Merge file, or it can be a full path and file name to use. If this setting is not present (or it is empty), the file is looked for in the location indicated by the value of the INSTALL_FOLDER setting. After a normal load of the Settings.LiveUpdate file, if the LiveUpdate.Settings.Merge file is present, its contents are loaded over the default settings. Once loaded, the file is deleted. When the settings are saved, the changes from the merge file are saved as the default settings.
MERGE_FILE_NO_DELETE	This setting is used to control whether or not the merge file is deleted once it is processed. By default (and if this setting is not present or if it is empty), if a merge file is found and loaded, it is then deleted. Setting this property to a nonempty value prevents the file from being deleted once it is loaded. This may be useful if the settings point to a shared file on a network that is used as a global settings merge file by everyone every time that LiveUpdate runs.
NEW_HOSTS_LOCATION	This specifies the full path to a file containing text-settings format host specifications, or it can contain a path to a folder that should be searched for a file called LiveUpdate.Settings.Hosts (which contains text-settings format host specifications). If this property is not present (or it is empty), the location indicated by INSTALL_FOLDER is searched for the LiveUpdate.Settings.Hosts file. After the settings are loaded normally, a check is done for this file. If found, any existing hosts are deleted from the settings, and the contents of this file are loaded as the new host specifications.

Table 5-1 Settings.LiveUpdate settings

Setting	Description
NEW_HOSTS_NO_DELETE	This controls whether or not the new host file is deleted once it is processed. By default (and if this setting is not present or it is empty), after a host file is found and loaded, it is deleted. Setting this property to a nonempty value prevents the file from being deleted once it is loaded. This may be useful if the settings point to a shared file on a network that is used as a global new hosts file to be used by everyone every time that LiveUpdate runs.
PRODUCT_CATALOG_FILE	This property contains the full path to the Product.Catalog.LiveUpdate file (which should be in the \Symantec\LiveUpdate folder beneath the PER_MACHINE_FOLDER).
PER_USER_FOLDER	The Per User folder as returned from the Shfolder.dll.
PER_USER_ROAMING_FOLDER	The Per User Roaming folder as returned from the Shfolder.dll.
PER_MACHINE_FOLDER	The Per Machine folder as returned from the Shfolder.dll. The location of this directory differs according to the operating system that is installed.

Table 5-1 Settings.LiveUpdate settings

Setting	Description
DOWNLOADS	This setting stores download resumption information. Each file that is downloaded using HTTP gets a setting named after its object name here, followed by a setting name. The Livetri.zip file always has a setting under this key as it is always checked to see if a new download is necessary. Other file information is kept until files are successfully downloaded. If downloads are not successful, this information can be used for download resumption (only available when HTTP is the protocol being used to download updates). An example of a DOWNLOADS entry: DOWNLOADS\LIVETRI.ZIP\CONTENT-LENGTH=676DOWNLOADS\LIVETRI.ZIP\LAST-MODIFIED=Tue, 28 Dec 1999 04:44:04 GMTDOWNLOADS\LIVETRI.ZIP\LOCALPATH=C:\WINNT\Profiles\All Users\Application Data\Symantec\LiveUpdate\Downloads\livetri.zipDOWNLOADS\LIVETRI.ZIP\SERVER=ussm-greendude.symantec.comDOWNLOADS\LIVETRI.ZIP\SERVERPATH=/liveupdate2/livetri.zipDOWNLOADS\LIVETRI.ZIP\STATUS=Complete
PREFERENCES	This setting contains general settings.
WORKINGDIRECTORY	This is used for download resumption and during normal file downloads to specify where to store temporary files.
USEPASSIVEFTPMODE	This entry switches LiveUpdate to passive mode FTP (the default setting on a clean installation). Passive FTP is more successful with some firewall configurations. If this value is nonzero, LiveUpdate uses passive FTP. If it is zero or does not exist, then LiveUpdate uses active FTP.

