LiveUpdate™ Administrator's Guide

LiveUpdate™ Administrator's Guide

Documentation version 2.5

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 for those customers enrolled in the Platinum Support Program
- 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.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- 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 (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Symantec License and Warranty
LiveUpdate™ Administrator's Guide

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "ACCEPT" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT ACCEPT" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND CONTACT SYMANTEC CUSTOMER SERVICE FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the property of Symantec, or its licensors, and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, You may make the number of copies of the Software licensed to You by Symantec as provided in Your License Module. Your License Module shall constitute proof of Your right to make such copies;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and
E. use the Software in accordance with any additional permitted uses set forth below.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;
G. use the Software in any manner not authorized by this license; nor
H. use the Software in any manner that contradicts any additional restrictions set forth below

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You;

provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

There are technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures to protect Symantec against software piracy. This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a computer to not more than a finite number of times for a finite number of computers. This License and the Software containing enforcement technology require activation as further set forth in the documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation, You will provide Your unique product key accompanying the Software and computer configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the documentation, or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event that You are not able to activate the Software over the Internet, or through any other method specified during the activation process, You may contact Symantec Customer Support using the information provided by Symantec during activation, or as may be set forth in the documentation.

4. Sixty Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes) at any time during the sixty (60) day period following the date of purchase.

5. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

6. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

7. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items,” as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and

other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

8. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. You agree to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

9. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

ACKNOWLEDGEMENTS

The Apache Software License, Version 1.1
Copyright (c) 1999, 2000 The Apache Software Foundation. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgement: “This product includes software developed by the Apache Software Foundation <http://www.apache.org/>.” Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear.
4. The names “The Jakarta Project”, “Tomcat”, and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <apache@apache.org>.
5. Products derived from this software may not be called “Apache” nor may “Apache” appear in their names without prior written permission of the Apache Software Foundation.
THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>. This product includes software developed by the Apache Software Foundation (http://www.apache.org/), namely Tomcat, Xerces, and Apache XML-RPC. A copy of the license may be found at www.apache.org/LICENSE. Copyright © 2000 The Apache Software Foundation. All rights reserved.

Copyright (c) 2001-2002, The HSQL Development Group All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
Neither the name of the HSQL Development Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HSQL DEVELOPMENT GROUP, HSQLDB.ORG, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Ultimate Technology, Inc. Open Source License, Version 1.1. Copyright (c) 1999-2003 Ultimate Technology, Inc. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgement: “This product includes software developed by Ultimate Technology, Inc. (http://www.UltimateTech.com/).” Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear.
4. Ultimate Technology and product names such as Ultimate Console may not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact info@UltimateTech.com.
5. Products derived from this software may not be called “Ultimate” nor may “Ultimate” appear in their names without prior written permission of Ultimate Technology, Inc.
THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Portions of this software are based upon other open source products and are subject to their respective licenses.

Contents

Chapter 1

Introducing the LiveUpdate Administration Utility

This chapter includes the following topics:

About LiveUpdate

LiveUpdate is the Symantec technology for automatically updating Symantec virus definitions and products. The LiveUpdate client is included with each Symantec product and is installed automatically. Periodically, the LiveUpdate client connects to a LiveUpdate server to check for new updates that apply to the Symantec products that are installed on the computer. If any updates are found, the LiveUpdate client prompts the user to download and install the update.

Downloading virus definitions and program updates usually requires a paid subscription, but the updates are included in many corporate contracts.

Symantec and Central LiveUpdate servers

LiveUpdate offers the option to use either a Symantec LiveUpdate server or, for host computers that are connected to a private network, an internal Central LiveUpdate server. Each LiveUpdate client can be configured separately to use either server. When a Symantec server is used, LiveUpdate clients connect using HTTP or FTP to a server that is located at a Symantec LiveUpdate site. If an internal Central LiveUpdate server is used, clients communicate with it for new updates.

Using a Central LiveUpdate server means that clients do not need to connect to an external network for virus definitions and product updates. This reduces the LiveUpdate traffic between the local network and Symantec LiveUpdate sites. In addition, using a Central LiveUpdate server gives you control over the types of updates that are available to users, and supports the use of Custom Content publishing, a new feature in LiveUpdate.

See "About LiveUpdate custom content publishing" on page 105.

When you configure a Central LiveUpdate server, the LiveUpdate Administration Utility (LuAdmin) performs the following tasks:

- Selects the Symantec products and languages for which updates will be downloaded
- Provides the full path to the directory in which downloads will be stored
- Retrieves all of the update packages and related index files from the Symantec LiveUpdate site that apply to the selected products

The LiveUpdate Administration Utility stores all of the downloaded update packages and index files on the local server. After the updates are initially retrieved, LuAdmin checks with the Symantec LiveUpdate site for new update packages and automatically retrieves and stores them in the designated directory.

You may want to set up the Central LiveUpdate server on a separate computer from the LiveUpdate Administration Utility. New updates can then be tested before they are moved to the Central LiveUpdate server.

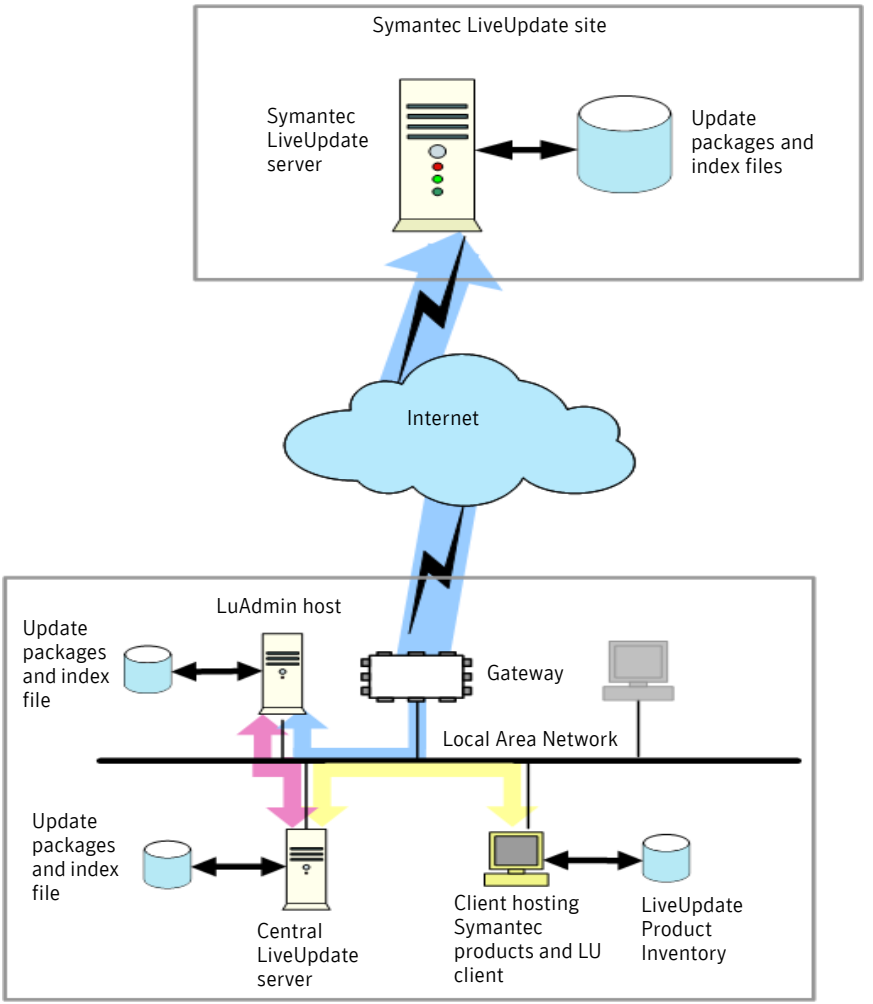
Once the Central LiveUpdate server has been configured, you can use LuAdmin to establish communication with client computers on the network. You can select the HTTP, FTP, or LAN transport method, and then create a LiveUpdate host file based on your selection. The host file contains the information that is needed by the client to connect to the Central LiveUpdate server.

The host file is then distributed to each of the clients on the network. Depending on the time interval that has been set, each LiveUpdate client periodically connects to the Central LiveUpdate server and checks for new updates.

Applicable updates are automatically downloaded from the Central LiveUpdate server and installed on the clients.

Figure 1-1 shows a typical network using a Central LiveUpdate server.

Figure 1-1 Network using a Central LiveUpdate server



The LiveUpdate Administration Utility

The LiveUpdate Administration Utility (LuAdmin) maintains a local LiveUpdate repository for product and virus definitions updates. It checks with an external Symantec LiveUpdate site at frequent intervals for new updates and downloads the updates that apply to the Symantec products that are installed on the local network.

The LiveUpdate Administration Utility is typically installed on one computer on the network. The LiveUpdate Administration Utility does not need to be installed on the same server that is used as the Central LiveUpdate server. You can periodically move the update packages and their associated index files from the LiveUpdate Administration Utility host to the Central LiveUpdate server, based upon schedules and protocols that you determine, which replaces the packages and index files that were previously on the computer.

What's new in LiveUpdate

LiveUpdate (Win32) version 2.5 includes the following new enhancements and features:

SESA™ integration	LiveUpdate clients are integrated with Symantec Enterprise Security Architecture (SESA) if the SESA Agent is running. This lets you define and propagate settings for LiveUpdate clients across an entire network using the Symantec management console. See "About LiveUpdate and SESA" on page 79.
Improved Automatic LiveUpdate notification	LiveUpdate clients display a small dialog box above the system tray that prompts you to run LiveUpdate. The dialog box is displayed until you click Yes or No to run the update.
Host file integrity check	LiveUpdate attempts to prevent possible Denial of Service (DoS) by searching for Symantec LiveUpdate entries in the Windows host files. The presence of these entries may indicate Trojan horse or virus activity. If they are found, you are given the option of deleting the entries, or retaining them if they are valid. The host file integrity check setting is in the Settings.LiveUpdate file. See "About LiveUpdate client configuration files" on page 63.
New PreCondition	The new PreCondition GetProductPropByMoniker queries the properties set in the Product Inventory. You can use the PreCondition GetProductPropByMoniker when you want to target all language versions of a particular product. See "Using PreConditions" on page 139.

Support for WinRAR compression

Support has been added for LiveUpdate packages that are compressed with RAR. LiveUpdate attempts to decompress the file using RAR, and if that fails, it attempts to unzip it. If both attempts fail, LiveUpdate reports an error and does not process the update.

DIS script logging

The DIS engine is enhanced to log verbose information for all the commands that are currently supported.

The following information is logged:

- Errors
- Start
- End
- Parameters

For example, when a Delete DIS primitive is processed and fails, the following is logged:

```
DIS - DELETE ("c:\somedir\somefile") <BEGIN>
DeleteFile failed with error 0x2
DIS - DELETE (0x802A0026) <END>
```

New installation versions

LiveUpdate includes the following new installation versions:

- Lusetup.exe is the package for the Web-based installer and contains both the LiveUpdate base files and the LiveUpdate SESA integration files.
- Lusetup-lt.exe is also used for Web-based installations, but contains only the LiveUpdate base files.

See "About LiveUpdate client files" on page 60.

Last known good inventory

LiveUpdate will attempt to roll back to a last known good inventory file when it detects a corrupt Product Inventory. The setting is PREFERENCES\PRODUCT_INVENTORY_INTEGRITY_CHECK.

The following conditions trigger a roll back:

- LiveUpdate is unable to unobfuscate the current Product Inventory due to corruption.
- The Product Inventory was not found.
- The only command lines registered in the Product Inventory are the ones owned by LiveUpdate. In this scenario, the InstalledApps regkey is first checked to determine if any Symantec applications are installed.

See "Settings.LiveUpdate" on page 64.

Time-out settings	LiveUpdate has new settings to specify values for connect and data read Internet options. Each setting is read at initialization time, and is processed as a DWORD. The unit of measurement is in seconds. The default setting for each value is 30 seconds. The minimum value is 5 seconds. The new settings are as follows: ■ PREFERENCES\INTERNET_CONNECT_TIMEOUT ■ PREFERENCES\INTERNET_READ_DATA_TIMEOUT See "Settings.LiveUpdate" on page 64.
Technical support integration	LiveUpdate has enhanced error support codes to help you identify and resolve error conditions in LiveUpdate. When an error occurs, the error message includes a link to the corresponding article in the Symantec Technical Support Knowledge Base.

Components of LiveUpdate

Table 1-1 lists the LiveUpdate components and their functions.

Table 1-1 LiveUpdate components

Component	Function
LiveUpdate client	The LiveUpdate client is automatically installed on every computer that has a Symantec product installed. The LiveUpdate client handles checking for, downloading, and installing available updates for all Symantec products on the computer. See "Upgrading the LiveUpdate client" on page 59.
LiveUpdate Administration Utility (LuAdmin)	The LiveUpdate Administration Utility is typically installed on one computer on the network. LuAdmin maintains a local and up-to-date repository of product and virus definitions updates, and their related index files, that is used by other computers on the network. LuAdmin periodically checks for and downloads new updates. See "How the LiveUpdate Administration Utility works" on page 24.

Table 1-1 LiveUpdate components

Component	Function
Symantec LiveUpdate server	A LiveUpdate server is located at one of the LiveUpdate sites maintained by Symantec. When a Central LiveUpdate server is not used, clients communicate directly with a Symantec LiveUpdate site to check for new virus definitions and program updates. When a Central LiveUpdate server is used, only the computer running LuAdmin communicates with a Symantec LiveUpdate server. See "Symantec and Central LiveUpdate servers" on page 14.
Central LiveUpdate server	A Central LiveUpdate server is on an internal network that is used to store LiveUpdate packages and index files. LiveUpdate clients direct their requests for updates to this server, instead of communicating with a server that is located at a Symantec site. Normally, an FTP, HTTP, or HTTPS server is used, but a standard network server may also be used. Periodically, you may want to transfer new update packages and index files from the LiveUpdate Administration Utility to the Central LiveUpdate server. See "Setting up a Central LiveUpdate server" on page 34.

LiveUpdate product and index files

LiveUpdate uses the following files to maintain catalog and index information:

Client Product Inventory	A file that must exist on each computer where the LiveUpdate client is installed. The Client Product Inventory is maintained and used by the client. It contains information about each Symantec product that is installed on the client, including product indentifiers, version numbers, language, release date sequence numbers, and other product attributes.
Update Index (xxxxtri.zip)	A compressed file that is sent by the LiveUpdate server to the client in response to a request for new updates. This file is comprised of the Update Index file, a Symantec signature, and a guard file. The Update Index file contains an index entry, or specification, for every update package that is available on the server (whether it is a Symantec server or a Central LiveUpdate server). These entries contain the same information that is in the Client Product Inventory.
Update Package	A set of files that contain the update content that is to be installed on the client. There is one Update Package for each update that is listed in the Update Index file. The signature and guard files that are sent with the xxxxtri.zip file are used to authenticate the Update Package and ensure that it has been delivered without modification.
All Products List (Products.xml)	A file that contains basic product identifiers and attributes for every product that uses LiveUpdate. This file is used by LuAdmin to generate the list from which users can select the product versions and language versions. This file is refreshed each time that LuAdmin performs an update operation.

The LiveUpdate Administration Utility and LiveUpdate client have additional files.

See "LiveUpdate Administration Utility files" on page 28.

See "About LiveUpdate client configuration files" on page 63.

How LiveUpdate works

When you start LiveUpdate, it displays a list of the registered Symantec products that are 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 finds and connects to either an external Symantec server or an internal Central LiveUpdate server that has been set up by an administrator using the LiveUpdate Administration Utility.

LiveUpdate operates in either Interactive or Express mode. In Interactive mode, LiveUpdate downloads a list of updates available for your Symantec products. You can then choose which updates to install. If you run LiveUpdate in Express mode, LiveUpdate automatically installs all the updates for your Symantec products.

How clients are updated when using a Symantec LiveUpdate server

The following steps are performed when a client uses a Symantec LiveUpdate server for its updates:

Start up	The LiveUpdate client performs an update check periodically, based on a time interval setting that you define for the client. When LiveUpdate is started on the client, the local Client Product Inventory, which lists all of the Symantec products that are installed on the client, is read.
Request Update Indexes	For each Symantec product that is installed, there is an entry in the Client Product Inventory that contains the name of the Update Index file in which the updates are listed. The client collects the Update Index file names and sends a request to the LiveUpdate server for these files to be downloaded to the client.
Check Update Indexes	When the Update Index files have been received by the client, the client checks each of the products in the local Client Product Inventory against its index file to see if there are any new updates available for it. If a match is found, the corresponding Update Package is added to the list of updates to retrieve.

Update Package Request	After each product in the Client Product Inventory has been checked against its Update Index, the client checks the list of updates. If the list is empty, the LiveUpdate operation is immediately terminated on the client. If there are Update Packages listed, they are automatically downloaded using the default Express mode setting. If Interactive mode is enabled, the client displays the list and prompts the user to select the updates to be downloaded. If the user selects one or more of the updates, a request is sent to the LiveUpdate server for them. If the user declines all of the updates, the LiveUpdate operation is terminated.
Update Package Installation	When the Update Packages have been downloaded, the client verifies that the updates match those that were initially requested, and that they have been delivered without modification. Each Update Package is then installed on the local computer. Following the installation, the local Client Product Inventory is updated.
Update completion	The update operation is terminated.

How clients are updated using a Central LiveUpdate server

The following steps are performed when a client uses a Central LiveUpdate server for its updates:

Start up	The LiveUpdate client performs an update check periodically, based on a time interval setting that you define.
Request Update Indexes	The client sends a request to the Central LiveUpdate server for the Update Index file (xxxxtri.zip).
Check Update Indexes	When the client has received the Update Index file, it checks each of the products in its local Client Product Inventory against the Update Index file to see if there are any new updates available. If a match is found, the corresponding Update Package is added to the list of updates to be downloaded.

Update Package Request	After each product in the Client Product Inventory has been checked against its Update Index file, the client checks the list of updates. If the list is empty, the LiveUpdate operation is immediately terminated on the client. If there are Update Packages listed, they are automatically downloaded using the default Express mode setting. If Interactive mode is enabled, the client displays the list and prompts the user to select the updates to be downloaded. If the user selects one or more of the updates, a request is sent to the LiveUpdate server for them. If the user declines all of the updates, the LiveUpdate operation is terminated and no updates are downloaded.
Update Package Installation	When the Update Packages have been received, the client authenticates the sender and verifies that the packages have been delivered without modification. Each Update Package that is accepted by the client is installed on the local computer. Following each installation, the local Client Product Inventory is updated to reflect the package that was installed.
Update completion	The update operation is terminated.

You can configure a LiveUpdate host file for LiveUpdate clients version 1.6x and later so that they can download updates from the closest internal LiveUpdate server. This typically results in decreased download times. You can also configure the host file to use an external LiveUpdate server.

See "Creating a LiveUpdate host file for clients" on page 36.

LiveUpdate clients version 1.7x and later perform additional authentication and error checking. Descriptive warnings and error messages assist in troubleshooting LiveUpdate failures.

See "Understanding LiveUpdate package authentication" on page 74.

How the LiveUpdate Administration Utility works

The LiveUpdate Administration Utility (LuAdmin) has its own update checking and retrieval operation. This operation is similar to the one that is performed by the client. However, there are important differences.

The following steps are performed when LuAdmin is updated:

Start up	The LiveUpdate Administration Utility performs an update check periodically based on its time interval setting.
Request Update Indexes	The LiveUpdate Administration Utility sends a request to a Symantec LiveUpdate server for the Update Index file (xxxxtri.zip) to be retrieved.
Check Update Indexes	When the LiveUpdate Administration Utility receives the Update Index file, it checks each product in its Product Inventory against it to see if there are any new updates available. The Product Inventory for LuAdmin contains not only Symantec products that are installed on the computer on which LuAdmin is installed, but also those for which updates are being maintained on behalf of the other computers on the network. If a match is found, the corresponding Update Package is added to the list of updates to be downloaded.
Update Package request	After each product in the Client Product Inventory has been checked against the Update Index file, LuAdmin checks the list of updates to be requested. If the list is empty, LuAdmin skips to the Retrieve Product List operation immediately. If the list is not empty, LuAdmin sends a request to the Symantec LiveUpdate server for the selected Update Packages.
Store Update Packages	When the Update Packages that were ordered have been received, the client authenticates the sender and verifies that the packages have been delivered without modification. Each Update Package that is accepted by the client is stored on the local computer. The Client Product Inventory is updated to reflect the stored packages.
Create new local Update Index	Using the Update Index file that was received from the Symantec LiveUpdate server earlier as a starting point, LuAdmin creates an Update Index for the local network by eliminating entries for products that are not supported by the Central LiveUpdate server. At the same time, the new Update Index file is compared to the previous Update Index. Any Update Packages that were listed in the old index, but are not included in the new index, are deleted.

Retrieve Product List	LuAdmin requests the Product List from the Symantec LiveUpdate server. This file is stored locally and is used to set download options, specifically to select products and language versions to be supported on the Central LiveUpdate server.
Update completion	The update operation is terminated.

LuAdmin and Central LiveUpdate

The LiveUpdate Administration Utility continues to update its cache of update packages periodically using the download settings that you defined for it. On most networks, you can perform some type of testing and acceptance process on new update packages. Then you can copy the update packages, and the new Update Index file, from the computer that is hosting LuAdmin to the Central LiveUpdate server.

You can use LuAdmin to manage update retrieval and storage operations on a continuing basis, including the following:

- Add and delete Symantec products and languages for which update packages are retrieved and made available on the Central LiveUpdate server.
- View and manage the local LiveUpdate repository of Symantec product and virus definitions updates and related files.
- Set the time intervals for checking the Symantec LiveUpdate site for new updates.
- View, add, delete, and manage custom content Update Packages that are stored on the Central LiveUpdate server and related index information.
- View and manage the LiveUpdate event log.

What you can do with the LiveUpdate Administration Utility

Using the LiveUpdate Administration Utility (LuAdmin), you can set up and manage a Central LiveUpdate server. The Central LiveUpdate server can be either an intranet HTTP, HTTPS, or FTP server, or a directory on a standard file server. Once a Central LiveUpdate server is set up, you can use LuAdmin to create configuration files for LiveUpdate clients so that they send their LiveUpdate requests to the Central LiveUpdate server rather than to an external Symantec LiveUpdate site.

Note: The LuAdmin host file editor only supports FTP, HTTP, and LAN. If you want to point to an HTTPS server, you can create a host file that specifies FTP, HTTP, or LAN and then manually change that setting in the LiveUpdate.Settings file. See "About LiveUpdate client configuration files" on page 63.

You can use the LiveUpdate Administration Utility to perform the following administrative tasks:

- Create a Central LiveUpdate server.
  See "Setting up a Central LiveUpdate server" on page 34.
- Configure LiveUpdate clients to use the Central LiveUpdate server.
  See "Configuring clients to use a Central LiveUpdate server" on page 36.
- Change update retrieval settings.
  See "Changing LiveUpdate Administration Utility retrieval settings" on page 45.
- View Update Packages and other product files.
- View and edit LiveUpdate events.
  See "Working with LiveUpdate events" on page 50.

Where to get more information about LiveUpdate

The Symantec Web site includes information on troubleshooting LiveUpdate and the LiveUpdate Administration Utility, product updates, and knowledge base articles. On the Web, go to www.symantec.com/techsupp/

Chapter 2

Installing the LiveUpdate Administration Utility

This chapter includes the following topics:

Before you install

Before you install the LiveUpdate Administration Utility, you should become familiar with where the set up program installs the software. Make sure that your LiveUpdate clients are updated to the correct version for full compatibility and that your environment meets the system requirements.