Table 5-1 Settings.LiveUpdate settings

Setting	Description
ALL TRANSPORTS AVAILABLE	This setting allows an override of the default rule to only allow LAN/UNC hosts if the LAN HAL DLL is present. There is no longer a LAN HAL. When converting from an old installation, the PREFERENCES_LAN_HAL_PRESENT setting is created if a previous LAN HAL is detected. The value of this setting is 0 if false, and 1 if true.
LAN_HAL_PRESENT	This setting is created during installation when converting from an earlier version of LiveUpdate. It is also created if the distribution of a LAN HAL to the client computer in a corporate environment that uses a legacy version of LuAdmin is detected. If the S32luhl1.dll is found in the installation folder, this setting is created. The value of this setting is not important because all that is checked for is a nonempty value.
NON_SYMANTEC_HOST	This setting is created when at least one host entry contains the property IS_SYMANTEC=NO. It is checked every time that the host information is loaded (from any source). The presence of this setting is used to detect corporate mode.
LOGEVENTS	If this setting is nonzero, events are logged to the file indicated in the PREFERENCES_LOG_FILE_NAME setting.
LOG_BACKUPCOUNT	If this setting is nonzero, it specifies the number of log file backups that will be kept on a rotating basis. As each new log file is created, the existing log files are rotated down with the oldest one (highest number) being deleted. The default is 10.
PRODUCT_CATALOG_ BACKUPCOUNT	If this setting is nonzero, it specifies the number of Product.Catalog.LiveUpdate file backups that are kept on a rotating basis. As each new Product.Catalog.LiveUpdate file is saved, the existing backup files are rotated down with the oldest one (highest number) being deleted. The default it 10.

Table 5-1 Settings.LiveUpdate settings

Setting	Description
SETTINGS_FILE_ BACKUPCOUNT	If this setting is nonzero, it specifies the number of Settings.LiveUpdate file backups that are kept on a rotating basis. As each new Settings.LiveUpdate file is saved, the existing backup files are rotated down with the oldest one (highest number) being deleted. The default is 10.
LOG_FILE_NAME	This setting contains the full path to the log file. If LOGEVENTS is on, events are logged to the file indicated in this property's value. If this property is not set, but LOGEVENTS is on, this property's default value is set to Log.LiveUpdate with the PER_MACHINE_FOLDER as the path. The file is overwritten each session.
INTERNET CONNECTION	This setting determines remote access server (RAS) characteristics. Values are numeric (DWORD). A value of 0 means to use IE settings (if IE is configured to use a RAS, it will be used, and so on). A value of 2 means to silently dial the LiveUpdate-specific settings specified in the RAS settings.
UIRUNONCE	The first time the user interface runs, the user can view the connection settings for RAS and proxy. Set this value to 0 to force the connection settings window to reappear.
CORPORATE_MODE	Corporate mode preferences are set when an LuAdmin environment is detected. Corporate mode is indicated when this string is present and set to any value. If this setting is absent or set to an empty value, corporate mode is not being used. Corporate mode is true if the LAN HAL is present, or if there is a non-Symantec host entry present. There are separate settings indicating these two conditions, and they may be used instead. At this time, corporate mode is automatically set if at least one of these conditions is true. This is used to determine if the URL= Tri entry property should be obeyed. If in corporate mode, it is not, unless CORPORATE_ALLOWED_URL_HOSTS is active.

Table 5-1 Settings.LiveUpdate settings

Setting	Description
CORPORATE_ALLOWED_ URL_HOSTS	This value sets whether URL hosts can connect when corporate mode is active. It can be one or more of the following strings: LAN, HTTP, or FTP. If more than one is specified, use commas to separate them.
SELECTEDRAS	If RAS_USE_IE_RAS exists and is set to a non-empty value, then the settings for a custom RAS are ignored. If RAS_USE_IE_RAS doesn't exist, or if it is set to an empty value, then the custom RAS settings as indicated by RAS_SELECTEDRAS are used.
USERNAME PASSWORD	The property names for the user name and password of a given RAS have to be constructed, as they are under PREFERENCES\RAS\<RAS NAME>\USERNAME:ENC and PREFERENCES\RAS\<RAS NAME>\PASSWORD:ENC. <RAS NAME> represents the descriptive name of the RAS entry to which the user name and password apply.
USE_HTTP_PROXY USE_FTP_PROXY	These can be set to activate proxies.
USE_IE_PROXY	USE_IE_PROXY causes LiveUpdate to use the proxy settings (if any) specified in the IE control panel. This is the default on a clean computer.
AUTHORIZATION	The PREFERENCES\PROXY\AUTHORIZATION setting's value is used in a proxy-authorization HTTP header sent in an InternetOpenUrl() request for FTP transfers. A proxy-authorization header has the form: proxy-authorization: scheme login:password, where scheme is Basic, NTLM, and so on, and login:password is UUEncoded.
HTTPAUTHORIZATION	The PREFERENCES\PROXY\ HTTPAUTHORIZATION is used similarly to PREFERENCES\PROXY\AUTHORIZATION, but for HTTP proxy-authorization headers.
HOSTS	This setting contains host file information.