The LiveUpdate Administration Utility and LiveUpdate client compatibility

Because of the changes in configuration file locations in LiveUpdate version 1.6x and later, it is important that you use the correct version of the LiveUpdate Administration Utility (LuAdmin) when you manage LiveUpdate client

computers. Table 2-1 lists the versions of the LiveUpdate Administration Utility that you can use with the versions of the LiveUpdate client.

Table 2-1 LiveUpdate version compatibility

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

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

LiveUpdate Administration Utility files

Table 2-2 lists and describes the files that are used by the LiveUpdate Administration Utility.

Table 2-2 LiveUpdate Administration Utility files

File	Description
401comup.exe	Common control update (Comctl32.dll) that is required by LuAdmin.exe. The LuAdmin installer detects if the host computer needs this update. The installer copies the file to the LiveUpdate Administration install folder.
ISLUA.DLL	Custom install and uninstall library.
Lua1d5.rtf	File that describes what's new in the LiveUpdate Administration Utility.
LuAdmin.exe	LiveUpdate Administration Utility program.
LuAdmin.hst	Host file that contains information that is used by LuAdmin to connect to a Symantec LiveUpdate site.
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 and editable in the log file viewer within the LiveUpdate Administration Utility. See "Viewing and deleting events" on page 50.

Table 2-2 LiveUpdate Administration Utility files

File	Description
Luaupdat.exe	Executable file. When the LiveUpdate Administration Utility itself is being updated, this file closes the LiveUpdate Administration Utility, runs LiveUpdate, then relaunches the LiveUpdate Administration Utility. This eliminates the need to restart the computer.
Products.xml	File that contains a comprehensive list of Symantec products. This file is the source of the product information that is displayed by LuAdmin in the Retrieve Updates window, where the product and language versions are selected for the update retrieval operation. Every time that the LiveUpdate Administration Utility checks for updates, the Product List is updated. This file also stores your LiveUpdate Administration Utility preferences. The contents of this file are viewable in the log file viewer within the LiveUpdate Administration Utility. See "Viewing and deleting events" on page 50.
README.TXT	Text file that documents the latest changes to the LiveUpdate Administration Utility, as well as any technical and late-breaking information that is not included in the Administrator's Guide.
S32luhl1.dll	File that is distributed to client computers if the Central LiveUpdate server is set as a UNC path instead of an FTP or HTTP server.
SAMPLE.HST	Host file that is customized by LuAdmin to provide clients with location and method directions for connecting to the internal Central LiveUpdate server.
SilntLuA.exe	Silent LiveUpdate Administrator executable file. See "Retrieving packages automatically" on page 29.
SYMZIP.DLL	LiveUpdate ZIP engine/compression library.
Uninst.isu	File that uninstalls the LiveUpdate Administration Utility.

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

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 5.0 or later
- Pentium 100-MHz processor or faster
- 16 MB RAM
- 25 MB hard disk space (up to 3 GB of additional space for LiveUpdate packages)

For LiveUpdate clients 2.0 and later, the system requirements are as follows:

- Windows 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 or faster
- 16 MB RAM
- 10 MB hard disk space (up to 50 MB of additional space for package downloads depending on the size of the LiveUpdate package)

Installing the LiveUpdate Administration Utility

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

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

To install the LiveUpdate Administration Utility

- Launch luau.exe, and then follow the on-screen instructions.

Post-installation tasks

You can complete the following post-installation tasks: Set up a Central LiveUpdate server.

See “Setting up a Central LiveUpdate server” on page 34.

Updating the LiveUpdate Administration Utility

The LiveUpdate Administration Utility (LuAdmin) can update itself. When the LuAdmin finishes downloading packages, it automatically checks for new LiveUpdate Administration Utility updates and, if one is found, downloads it.

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

To update the LiveUpdate Administration Utility

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. On the Tools menu, click **Update LiveUpdate Administration Utility**.
3. Click **Next** to see the available updates.
4. Click **Finish**.

Uninstalling the LiveUpdate Administration Utility

You can uninstall the LiveUpdate Administration Utility using Add/Remove Programs in the Windows Control Panel.

Chapter 3

Using the LiveUpdate Administration Utility

This chapter includes the following topics:

Starting the LiveUpdate Administration Utility

When you install the LiveUpdate Administration Utility, it creates a shortcut to LuAdmin.exe under the Programs folder.

To start the LiveUpdate Administration Utility

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

Setting up a Central LiveUpdate server

After you have installed the LiveUpdate Administration Utility, you must create and configure a Central LiveUpdate server.

The following steps must be performed:

Set download options.	Using LuAdmin, you first select the Symantec products and languages that you want to download from the Symantec LiveUpdate site and support on the Central LiveUpdate server. You also enter the location on the server in which Update Packages will be stored locally. See "Setting update retrieval options" on page 34.
Download initial updates.	Using LuAdmin, you download all of the available Update Packages, and their related Update Index files, from the Symantec LiveUpdate site for the products and languages that you've selected, and then store them in the location on the host computer that you've designated for that purpose. See "Retrieving Update Packages" on page 35.
Transfer updates to the Central LiveUpdate server.	You copy all of the Update Packages and the Update Index file to the Central LiveUpdate server (LuAdmin is not used to do this).

Setting update retrieval options

You can select products for which to retrieve updates and languages in the following ways:

- Select the primary language that applies to all of the products and then select full product lines.
- Select individual product components and the language versions for each.

You must also designate the directory in which downloaded update packages will be stored.

To set update retrieval options

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. In the LiveUpdate Administration Utility window, in the left pane, click **Retrieve Updates**.
3. In the right pane, under Languages of Updates, select a 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, clicking **Details**, and then checking the Languages and Product Updates to download.
  When you select individual product components to update, you may miss other available updates. For example, new virus definitions files for Symantec 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 in which you want to download updates.
- Click **Browse** and specify a download directory.
  The download directory can be any directory on the server or a directory on the FTP or HTTP server.

Retrieving Update Packages

LuAdmin retrieves the Update Packages and stores them in the directory that was defined in the download settings.

LuAdmin also downloads the Update Index files for the products that are selected and edits them to eliminate index entries for Update Packages that were not selected. These index files include Symtri.zip, Livetri.zip, and Symtri16.zip, as well as Products.xml. These files are required by different versions of LiveUpdate.

To retrieve update packages

1 Start LuAdmin.
See "Starting the LiveUpdate Administration Utility" on page 33.

2 In the LiveUpdate Administration Utility window, in the left pane, click **Retrieve Updates**.

3 In the right pane, click **Retrieve** to begin downloading update packages.

4 Follow the on-screen instructions.

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

See "Working with LiveUpdate events" on page 50.

Configuring clients to use a Central LiveUpdate server

Liveupdt.hst is the host file that controls the LiveUpdate operation on client computers. When a LiveUpdate client is installed, it is configured to use a Symantec LiveUpdate server. To direct LiveUpdate clients to retrieve updates from a Central LiveUpdate server instead, a new host file must be created using LuAdmin, and then distributed to each client computer on the network.

See "Creating a LiveUpdate host file for clients" on page 36.

The host file tells the LiveUpdate client the name and location of the Central LiveUpdate server and how to connect to it. The type of server that is used for the Central LiveUpdate server, FTP, HTTP, or LAN, dictates the type of connection that is used by the client. The name and location information must be consistent with the type of server that is used.

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

Creating a LiveUpdate host file for clients

You can build host files for multiple server types, so that if the client fails in an attempt to connect to a LiveUpdate server, it is directed to another server. FTP, HTTP, and LAN hosts are supported by LiveUpdate.

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

Create a LiveUpdate host file for clients

You can create a host file for the following server types:

- FTP
- HTTP
- LAN

To create a LiveUpdate host file for FTP

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. In the LiveUpdate Administration Utility window, 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 Central LiveUpdate server.
   - Under Country / Area, type the country in which your Central LiveUpdate 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**
     See "Enabling TCP/IP by location" on page 41.
8. In the upper-right-hand side of the window, select one of the following:
   - 32 bit: If you install the 32-bit version, the file names start with S32. This option is selected by default.
   - 16 bit: 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.

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

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 Start LuAdmin.
See "Starting the LiveUpdate Administration Utility" on page 33.

2 In the LiveUpdate Administration Utility window, 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. 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 Central LiveUpdate server.
- Under Country / Area, type the country in which your Central LiveUpdate 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**
  See "Enabling TCP/IP by location" on page 41.

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

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

9 Save the customized file as Liveupdt.hst.

To create a LiveUpdate host file for a LAN

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. In the LiveUpdate Administration Utility window, 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 the 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 who is 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 that contains the LiveUpdate package.

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

   Do not use a UNC location for Windows NT clients and servers. If you use a scheduling utility, LiveUpdate can't connect to a UNC location unless the LiveUpdate files reside in a shared resource on the Windows 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 (luau.exe) and supporting documentation from the Symantec Web site at: http://www.symantec.com/techsupp/files/lu/lu.html
8. On the File menu, click **Save As**.
9. Save the customized file as Liveupdt.hst.

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 the following components:

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

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.

By default, the UNC DLL becomes the exclusive transport when it is present. This prevents users from using FTP when you have specified a UNC path.

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.

To configure LiveUpdate UNC support (LAN transport)

- 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.

Implementing LiveUpdate UNC support

After you create the host file, you must 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.

An issue exists for Windows 95/98 computers that connect to a Windows NT server. Windows 95/98 users must have access rights to the resource. You should not use a UNC location for Windows NT workstations and servers. On LAN connections, LiveUpdate ignores user names and passwords that are 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 that connect to a UNC network location, the user who is logged on to the network must have access rights to the network resource. The user name and password that are 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.

To implement LiveUpdate UNC support

1. Create and distribute a new Liveupdt.hst file.
   See "Creating a LiveUpdate host file for clients" on page 36.
2. Distribute S32luhl1.dll to the workstations.
   This file is in the LuAdmin folder.
3. Create the update retrieval folder.
   See "Retrieving Update Packages" on page 35.

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 enable TCP/IP by location

- 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 that is defined within the host.

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

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	192.168.159.0

Table 3-1 Sample host configuration

Option	Entry
Host entry subnet mask	255.255.255.0
IP address of client workstation	192.168.159.20

The IP address of the client workstation with the subnet mask applied is 192.168.159.0. 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 192.168.155.80 and the subnet mask is applied (resulting in 192.168.155.0), 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 available connection option. 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.

See "Configuring LiveUpdate UNC support (LAN transport)" on page 40.

Retrieving Update Packages automatically

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 the LiveUpdate Administration Utility to select the products to support, the language to use, and the download location.

See "Setting update retrieval options" on page 34.

Once Silent LiveUpdate Administrator exits, the settings are saved and Silent LiveUpdate Administrator uses them every time that it runs.

To retrieve Update 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

Enabling location profiles

LiveUpdate supports the use of multiple connection profiles. A connection profile is a list of hosts that can be used when that profile is selected. This lets users connect to a specific LiveUpdate server depending upon their location. For example, you could set up a profile to be used when a laptop is connected to the LAN and another when it is being used on the road, and a third when the laptop is being used at home.

In the following example, the host list contains three hosts. All three belong to the WORK profile, and the last two also belong to the HOME profile. Since the SET_PROFILE setting is set to HOME, LiveUpdate will only try connecting to the last two hosts. It will connect to HOSTS\1 then HOSTS\2 if it fails to connect to the first one. If SET_PROFILE was set to WORK, then LiveUpdate would try HOSTS\0 -> HOSTS\1 -> HOSTS\2 in that order. The ordering of which host gets used in which order is first determined by the profile selected but also by the ordering of the host in the whole list. Profile ordering within a single host is of no significance.

```
HOSTS\SET_PROFILE=HOME

HOSTS\0\ACCESS=luserver.xyz.com

HOSTS\0\ACCESS2=https://luserver.xyz.com

HOSTS\0\TYPE=HTTPS

HOSTS\0\PROFILE\0=WORK

HOSTS\1\ACCESS=liveupdate.symantec.com

HOSTS\1\ACCESS2=http://liveupdate.symantec.com

HOSTS\1\IS_SYMANTEC=N%9-U,&[>@M

HOSTS\1\TYPE=HTTP

HOSTS\1\PROFILE\0=HOME

HOSTS\1\PROFILE\1=WORK

HOSTS\2\ACCESS=update.symantec.com/opt/content/onramp
```

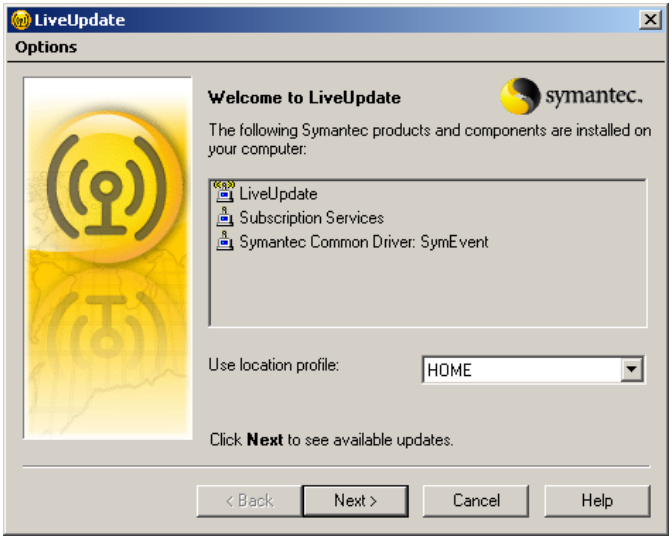
```
HOSTS\2\ACCESS2=ftp://update.symantec.com/opt/content/onramp

HOSTS\2\IS_SYMANTEC=N%9-U,&[>@M

HOSTS\2\TYPE=FTP

HOSTS\2\PROFILE\0=HOME

HOSTS\2\PROFILE\1=WORK
```

If you wanted to change the host ordering of the WORK profile to HOSTS\0 -> HOSTS\2 -> HOSTS\1 instead, remove HOSTS\1 from the WORK profile and create a duplicate entry of HOSTS\1 as HOSTS\3. Then you would add HOSTS\3 to the WORK profile as follows.

```
HOSTS\3\ACCESS=liveupdate.symantec.com

HOSTS\3\ACCESS2=http://liveupdate.symantec.com

HOSTS\3\IS_SYMANTEC=N%9-U,&[>@M

HOSTS\3\TYPE=HTTP

HOSTS\3\PROFILE\0=WORK
```

You enable Location Profiles by editing the Settings.LiveUpdate file and adding the HOSTS\{n}\PROFILE\{x}={pname} line to at least one host. The location profile name can be up to 36 characters in length. When the LiveUpdate client is started, the user has the option to select which location profile to use (Figure 3-1).

Figure 3-1 Location profile



The LiveUpdate client will then use the host that is designated by the profile to connect to the appropriate Central LiveUpdate server or Symantec LiveUpdate site.

Note: If the HOSTS\SET_PROFILE setting doesn't match an existing profile name, LiveUpdate will use the profile of the first host that has a profile set.

To enable location profiles

- Add the following settings to the Settings.LiveUpdate file:

HOSTS\{n}\PROFILE\{x}={pname}	Name of the profile that this host belongs to, where n is the number of the host, x is the number of the profile, and pname is the name of the profile. For example, HOSTS\0\PROFILE\0=WORK.
HOSTS\SET_PROFILE	Name of the profile to use. LiveUpdate will default to retrieving updates from HOSTS/0 if this setting is not set, or if it is set to a nonexistent location profile name.

See "About LiveUpdate client files" on page 60.

Changing LiveUpdate Administration Utility retrieval settings

You will need to make changes to the LiveUpdate retrieval settings when any of the following occur:

- A product is added to or deleted from those that are being updated through the Central LiveUpdate server.
- The Central LiveUpdate server is reinstalled on a new host computer.
- The host computer for the Central LiveUpdate server is moved to a new location on the network.
- The time interval for update checking by LuAdmin changes.

Adding a product

When a new Symantec product is installed on managed client computers on the network, you will need to change the LiveUpdate Administration Utility retrieval settings.

To add a product

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. In the LiveUpdate Administration Utility window, in the left pane, click **Retrieve Updates**.
3. In the right pane, under Symantec Product Line, do one of the following:
   - Check the Symantec product lines that you want to add.
     Be careful not to remove any already selected products.
   - Select the individual product components for the product that you want to add by checking the product line, clicking **Details**, and then checking the Languages and Product Updates to retrieve.

   The next time that LuAdmin checks for updates, it retrieves all of the currently available Update Packages for the added product and adds the Update Packages to the Update Index file.

Removing a product

When a Symantec product is uninstalled from client computers, you will need to change the LiveUpdate Administration Utility retrieval settings.

To remove a product

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. In the LiveUpdate Administration Utility window, in the left pane, click **Retrieve Updates**.
3. In the right pane, under Symantec Product Line, do one of the following:
   - Uncheck the Symantec product lines that you want to remove.
   - Select the individual product components for the product being removed by checking the product line, clicking **Details**, and then checking the Languages and Product Updates to be removed.

   The next time LuAdmin checks for updates, it removes all of the Update Packages for the product that is removed and deletes these Update Packages from the Update Index file.

Clearing the download directory

Once you have downloaded an update, it is always available to LiveUpdate clients. Changing the product selections on the Retrieve Updates window doesn't affect the availability of downloaded updates. You can clear the download directory of updates that you do not want clients to receive.

Note: If you have enabled clients to retrieve custom content and are using the download directory to store custom content files, the custom content files are also removed.

To clear the download directory

- In the LiveUpdate Administration Utility window, click **Tools** > **Clean Up Download Directory**.

Handling interrupted downloads

The LiveUpdate Administration Utility detects when a download is interrupted. When you restart the download, assuming that no application settings have changed, LuAdmin continues from where it left off, and 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), LuAdmin treats the incomplete downloads that were cached from the preceding interrupted session as part of the current session. To avoid this, you must either restart with the same application settings or remove the cached incomplete downloads from Program Files\LiveUpdate Administration\TEMP

If products are missing from the updates checklists

If you have recently installed the LiveUpdate Administration Utility, you may notice that items such as Symantec AntiVirus Definitions, Symantec Client Firewall, and Symantec Client VPN are missing from the Symantec Product Line checklist. SymAllLanguages may also be missing from the Languages of Updates checklist.

In this case, you must select a product that is available in the checklist and update it first. Once you have successfully updated one product, new options are added automatically to the checklists.

Note: If you click **Tools** and then **Update LiveUpdate Administration Utility**, LuAdmin will be updated to the latest version, but this will not always update the checklists.

To update the Symantec Product Line and Languages of Updates checklists

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. In the LiveUpdate Administration Utility window, in the left pane, click **Retrieve Updates**.
3. In the right pane, under Languages of Updates, check **English**.
4. Under Symantec Product Line, check **Symevent**.
5. Click **Retrieve**.
   After the LiveUpdate Administration Utility has retrieved the updates, it adds new entries to the product list.

Using custom LiveUpdate packages

Symantec Security Response 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 on a LiveUpdate production server, that detect and remove a new virus.

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

The merging process requires that the .trx file be merged into a full index file. The LiveUpdate Administration Utility attempts to replace entries in the LiveUpdate catalog file (Livetri.zip) with matching entries from the .trx file. If an entry in the .trx file does not have a corresponding entry in the catalog file, the merge fails.

The first time that you attempt to manually merge a .trx file, a complete .tri file must be present.

To merge custom LiveUpdate packages for the first time

1. Copy the .trx file that you received from Symantec to a folder on the hard drive.
2. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
3. On the Tools menu, click **Options**.
4. On the Retrieve tab, do one of the following:
   - Under Retrieve Update Options, uncheck **Remove unselected products from TRI files**.
   - Under Retrieving Previous Updates, check **Only retrieve new updates**. This temporarily reduces the size of the download. It is not necessary to retrieve previously downloaded files. This ensures that a full index file is retrieved.
5. Click **OK**.
6. In the left pane, click **Retrieve Updates**.
7. In the right pane, under Download Directory, browse to the location of the .trx file that was copied in step 1.
8. Under Languages of Updates and Symantec Product Line, select the languages and products that you want to update, and then click **Retrieve**.
   The latest .tri files are downloaded without removing unused entries.
   If there are products or languages missing, see "If products are missing from the LiveUpdate Administration updates checklists" on page 53.
9. In the left pane, click **Custom Updates**.
10. In the Custom update location dialog box, type the location that was specified in step 7, and then click **Merge**.
    The LiveUpdate Administration Utility compares the dates of the custom update and your most recent LiveUpdate virus definitions update and merges the files as appropriate. The Active custom updates box lists the current custom updates that are being applied by the LiveUpdate Administration Utility.
11. After the merge is complete, on the Tools menu, click **Options**.
12. On the Retrieve tab, click **Remove unselected products from TRI files**, then click **OK**.
13. In the left pane, click **Retrieve Updates**.

14 Repeat steps 6-8, using the folder in step 7 where the .trx file has been copied.
This removes any unwanted entries from the index file. It does not remove the required .trx entries from the .tri file.

15 Replace all of the files on the LiveUpdate server with the contents of the folder in step 7.
The LiveUpdate server index file now contains only the products that you want with the proper references to the LiveUpdate packages that were in the .trx file.
All subsequent updates will allow the proper merging of the .trx files.

Working with LiveUpdate events

The LiveUpdate Administration Utility includes an event log file which records events such as the following:

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

Viewing and deleting events

You can view events in, or remove events from, the event log file.

To view events in or delete events from the LiveUpdate Administration Utility event log file

1 Start LuAdmin.
See "Starting the LiveUpdate Administration Utility" on page 33.

2 In the LiveUpdate Administration Utility window, in the left pane, click **Log File**.

3 In the right pane, do one of the following:

View events	Under Filter by Type and Filter by Status, check the events that you want to filter.

Delete events	In the right pane, do one of the following: ■ Under LiveUpdate Administration Utility Log, select the event to remove, and then click **Remove**. ■ To remove all entries, click **Remove**, and then select **Entire Log file**. To remove selected entries, click **Selected Types or Statuses**, and then under Type and Status, check the entries to remove.

4 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 servers that are running on Windows NT/2000/XP can automatically receive LiveUpdate settings that are configured from the Symantec System Center. This lets them connect to your internal LiveUpdate server to download updates.

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

1. In the left pane of the Symantec System Center, right-click the parent server, server group, or client group, and then click **All Tasks** > **LiveUpdate** > **Configure**.
2. Click **Internal LiveUpdate Server**.

3. Type the name of the server.
   The Description boxes are optional.
4. If you are using an FTP or HTTP server, type the appropriate data.
   The Login Name and Password boxes are used only for FTP or HTTP servers, not for shared directories.
5. Under Connection, type the UNC path to your shared directory, or the URL or IP address for your HTTP or FTP server.
6. Under Type, select one of the following:
   - FTP
   - HTTP
   - LAN
7. Check **Apply settings to all clients**.
8. Click **Apply**, and then click **OK**.
9. If you have multiple parent servers and are configuring hosts from the parent server, repeat steps 1-8 for each parent server to have all clients and servers receive the changes.

Configuring multiple LiveUpdate servers for the Symantec System Center

The Symantec System Center lets you configure multiple LiveUpdate servers. If LiveUpdate is unable to successfully connect to the first LiveUpdate server, it will try other LiveUpdate servers until it is successful.

For example, you may want to configure your clients to run LiveUpdate from an internal Network share and if that fails, to connect to Symantec's LiveUpdate servers.