Table 5-1 Settings.LiveUpdate settings

Setting	Description
NUM_HOSTS	This setting shows the number of host entries listed.
NAME	This setting is used for display purposes. It shows to which host a connection is attempted.
TYPE	TYPE can be FTP, HTTP, or LAN. (Modem is no longer supported and modem entries are ignored.)
ACCESS	This setting usually contains the portion of the URL that is beyond the protocol specifier. For example, for an FTP host with a fully qualified URL of ftp://update.symantec.com/liveupdate, the Access property's value would be update.symantec.com/liveupdate while the Access2 property's value would be ftp://update.symantec.com/liveupdate.
ACCESS2	This always contains the fully qualified URL of the host.
LOGIN:ENC PASSWORD:ENC	These settings contain the Login and Password (if any) used to connect.
SUBNETSUBNETMASK	When selecting hosts, the current IP address is masked with the subnet mask and the result is compared with the value of the subnet property of the current host entry. If they match, that host is used. Otherwise, it is skipped. A zero value for both subnet and subnet mask will always match every IP address.
IS_SYMANTEC	This setting determines if the server is a Symantec server or not. Of primary importance to determining if the password should be shown in LuAdmin.
HOST_NUMBER	This setting contains the identifier of the host.

Note: The LAN HAL (S32luhl1.dll) is a legacy file transport method that lets LiveUpdate retrieve files from a specific location using a UNC path. You should not use this method for NT workstations and servers. If you use the Norton Program Scheduler, LiveUpdate will not be able to connect to a UNC location unless the LiveUpdate files reside in a shared resource on the NT server that all users are authorized to access (a NULL share).

Understanding corporate mode settings

When LiveUpdate 1.6 or later is installed on a computer meeting either of the following criteria, it activates a condition called corporate mode:

- A custom host file (Liveupdt.hst) is detected on the computer in the LiveUpdate program files location.
- A LAN HAL (S32luhl1.dll) exists from a version of LiveUpdate earlier than 1.6 in the LiveUpdate program files location.

While in corporate mode, LiveUpdate behavior changes in two ways. First, it does not attempt to use the URL= line in the TRI file to download a file. This circumvents the possibility of LiveUpdate attempting to go through the firewall when downloading. You can modify this setting by changing the CORPORATE_ALLOWED_URL_HOSTS setting in the Settings.LiveUpdate file. For example:

CORPORATE_ALLOWED_URL_HOSTS=HTTP

Second, LiveUpdate will not continue trying to connect to Symantec hosts if the internal entries fail. To change this behavior and allow access to all hosts (for example, during server failure), you may add the following setting to the Settings.LiveUpdate file:

ALL TRANSPORTS AVAILABLE=YES

With this value in place, LiveUpdate continues to attempt a connection to the first host entries, but if the connection fails, it uses an Internet connection to connect to Symantec servers. This is useful for environments in which the corporate LiveUpdate server is not always available.