To configure multiple LiveUpdate servers for the Symantec System Center

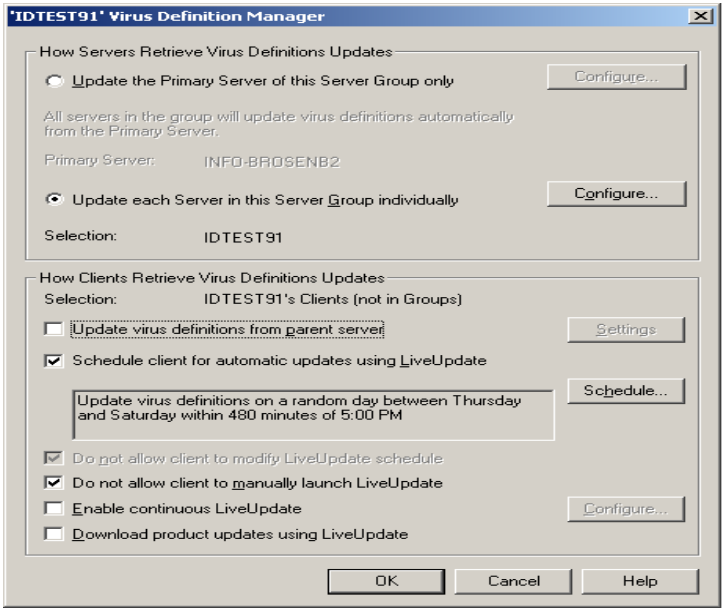
1. In the Configure LiveUpdate dialog box, click **New**.
   You will see 2 of 2 listed. You can configure up to 32 hosts.
2. To add the Symantec LiveUpdate Internet site to the list of hosts, in the URL or IP address box, type **liveupdate.symanteclive update.com**
3. Under Type, click **HTTP**.
4. Click **Apply**.
5. Click **OK**.

Enabling and scheduling client updates from the Symantec System Center

After you create a new host file, you must enable LiveUpdate to perform scheduled updates of the clients.

To enable and schedule client updates from the Symantec System Center

1. In the left pane of the Symantec System Center, right-click the parent server, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, under How Clients Retrieve Virus Definitions Updates, uncheck **Update virus definitions from parent server**.



3. Do any of the following:
   - To specify the frequency and time, check **Schedule client for automatic updates using LiveUpdate**, and then click **Schedule**.
     To configure Randomization and Missed Event options, click **Advanced**.
   - Uncheck **Do not allow client to manually launch LiveUpdate**.
4. Click **OK**.

Configuring NetWare servers to retrieve updates in the Symantec System Center

The LiveUpdate Administration Utility will not retrieve updates for NetWare Symantec AntiVirus servers. However, 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/vpcur8.lst
- ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/navup8.exe

---

Note: For the NetWare server to download virus definitions from the internal Central LiveUpdate server, you must configure the NetWare server to use TCP/IP and FTP correctly.

To configure NetWare servers to retrieve updates in the Symantec System Center

1. In the left pane of the Symantec System Center, right-click the NetWare server, and then click **All Tasks** > **Symantec AntiVirus** > **Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, under How Servers Retrieve Virus Definitions Updates, click **Update each Server in this Server Group individually**, and then click **Configure**.
3. In the Configure Primary Server Updates dialog box, click **Source**.
4. In the Setup Connection dialog box, click **LiveUpdate (Win32) / FTP (NetWare)**.
5. Click **Configure**.
6. In the Configure FTP dialog box, type the FTP information that is needed to access the internal Central LiveUpdate server.
   Changes that are made here apply to NetWare servers only.
7. Click **OK**.

Note: In order for the NetWare server to download definitions from an FTP server, it must be configured correctly to use TCP/IP.

Configuring a host file for unmanaged clients

If you have unmanaged clients, you must create a new host file and distribute it to your clients.

Note: When you run LiveUpdate 1.6 or 1.7 on the client computers, the Liveupdt.hst file is converted to the Settings.Liveupdate file and the Liveupdt.hst file is deleted. The LiveUpdate 1.6 and 1.7 Settings.Liveupdate file takes the place of the Liveupdt.hst file from LiveUpdate 1.5.

To configure and distribute a host file for unmanaged clients

1. Start LuAdmin.
   See "Starting the LiveUpdate Administration Utility" on page 33.
2. In the LiveUpdate Administration Utility window, in the left pane, click **Host File Editor**.
3. On the File menu, click **New** > **Host File**.
4. In the right pane, 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. Save the customized file as Liveupdt.hst.
   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 following files to the C:\Program Files\Symantec\LiveUpdate folder on each client:

- Liveupdt.hst
- S32luhl1.dll

  This file only needs to be copied 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.

Chapter 5

Working with LiveUpdate clients

This chapter includes the following topics:

Upgrading the LiveUpdate client

The LiveUpdate client is updated by LiveUpdate itself. You can also download the latest LiveUpdate client setup file. The client can be installed silently when you run it manually. You can also create a log file for the installation.

Upgrade the client

To download the latest LiveUpdate client setup file

- Do one of the following:
  - 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 computers directly from your internal server.

To install the LiveUpdate client silently

- Do one of the following:
  - For LiveUpdate version 1.6.x and later, at the command line, type **`Lusetup /s /a /q`**
  - For LiveUpdate version 1.5.x and earlier, at the command line, type **`Lusetup /s`**

To create a log file of the Lusetup installation

- At the command line, type **`Lusetup /a/log`**
  This creates a log file named Luinstall.log in the Windows folder.

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

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

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 about 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 the conversion, the Liveupdt.hst file is deleted.

About LiveUpdate client files

Table 5-1 lists the files that are used by the LiveUpdate client.

Table 5-1 LiveUpdate client files

File	Description
Settings.Default.LiveUpdate	Backup copy of the original default settings for the LiveUpdate client. For reference only.
ALUNOTIFY.EXE	Automatic LiveUpdate notification functionality.

Table 5-1 LiveUpdate client files

File	Description
AUPDATE.EXE	Automatic LiveUpdate executable. Used to retrieve product or content updates automatically
LUSETUP.EXE	LiveUpdate custom installer application that contains both the LiveUpdate base files and the SESA integration files.
LUSETUP-LT.EXE	LiveUpdate light installer that contains only the LiveUpdate base files
LUALL.EXE	Main LiveUpdate executable file that displays all product user interface: May be run from the command line
LuComServer.EXE	LiveUpdate engine file
LuComServerPS.DLL	LiveUpdate engine file
Ludirloc.dat	Configuration file that stores the initial location of the LiveUpdate settings files: May be referenced later by LiveUpdate if it cannot find the LiveUpdate settings files
LUINFO.INF	File that is used by the LiveUpdate installer: Contains a list of the files that were installed by LiveUpdate
LUInit.exe	LiveUpdate installer file
LUInit.ini	LiveUpdate installer file
LUINSDLL.DLL	LiveUpdate installer file
LUPreCon.DLL	LiveUpdate advanced update selection engine
LuResult.txt	Created during installation: Contains the final installer status result
LUSESAIntegration.dll	LiveUpdate SESA integration functionality. This file is not included in the lusetup-lt.exe installer.
NDETECT.EXE	Automatic LiveUpdate executable: Used to determine the presence of an Internet connection
NetDetectController.DLL	Automatic LiveUpdate executable
pegclient.dll	SESA base file. This file is not included in the lusetup-lt.exe installer.
pegcommon.dll	SESA base file. This file is not included in the lusetup-lt.exe installer.

Table 5-1 LiveUpdate client files

File	Description
providerInst.jar	SESA base file. This file is not included in the lusetup-lt.exe installer.
ProductRegCom.DLL	LiveUpdate engine file
ProductRegComPS.DLL	LiveUpdate product integration functionality
README.TXT	Updated product information, including recent enhancements, bug fixes, and known issues
S32LIVE1.DLL	LiveUpdate engine file
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
winluproviderinst.jar	LiveUpdate SESA integration functionality. This file is not included in the lusetup-lt.exe installer

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 as follows:

Windows 2000 (clean installation, not an upgrade)	C:\Documents and Settings\All Users\ Application Data\Symantec
Windows 95	C:\Windows\Application Data\Symantec
Windows 98, Windows Me	C:\Windows\All Users\Application Data\ Symantec
Windows NT 4.0	C:\WinNT\Profiles\All Users\ Application Data\Symantec

Note: If you have upgraded your operating system, the LiveUpdate data folder may be in the directory that is listed for the previously installed operating system.

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 that is specified by Shfolder.dll is used. Shfolder.dll is distributed with Internet Explorer 5.0 and later. 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

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

- Product.Inventory.LiveUpdate
- Log.LiveUpdate
- Settings.LiveUpdate

These files are in the Symantec\LiveUpdate folder locations that are specific to each operating system. You can view and edit the information in these files with a text editor such as Notepad.

See "About LiveUpdate client configuration files" on page 63.

About LiveUpdate client configuration files

The configuration information for LiveUpdate client versions 1.6x and later is kept in the following locations:

- {LiveUpdate Data}\Downloads\
- Product.Inventory.LiveUpdate
- Log.LiveUpdate
- Settings.LiveUpdate

Up to ten copies of the Product.Inventory.LiveUpdate and Settings.LiveUpdate files are kept. As each of these files is overwritten, the previous version is saved with a prefix that indicates 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 file is deleted. You can configure the number of backups that are kept in the Preferences section of the Settings.LiveUpdate file.

You can 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.Inventory.LiveUpdate

The Product.Inventory.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.

Warning: Do not edit this file.

Log.LiveUpdate

LiveUpdate creates a log file, Log.LiveUpdate, that is in the Application Data\Symantec\LiveUpdate folder. At the beginning of each section 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. By default, the size of the log file is set to 1024 KB. The size can be configured using the PREFERENCE\LOG_FILE_SIZE setting in the Settings.LiveUpdate file. The minimum file size is 10 KB. When the LiveUpdate client runs, it checks for any legacy #.Log.LiveUpdate files and merges them into Log.LiveUpdate, with the newest entries at the bottom of the file.

Settings.LiveUpdate

Settings.LiveUpdate contains all of the LiveUpdate configurations, including download resumption information, host entries, LiveUpdate settings, and merge indicators. Table 5-2 lists the settings and describes how they are used.

Table 5-2 Settings.LiveUpdate settings

Setting	Description
INSTALL_FOLDER	This setting shows where LiveUpdate is installed.

Table 5-2 Settings.LiveUpdate settings

Setting	Description
SETTINGS_FILE	The settings file contains the full path to the Settings.LiveUpdate file (by default, in the \Symantec\LiveUpdate folder).
MERGE_FILE_ LOCATION	This setting contains the full path to the location to search for a Settings.Merge.LiveUpdate 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 that is 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 overwrite the default settings. Once it is 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 setting specifies the full path to a file that contains text-settings format host specifications. It can also contain a path to a folder that contains 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 that is 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 it is found, any existing hosts are deleted from the settings and the contents of this file are loaded as the new host specifications.

Table 5-2 Settings.LiveUpdate settings

Setting	Description
NEW_HOSTS_ NO_DELETE	This setting 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 host file by everyone every time that LiveUpdate runs.
PRODUCT_CATALOG_ FILE	This setting contains the full path to the Product.Catalog.LiveUpdate file (which should be in the \Symantec\LiveUpdate folder under PER_MACHINE_FOLDER).
PER_USER_FOLDER	This is the Per User folder as returned from the Shfolder.dll.
PER_USER_ ROAMING_FOLDER	This is the Per User Roaming folder as returned from the Shfolder.dll.
PER_MACHINE_ FOLDER	This is the Per Machine folder as returned from the Shfolder.dll. The location of this directory differs according to the operating system that is installed.
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 that is 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 (this is only available when HTTP is the protocol that is being used to download updates). Following is an example of a DOWNLOADS entry: DOWNLOADS\LIVETRI.ZIP\CONTENTLENGTH= 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.zip DOWNLOADS\LIVETRI.ZIP\SERVER=ussmgreen. symantec.comDOWNLOADS\ LIVETRI.ZIP\SERVERPATH=/liveupdate2/ livetri.zipDOWNLOADS\LIVETRI.ZIP\ STATUS=Complete

Table 5-2 Settings.LiveUpdate settings

Setting	Description
PREFERENCES	This setting contains general settings.
INTERNET_CONNECT _TIMEOUT	This setting is used to specify the number of seconds LiveUpdate attempts to connect to the LiveUpdate server. The default is 30 seconds. The minimum value is 5 seconds. The default value will be used if the setting is not present or if it cannot be converted to a DWORD value.
INTERNET_READ_DATA _TIMEOUT	This setting is used to specify the number of seconds LiveUpdate takes to retrieve data from the LiveUpdate server. The default is 30 seconds. The minimum value is 5 seconds. The default value will be used if the setting is not present or if it cannot be converted to a DWORD value.
OSHOST_FILE_CHECK	This setting is used to enable or disable the host file integrity check. The default is YES (enabled). Any value other than NO will enable the check. If LiveUpdate finds a server name in the host file list that is a part of the symantec.com domain, you are given the following options: ■ Remove these entries from the hosts files (Recommended) This is the default option. LiveUpdate attempts to remove the entries from the host file. ■ Leave these entries in the hosts files (warn me about them later) LiveUpdate leaves the host file entries and alerts you about them the next time LiveUpdate runs. ■ Leave these entries in the hosts files (ignore them later) LiveUpdate leaves the host file entries and adds them to the list of host entries that are ignored.
OSHOST_FILE_CLEAN	This setting is used to enable automated OS hosts file cleaning. It is disabled by default. When this option is set to YES (enabled), and LiveUpdate runs in silent mode from either the command-line or from a scheduler, LiveUpdate automatically cleans any detected entries in all OS hosts files checked.

Table 5-2 Settings.LiveUpdate settings

Setting	Description
PRODUCT_INVENTORY_ INTEGRITY_CHECK	This setting is used to enable and disable the last known good inventory check. This check is only disabled when it is explicitly set to NO. If this setting is set to anything other than NO, or if it is not present, LiveUpdate will attempt to load a last known good Product Inventory file.
WORKINGDIRECTORY	This setting is used for download resumption and during normal file downloads to specify where to store temporary files.
USEPASSIVEFTPMODE	This setting 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.
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. (LAN HAL is not used in LiveUpdate versions later than 1.6). When you convert 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 you upgrade 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. **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 Windows NT workstations and servers. If you use the Norton Program Scheduler, LiveUpdate can't connect to a UNC location unless the LiveUpdate files reside in a shared resource on the Windows NT server that all users are authorized to access (a NULL share).

Table 5-2 Settings.LiveUpdate settings

Setting	Description
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 that is indicated in the PREFERENCES_LOG_FILE_NAME setting.
PRODUCT_CATALOG_ BACKUPCOUNT	If this setting is nonzero, it specifies the number of Product.Catalog.LiveUpdate file backups to keep 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 is 3 and the maximum is 10.
SETTINGS_FILE_ BACKUPCOUNT	If this setting is nonzero, it specifies the number of Settings.LiveUpdate file backups to keep 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 3 and the maximum 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 that is 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 Internet Explorer settings (if Internet Explorer is configured to use a RAS, it is used, and so on). A value of 2 means to silently dial the LiveUpdate-specific settings that are specified in the RAS settings.
UIRUNONCE	The first time the user interface runs, you can view the connection settings for RAS and proxy. Set this value to 0 to force the connection settings window to reappear.

Table 5-2 Settings.LiveUpdate settings

Setting	Description
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 used. Corporate mode is set to Yes if the LAN HAL is present, or if there is a non-Symantec host entry present. There are separate settings that indicate 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 it is running in corporate mode, it is not obeyed unless CORPORATE_ALLOWED_URL_HOSTS is active.
CORPORATE_ALLOWED_ URL_HOSTS	This setting 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 nonempty value, then the settings for a custom RAS are ignored. If RAS_USE_IE_RAS doesn't exist or 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 RAS must 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 settings can be set to activate proxies.
USE_IE_PROXY	This setting causes LiveUpdate to use the proxy settings (if there are any) that are specified in the Internet Explorer control panel. This is the default on a clean computer.

Table 5-2 Settings.LiveUpdate settings

Setting	Description
AUTHORIZATION	This setting is used in a proxy-authorization HTTP header that is sent in an InternetOpenUrl() request for FTP transfers. A proxy-authorization header has the following form: proxy-authorization: scheme login:password where scheme is Basic, NTLM, and so on, and login:password is UUEncoded.
HTTPAUTHORIZATION	This setting is used similarly to PREFERENCES\PROXY\AUTHORIZATION, but for HTTP proxy-authorization headers.
HOSTS	This setting contains host file information.
NUM_HOSTS	This setting shows the number of host entries that are listed.
NAME	This setting is used for display purposes. It shows to which host a connection is attempted. If a name has not been specified, the URL is displayed.
TYPE	This setting 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 setting always contains the fully qualified URL of the host.
LOGIN:ENC PASSWORD:ENC	These settings contain the Login and Password (if any) that are used to connect.
SUBNET SUBNETMASK	When you select 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, the host is used. Otherwise, it is skipped. A zero value for both subnet and subnet mask always match every IP address.

Table 5-2 Settings.LiveUpdate settings

Setting	Description
IS_SYMANTEC	This setting determines whether or not the server is a Symantec server. This is important in determining if the password should be shown in LuAdmin.
HOST_NUMBER	This setting contains the identifier of the host.
HOSTS\{n}\PROFILE\{x}={pname}	This setting is the name of the profile that this host belongs to when you want to allow clients to use location profiles. See "Enabling location profiles" on page 43.
HOSTS\SET_PROFILE	This setting is the name of the profile to use when using location profiles. LiveUpdate will default to retrieving updates from HOSTS/0 if this setting is not set, or is set to a non-existing location profile name.

Understanding corporate mode settings

When LiveUpdate 1.6 or later is installed on a computer that meets 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 the following ways:

- It does not attempt to use the URL= line in the TRI file to download a file. This prevents LiveUpdate from attempting to go through the firewall when it is 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
- LiveUpdate does 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.

Adding or changing LiveUpdate client computers

You can add new clients to the network and change their settings so that they can either receive updated virus definitions and program files from a Central LiveUpdate server or directly from a Symantec LiveUpdate site.

Adding a new client computer to the network

When a new client computer that uses Symantec products is first connected to the network and is to retrieve updates from the Central LiveUpdate server, you distribute the host file (Liveupdt.hst) that was created when the Central LiveUpdate server was set up to the new client computer using your preferred distribution tool.

If this file has been deleted or changes to it are needed, create a new custom host file (Liveupdt.hst) that points client computers to the internal server using the LiveUpdate Administration Utility.

See "Creating a LiveUpdate host file for clients" on page 36.

Changing a client computer to receive updates from a Symantec LiveUpdate server

When a client computer that previously received its updates from an internal Central LiveUpdate server is to be re-configured to get its updates from a Symantec LiveUpdate server, the following steps are required:

- Using the LiveUpdate Administration Utility, create a custom host file (Liveupdt.hst) that will direct a client computer to a Symantec LiveUpdate server for its updates.
  See "Creating a LiveUpdate host file for clients" on page 36.
- Distribute the new host file (Liveupdt.hst) to the client computer using your preferred distribution tool.

Changing a client computer to receive updates from a Central LiveUpdate server

When a client computer that previously received its updates from a Symantec LiveUpdate server is to be re-configured to get its updates from a Central LiveUpdate server, you distribute the host file (Liveupdt.hst) that was created to

direct client computers to the Central LiveUpdate server to the client computer using your preferred distribution tool.

In the event that this file has been deleted or changes to it are needed, create a new custom host file (Liveupdt.hst) that points client computers to the internal server using the LiveUpdate Administration Utility.

See "Creating a LiveUpdate host file for clients" on page 36.

Understanding LiveUpdate package authentication

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

Each new update is accompanied by a cryptographic signature, which is 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, an 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.

Ensuring that Automatic LiveUpdate and scheduled LiveUpdate authenticate

When LiveUpdate runs from either an Automatic LiveUpdate (ALU) or a scheduled LiveUpdate session, you may need to configure the client computer differently to handle these special cases. When LiveUpdate authenticates an HTTP Web server (for HTTPS hosts) or the signer of a LOTS file (only for custom content), it must search the system's certificate store to find a trusted root certificate.

By default, when a user installs a trusted root certificate, it is available only from that user account. If the default certificate store is used, a trusted root certificate is not available to other user accounts on that system, including the LocalSystem account under which most services run. ALU and scheduled sessions of LiveUpdate run within the LocalSystem account, and are subject to these limitations.

If your CA's certificates are added as trusted roots only for the current user account, then LiveUpdate may experience one of the following errors when not running within the same account:

Server not trusted	This happens when LiveUpdate is configured to connect to an HTTPS host whose certificate was issued by a CA that is not a trusted root.
Failed to authenticate custom content	This happens when LiveUpdate is configured to use custom content, and has a LOTS file signed by a certificate that was issued by a CA that is not a trusted root.

If your trusted root certificate is not one of the default trusted roots provided by Microsoft, then you need to add your trusted root certificate manually to ensure that it is available to all users. For example, if you issued your HTTPS Web server certificate or your LOTS signing certificate from an in-house certificate authority (CA), you need to add these certificates as trusted roots on all LiveUpdate client systems that connect to your HTTPS server or that use your LOTS file. If your certificates were issued by commercial CAs that are not installed by default in Microsoft's trusted root certificate store, you also need to add them as trusted roots. To avoid having to add trusted root certificates so that LiveUpdate works properly, you should obtain these certificates from well-known CAs that are installed in Microsoft's default trusted root certificate store, such as VeriSign®.

Adding trusted root certificates

You can make new trusted root certificates available to all accounts on a computer by adding them to the Local Machine certificate store, rather than to the current user certificate store (the default).

You can do this in the following ways:

- By using the Microsoft Management Console
- By using the Certificate Import Wizard

To add trusted root certificates using the Microsoft Management Console

1. In the Microsoft Management Console, on the File menu, click **Add/Remove Snap-in**.
2. In the Add/Remove Snap-in dialog box, click **Add**.
3. In the Add Standalone Snap-in dialog box, under Available Standalone Snap-ins, click **Certificates**, and then click **Add**.

4 In the Certificates snap-in window, click **Computer Account,** and then click **Next**.

5 Click **Local computer**.

6 Click **Finish**, and then click **Close**.

7 Click **OK**.

8 In the Microsoft Management Console, in the left pane, expand **Certificates (Local Computer)**.

9 Expand **Trusted Root Certification Authorities**.

10 Right-click the **Certificates** folder, and then click **All Tasks** > **Import**.

Follow the on-screen prompts in the Certificate Import Wizard to import your trusted root certificate file. Allow the certificate to be placed in the default certificate store Trusted Root Certification Authorities.

To add trusted root certificates using the Certificate Import Wizard

1 In Windows Explorer, right-click the trusted root certificate file, and then click **Install Certificate**.

2 In the Certificate Import Wizard, click **Next**, and then click **Place all certificates in the following store**.

3 Click **Browse**.

4 In the Select Certificate Store dialog box, click **Show physical stores**.

5 Expand **Trusted Root Certification Authorities**.

6 Click the **Local Computer** folder, and then click **OK**.

7 In the Certificate Import Wizard, click **Next**, and then click **Finish**.

LiveUpdate should now be able to access the trusted root when running under any account on the local computer. This enables the custom content and HTTPS hosts features to work properly under any account on the computer, including ALU and scheduled LiveUpdates.

Running LiveUpdate from a command line or scheduler

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

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

To run LiveUpdate from a command line or scheduler

- At the command line, 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

Some examples are as follows:

vpdn_lu.exe /fUpdate /s	Retrieve virus definitions silently.
vpdn_lu.exe /fVirusdef /s	Retrieve product updates silently.
vpdn_lu.exe /s	Retrieve product updates and definitions silently.

Chapter 6

Managing LiveUpdate clients with SESA

This chapter includes the following topics:

About LiveUpdate and SESA

In LiveUpdate version 2.5, clients are integrated with Symantec Enterprise Security Architecture (SESA) if the SESA Agent is running. This lets you define and propagate settings for LiveUpdate clients across an entire network using the Symantec management console.

For LiveUpdate, SESA lets you do the following:

- Define LiveUpdate client configurations that can be applied to groups of client computers or users.
- Modify a LiveUpdate configuration and automatically apply the updated configuration to all of the LiveUpdate clients that use it.