Understanding LiveUpdate 1.7 package authentication

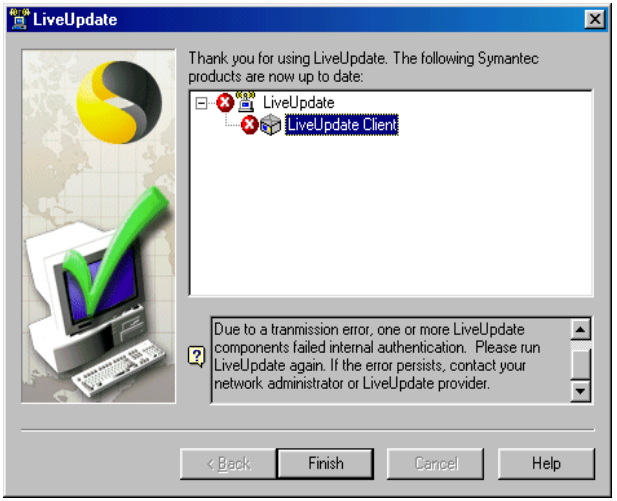
LiveUpdate 1.6x and 1.7 secure the download process by checking file signatures before delivering any LiveUpdate content to the user. In addition, LiveUpdate 1.7 secures and authenticates downloaded packages to each client, server, and gateway.

Each new update is accompanied by a cryptographic signature, which is then signed using a private key that is stored on a secure Symantec server. The resulting digital signature is stored in a signature file, which is compressed into the Livetri.zip file along with the catalog file.

If any of the authentication checks fail, a descriptive error message appears and the activity is recorded in the log file. On Windows NT computers, an error is also written to the NT event log.

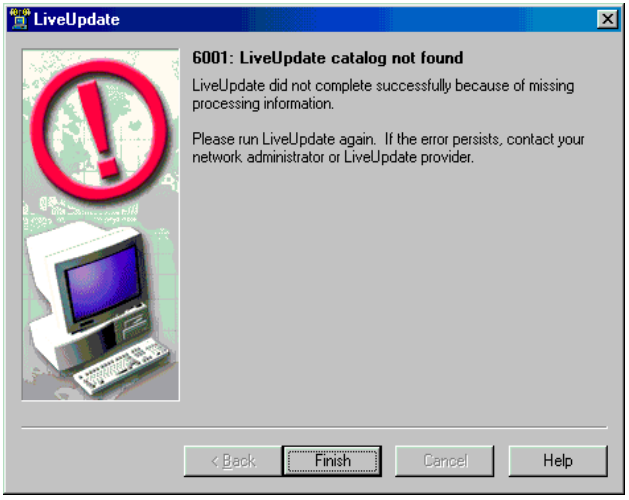
If you download a LiveUpdate package that cannot be authenticated, or if a replication error occurs when a newer update is made available, you will see the error message in Figure 5-2. In this case, you must wait one to two hours before running LiveUpdate again.

Figure 5-2 Package authentication error



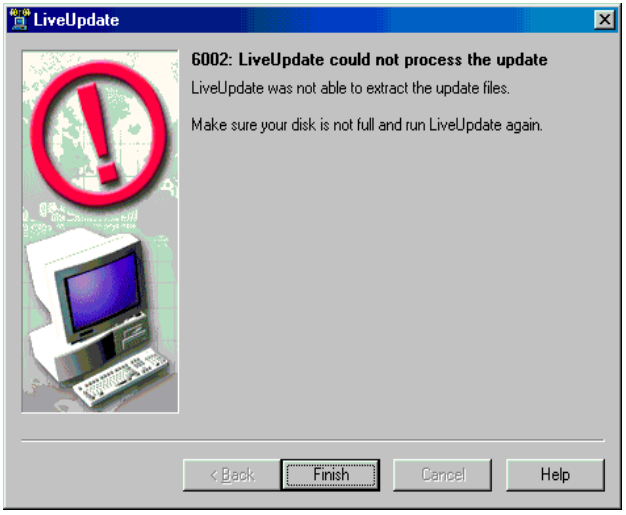
If the TRI file cannot be authenticated, you will see the error message in Figure 5-3.

Figure 5-3 TRI file authentication error



If LiveUpdate downloads a corrupted catalog file, you will see the error message in Figure 5-4. Ensure that the hard disk is not full. If it is not full, the LiveUpdate server may have been updated while you were downloading. Wait an hour, and then run LiveUpdate again.

Figure 5-4 Corrupted catalog file error



Index

I

L

M

N

P

R

S

T

U

W