- View the number of Symantec products that are installed on each client computer.
- Perform queries on and create reports for LiveUpdate events for a single client computer or for groups of clients.

For information on other SESA administrative operations, see the *Symantec Enterprise Security Architecture Implementation Guide*.

Automatic detection of the SESA Agent

In LiveUpdate version 2.1, a LiveUpdate client automatically detects whether the host computer is managed by SESA or not each time that a LiveUpdate session is started. If a SESA Agent is present, the client retrieves its configuration settings from the SESA Agent.

This means that the order of installing the SESA Agent and LiveUpdate client is of no importance. Regardless of the order, the LiveUpdate client detects the presence of the SESA Agent and, if the SESA Agent is installed, the client uses the SESA configuration, logging, and inventory services.

If the client does not detect the SESA Agent, or is unable to communicate with the SESA Agent successfully, it runs independent of SESA using the last settings that were used. Events that would have been submitted to SESA are logged locally. Events are not visible from the Symantec management console until connection is re-established with the SESA Agent and SESA Manager. Any missed events are not resent to the Symantec management console.

Warning: The SESA Integration Package (SIP) for LiveUpdate should not be uninstalled. The LiveUpdate SIP is part of the base installation of SESA and uninstalling it will cause the Update reporting of the SESA Agent and SESA Manager to fail.

How SESA manages LiveUpdate client settings

For LiveUpdate clients, you can define a SESA configuration that assigns values to some or all of the LiveUpdate client settings that can be managed through SESA. There are some LiveUpdate settings that cannot be managed through SESA.

This configuration is stored by SESA in the SESA Directory under LiveUpdate Product. SESA makes a distinction between a Product and a copy of that Product installed on a computer on the network. It is very important to distinguish the

SESA LiveUpdate Product, where configurations and settings are stored, from installed copies of the LiveUpdate client.

In SESA, a Product object pertains to a specific version of a Symantec product that has been integrated with SESA. A Product is comprised of one or more Software Features. A Software Feature is a separately configurable component of the Product. Some products have only one Software Feature. Many products, however, have multiple Software Features.

A SESA configuration is a collection of settings. A setting is a setting name paired with a setting value. SESA configurations are stored under, and contained by, the Software Feature to which they apply.

In SESA, product configurations are not assigned or linked directly to installed products. Instead, configurations are linked to specific network locations, computers, users, or groups. In most cases, configurations will be linked to one or more SESA groups that each contain many computers or users. This makes managing product settings across the network easier and less subject to error.

Once a configuration is defined and stored, and then distributed, it can be linked to a location or to one or more groups of computers or users. This lets you define a few configurations for LiveUpdate that cover all of the LiveUpdate clients that are installed on the entire network. By default, all clients that are connected to a given SESA Manager are part of the default configuration for a given Product Feature Folder, for example, Windows LiveUpdate or Java LiveUpdate.

About the Symantec management console

Administrators define configurations and apply them using the Symantec management console. The Symantec management console lets you view the entire SESA Directory, including the following:

- Network organization, including domains, locations, and computers
- Symantec products defined and available on the network; configurations modifiable and available for each product
- The Symantec products actually installed on each computer on the network
- SESA groups with their members and associations (it is through these associations that groups, and their members, are linked to configurations)

The Symantec management console gives you many capabilities including event query and report creation. For more information, see the *Symantec Management Console User's Guide*.

You can also add and modify information that is stored in the SESA Directory through the Symantec management console. For LiveUpdate, you can define new client versions to SESA, create or modify client settings and configurations,

and create or remove associations of SESA groups with LiveUpdate client configurations.

Viewing Windows LiveUpdate events

When LiveUpdate is integrated with SESA, you can view events that report the status of LiveUpdate sessions on computers in your network environment.

To see Windows LiveUpdate events in the Symantec management console, the SESA Agent must first establish a connection with the SESA Manager.

View Windows LiveUpdate events

You can view the status of the SESA Agent startup on the Events view tab of the Symantec management console. Failed Agent Start-up Events are listed in the left pane under System Events > SESA System.

All other Windows LiveUpdate events appear on the Events view tab of the Symantec management console in the left pane under System Events > LiveUpdate.

To view SESA Agent startup events

1. In the Symantec management console, on the Events view tab, in the left pane, expand **System Events** > **SESA System**.
2. Click **Failed Agent Start-up Events**.
   The status bar in the lower-left corner of the window indicates how many events are in the report and which events you are currently viewing.

To view all other Windows LiveUpdate events

1. In the Symantec management console, on the Events view tab, in the left pane, expand **System Events** > **LiveUpdate**.
2. Select any of the reports.
   The status bar in the lower-left corner of the window indicates how many events are in the report and which events you are currently viewing.

About Windows LiveUpdate client configurations

In SESA, Windows LiveUpdate client configurations are broken into the following groups of settings:

- General
- Windows LiveUpdate

- Custom Content
- Windows Hosts

You can use the Symantec management console to create and distribute additional Windows LiveUpdate configurations to one or more computers on which LiveUpdate is installed.

When you create or modify a Windows LiveUpdate configuration, you must specify the LiveUpdate computers to associate with the configuration. You must also specify the SESA organizational unit to which the computer or computers belong. You can specify any configuration groups to which the computer or computers belong.

Windows LiveUpdate configurations let you specify network proxy server settings that may be required for LiveUpdate sessions in your network environment. You can also specify additional LiveUpdate HTTP or FTP servers to use for downloading product updates. In addition, you can create a LiveUpdate configuration to specify that certain LiveUpdate computers use a LiveUpdate configuration file other than the default. Similarly, you can specify that certain LiveUpdate computers use an internal, Central LiveUpdate server that you have set up using the LiveUpdate Administration Utility.

You can create a new Windows LiveUpdate configuration.

See "Modifying and creating Windows LiveUpdate configurations" on page 91.

After the configuration is created, you can make changes to it.

See "Modifying a Windows LiveUpdate configuration" on page 94.

General settings

The General tab displays the name and description of the selected Windows LiveUpdate configuration. A Windows LiveUpdate configuration is a collection of settings that you can apply to products on computers directly or by way of configuration groups or organizational units.

By default, SESA uses the Default Windows LiveUpdate configuration.

The General tab contains the following options:

Configuration name	The name of the configuration. You cannot modify this name after you create it.
Description	The configuration description. You cannot change the description of the Default configuration.
Last Modified On	The date that is set automatically when you change a configuration. You cannot change it manually.

Windows LiveUpdate settings

You can define the Windows LiveUpdate settings listed in Table 6-1. Only one set of these settings may be included in a single LiveUpdate configuration.

Table 6-1 Windows LiveUpdate settings

SESA property name	Setting name	Description
Overwrite settings?	None	Tells the LiveUpdate client how to apply the settings that were received from SESA to the client's Settings file. This property name is displayed by the Symantec management console as a drop-down list that has the values Replace and Overwrite. If you select Replace, LiveUpdate replaces its existing Settings data with the settings from SESA. If you select Overwrite, LiveUpdate overwrites the existing Settings data with the settings from SESA, but it doesn't delete any Settings values that are not changed by SESA.
Send LiveUpdate Start Session Events	SESA_EVENT\ SESSION_START_ VERBOSITY	Tells LiveUpdate which type of Session Start Events to send. If the switch is set to All, LiveUpdate sends all Session Start Events. If the switch is set to Error, LiveUpdate sends Session Start Events that have warning or higher severities. If the switch is set to None, LiveUpdate does not send any Session Start Events.
Send LiveUpdate End Session Events	SESA_EVENT\ SESSION_END_ VERBOSITY	Tells LiveUpdate which type of Session End Events to send. If the switch is set to All, LiveUpdate sends all Session End Events. If the switch is set to Error, LiveUpdate sends Session End Events that have warning or higher severities. If the switch is set to None, LiveUpdate does not send any Session End Events.
Send LiveUpdate Server Selection Events	SESA_EVENT\ SERVER_SELECTION_ VERBOSITY	Tells LiveUpdate which type of Server Selection Events to send. If the switch is set to All, LiveUpdate sends all Server Selection Events. If the switch is set to Error, LiveUpdate sends Server Selection Events that have warning or higher severities. If the switch is set to None, LiveUpdate does not send any Server Selection Events.
Send LiveUpdate Product Update Events	SESA_EVENT\ PRODUCT_UPDATE_ VERBOSITY	Tells LiveUpdate which type of Product Update Events to send. If the switch is set to All, LiveUpdate sends all Product Update Events. If the switch is set to Error, LiveUpdate sends Product Update Events that have warning or higher severities. If the switch is set to None, LiveUpdate does not send any Product Update Events.

Table 6-1 Windows LiveUpdate settings

SESA property name	Setting name	Description
Use LAN Hosts Only	ALL TRANSPORTS AVAILABLE and LAN_HAL_PRESENT	Determines whether LiveUpdate will use only LAN hosts to get updates. If this Boolean flag is set to TRUE, LiveUpdate tries to use LAN hosts to get updates. LiveUpdate sets the ALL TRANSPORTS AVAILABLE setting to 0 (false) and the LAN_HAL_PRESENT setting to TRUE if this SESA setting is true. If this setting is FALSE, LiveUpdate sets the ALL TRANSPORTS AVAILABLE setting to 1 (true) and deletes the LAN_HAL_PRESENT setting. This lets LiveUpdate use all host transports.
Enable client log file	LOGEVENTS	Determines whether a local log file is created. If this Boolean flag is set to TRUE, LiveUpdate creates a local log file. If this value is set to FALSE, LiveUpdate does not create a local log file.
Maximum Size allowable for LiveUpdate's local log file	LOG_FILE_SIZE	Holds the maximum size that the log file can occupy. The value is in kilobytes. The minimum log file size is 10 KB and the default value is 1024 KB.
Number of backup Product Inventory files	PRODUCT_ CATALOG_ BACKUPCOUNT	Holds the number of backup copies LiveUpdate will make of the Product Catalog file. The maximum value is 10.
Number of backup Settings files	SETTINGS_FILE_ BACKUPCOUNT	Holds the number of backup copies LiveUpdate will make of the Settings file. The maximum value is 10.
Use TRI file for URL lines?	CORPORATE_ ALLOWED_ URL_HOSTS	Allows or disallows LiveUpdate to use the URL lines in the TRI file. If this Boolean flag is set to TRUE, LiveUpdate uses the URL lines. The LiveUpdate property requires the Corporate Mode switch to be set for the ALLOWED_URL_HOSTS property to work correctly. LiveUpdate automatically sets the Corporate Mode switch each time that it receives a new set of configuration data.
Disable LiveUpdate Control Panel Applet?	DISABLE_CONTROL_ PANEL	Disables the LiveUpdate control panel applet. When this setting is TRUE, LiveUpdate won't install or use the control panel applet. If this setting is set to FALSE (default), the LiveUpdate control panel applet functions normally.

Table 6-1 Windows LiveUpdate settings

SESA property name	Setting name	Description
Environment	ENVIRONMENT	Describes the environment in which the computer is running. This drop-down list has the values RETAIL, CORPORATE, and NOT USED. The Environment switch tells the LiveUpdate computer whether it is running in an enterprise or a home user environment. LiveUpdate uses the Environment switch to determine whether the update should be installed. Since SESA is an enterprise product, the default value for the Environment switch in SESA is CORPORATE.
Lock Environment Switch	ENVIRONMENT_ LOCK	Locks the Environment setting. If this Boolean flag is set to TRUE, the Environment switch cannot be modified on the client's computer. The Environment switch can still be set via SESA, a Setting's merge file, or by directly editing the Settings file. If this flag is set to FALSE, any Symantec program can modify the Environment switch. By default, this flag is set to TRUE.
Use Express Mode	EXPRESS_MODE\ ENABLED	Switches LiveUpdate between Interactive mode and Express mode. If this Boolean flag is set to TRUE, LiveUpdate runs in Express mode and if it is FALSE, LiveUpdate runs in Interactive mode. By default, this flag is TRUE.
Automatically Start Express Mode	EXPRESS_MODE\ AUTO_START	Determines if the LiveUpdate process starts automatically once LiveUpdate is launched in Express mode. If this Boolean flag is set to TRUE, Express mode automatically starts its LiveUpdate session when it launches. If it is set to FALSE, the user must manually start Express mode. By default, this flag is TRUE. LiveUpdate ignores this flag if it is running in Interactive mode.
Disable Express Mode Stop Button	EXPRESS_MODE\ DISABLE_STOP_ BUTTON	Determines whether the Stop button in Express mode is enabled or disabled. If the Stop button is disabled, the user can't stop an Express mode session through LiveUpdate. If this Boolean flag is TRUE, the Stop button is disabled and if this flag is FALSE, the Stop button is enabled. By default, this flag is TRUE. LiveUpdate ignores this flag if it is running in Interactive mode.
Automatically Close Express Mode on Completion	EXPRESS_MODE\ AUTO_EXIT	Determines if the LiveUpdate process closes automatically after LiveUpdate completes running in Express mode.

Table 6-1 Windows LiveUpdate settings

SESA property name	Setting name	Description
Enable Enhanced Error Support	ENABLE_ENHANCED_ ERROR_SUPPORT	Determines whether LiveUpdate provides an extended error information URL for all error messages. If this Boolean flag is TRUE, LiveUpdate shows an Enhanced Error URL and if it is FALSE, LiveUpdate does not show the URL. By default, this flag is FALSE.
Enhanced Error Support Base URL	ENABLE_ENHANCED_ ERROR_SUPPORT_ URL	Provides an alternate base path for the Enhanced Error Support URL. If this text property is set, LiveUpdate looks for error pages on the page's URL. LiveUpdate expects that this property refers to a valid URL address. By default, this property is not set. If this property is not set, LiveUpdate uses the Symantec Technical Support Web site as the base URL.
Http Proxy Settings Source	PROXY\ HTTP_PROXY	Tells LiveUpdate how to get configuration information for an HTTP proxy. The options are Use Internet Options Settings, Use Custom Settings, Do not Use Any Proxy Settings, or Use Existing Client Settings. These options appear in the Symantec management console in a drop-down list. By default, this property is set to Use Existing Client Settings, which does not cause any change to the LiveUpdate client's Settings file.
Http Proxy Server	PROXY\ HTTPSERVER	Holds the URL to the HTTP proxy server. This value is only valid if the HTTP_PROXY setting is set to Use Custom Settings.
Http Proxy Port number	PROXY\ HTTPPORT	Identifies the port on which the HTTP proxy server is listening for traffic. This value is only valid if the HTTP_PROXY setting is set to Use Custom Settings.
Http Authentication Username	PROXY\ AUTHENTICATION\ BASIC\ HTTP_USERNAME	Holds the user name that is used for HTTP Basic Authentication.
Http Authentication Password	PROXY\ AUTHENTICATION\ BASIC\ HTTP_PASSWORD	Holds the password that is used for HTTP Basic Authentication. This property is only valid if the HTTP_USERNAME property is also set.

Table 6-1 Windows LiveUpdate settings

SESA property name	Setting name	Description
Ftp Proxy Settings Source	PROXY\ FTP_PROXY	Tells LiveUpdate how to get configuration information for an FTP proxy. The options are Use Internet Options Settings, Use Custom Settings, Do not Use Any Proxy Settings, or Use Existing Client Settings. These options appear in the Symantec management console in a drop-down list. By default, this property is set to Use Existing Client Settings, which does not cause any change to the LiveUpdate client's Settings file.
Ftp Proxy Server	PROXY\ SERVER	Holds the URL to the FTP proxy server. This value is only valid if the FTP_PROXY setting is set to Use Custom Settings.
Ftp Port number	PROXY\ PORT	Identifies the port on which the FTP proxy server is listening for traffic. This value is only valid if the FTP_PROXY setting is set to Use Custom Settings.
Do Not Manage dial-up accounts	RAS\DO_NOT_ MANAGE_RAS	Tells LiveUpdate how to deal with a RAS connection that is created during the LiveUpdate session. If this Boolean flag is set to TRUE, LiveUpdate does not attempt to close any RAS connection that was started during the LiveUpdate session. If this flag is set to FALSE, LiveUpdate attempts to close a RAS connection that started after the LiveUpdate session began. If LiveUpdate finds multiple RAS connections that have started since it first ran, LiveUpdate does not attempt to close any of these connections. When LiveUpdate is running in Interactive mode, the user is prompted to close the connection. **Note:** AOL Broadband users should set this option to TRUE.
Prevent Upgrades to LiveUpdate Client	PREVENT_INSTALL	Prevents the LiveUpdate installer from running. If this Boolean flag is set to TRUE, the LiveUpdate installer does not run unless LiveUpdate is not correctly installed on the user's computer. If this flag is set to FALSE, the LiveUpdate installer functions normally.
Prevent Uninstall of LiveUpdate Client	PREVENT_UNINSTALL	Determines whether LiveUpdate can be uninstalled. If this Boolean flag is set to TRUE, the LiveUpdate uninstaller does not uninstall LiveUpdate. If this flag is set to FALSE, the LiveUpdate uninstaller will behave normally.

Custom Content settings

You can define the Custom Content settings listed in Table 6-2 for Windows LiveUpdate versions only. Custom Content settings are not available for Java LiveUpdate clients. Only one set of Custom Content settings may be included in a single LiveUpdate configuration.

See "About LiveUpdate custom content publishing" on page 105.

Table 6-2 Custom Content settings

SESA property name	Setting name	Description
Overwrite Custom Content settings?	None	Tells the LiveUpdate client how to apply the Custom Content settings to the Settings file. This property name is a drop-down list that has the values Replace all host settings and Overwrite existing host settings. If you select the Replace option, LiveUpdate replaces its existing custom content data with the settings from SESA. If you select the Overwrite option, LiveUpdate overwrites the existing custom content values with the settings from SESA, but it doesn't delete any property values that are not set in SESA.
Enable Custom Content	CUSTOM_CONTENT	Determines whether custom content is received. If this Boolean flag is set to TRUE, LiveUpdate receives custom content. If this flag is set to FALSE, LiveUpdate ignores custom content. Custom content is defined as content in the custtri.zip file. This flag is set to FALSE by default.
Automatically Update the LOTS	UPDATE_LOTS_FILE	Determines whether LiveUpdate attempts to update the LOTS file. If this is set to YES, LiveUpdate attempts to update the LOTS file during each LiveUpdate session. If the LOTS file retrieval fails, LiveUpdate disables custom content for that session. If this is set to OPTIONAL, the LiveUpdate client looks for a new LOTS file, but if the file retrieval fails, custom content is still downloaded. If this is set to NO, the LiveUpdate client does not look for a new LOTS file.
LOTS HTTPS Server URL	LOTS\LOTS_HTTPS_URL	Contains the HTTPS URL that LiveUpdate should use to retrieve the LOTS file. This URL must be HTTPS or LiveUpdate does not update the LOTS file.
Username for LOTS Server	LOTS\LOGIN	Holds the user name that is required to log on to the HTTPS LOTS server.
Password for LOTS Server	LOTS\PASSWORD	Holds the password that is required to log on to the HTTPS LOTS server.

Windows Hosts settings

You can define the Windows Hosts settings listed in Table 6-3. You can define multiple sets of Windows Host configurations in a single configuration. Where you see Host 0 in the Property Name, or HOST\0\ in the Setting Name, the 0 indicates the Windows Host number. The first Windows Host has the number 0. The second Windows Host has the number 1 and so on.

Table 6-3 Windows Hosts settings

SESA property name	Setting name	Description
Overwrite or replace existing hosts?	None	Tells the LiveUpdate client how to apply the Windows Host settings from SESA to the Settings file. This property name is displayed by the Symantec management console as a drop-down list that has the values Replace all Windows Host settings and Overwrite existing Windows Host settings. If you select Replace, LiveUpdate replaces its existing Windows Host data with the Windows Host settings from SESA. If you select Overwrite, LiveUpdate overwrites the existing Windows Host data with the settings from SESA, but it doesn't delete any Windows Host values that are not changed by SESA.
Host 0 Type	HOSTS\0\TYPE	Holds the type of protocol used for this Windows Host. This data is displayed in the Symantec management console as a drop-down list that has the values HTTP, FTP, LAN, and HTTPS.
Host 0 URL	HOSTS\0\ACCESS HOSTS\0\ACCESS2	Holds the address and path to the LiveUpdate server's content.
Host 0 Name	HOSTS\0\NAME	Contains the display name for this Windows Host. LiveUpdate displays this name above the progress bar when it is connecting to the Windows Host for the first time. The LiveUpdate log file always displays the Host URL instead of or along with the Host name.
Host 0 Login	HOSTS\0\LOGIN	Contains the user name that is required to connect to this Windows Host. This Login is currently only supported for FTP. LiveUpdate ignores the Login for all other Windows Hosts.
Host 0 Password	HOSTS\0\PASSWORD	Contains the password that is associated with the Login user name. This password is currently only supported for FTP. LiveUpdate ignores the Password for all other Windows Hosts.

Table 6-3 Windows Hosts settings

SESA property name	Setting name	Description
Host 0 Subnet	HOSTS\0\SUBNET	Contains the IP address, which, along with the subnet mask, is used to filter out Windows Hosts that the LiveUpdate client can select. The subnet and subnet mask are applied to the IP address of the LiveUpdate client to determine if this client can use the Windows Host. The formula for subnet and subnet mask is if a logical AND between the LiveUpdate client IP address and the subnet mask equals the subnet IP address, the client may use the Windows Host. You can come up with a subnet and subnet mask combination that no IP address can satisfy.
Host 0 SubnetMask	HOSTS\0\ SUBNETMASK	Contains the subnet mask that is used with the subnet. See the Host 0 Subnet description for more information on how the subnet and subnet mask work together.

Modifying and creating Windows LiveUpdate configurations

You can create a new Windows LiveUpdate configuration, or modify an existing one, such as the Default configuration.

Modify and create Windows LiveUpdate configurations

Before you can distribute a Windows LiveUpdate configuration, you must first configure it for distribution. You can modify the Default configuration, or create a new Windows LiveUpdate configuration.

After you have created or modified a configuration, you can distribute it to Windows LiveUpdate computers.

See "Distributing a Windows LiveUpdate configuration" on page 94.

To modify an existing Windows LiveUpdate configuration

1. Edit the Windows LiveUpdate configuration properties to add the computers that will use the Windows LiveUpdate configuration.
   See "Editing Windows LiveUpdate configuration properties" on page 93.
2. Modify the Windows LiveUpdate configuration to specify configuration settings.
   See "Modifying a Windows LiveUpdate configuration" on page 94.

To create a new Windows LiveUpdate configuration

1. In the Symantec management console, on the Configurations view tab, in the left pane, under the top-level SESA domain, expand **LiveUpdate** > **Windows LiveUpdate**.
2. Right-click **Windows LiveUpdate**, and then click **New**.
3. In the first dialog box of the Create a new Configuration Wizard, click **Next**.
4. In the General dialog box, type a configuration name, a description (optional), and then click **Next**.
5. In the Computers dialog box, click **Add**.
6. In the Searching for Computers dialog box, in the Computer name text box, type a specific computer name or a combination of letters and an asterisk, and then click **Search**.
   By default, the Computer name text box contains an asterisk (*), which serves as a wildcard character, displaying all computers that have been defined.
7. On the Found tab, select one or more computers, and then click **OK**.
8. Repeat steps 5 through 7 as necessary, and then click **Next**.
9. In the Configuration Groups dialog box, do one of the following:
   - If your computer or computers belong to a configuration group, click **Add**, select the configuration group to which the computer or computers belong, click **OK**, and then, in the Configuration Groups dialog box, click **Next**.
   - If your computer or computers do not belong to a configuration group, click **Next**.
10. In the Organizational Units dialog box, to associate an organizational unit with the selected computer, click **Add**.
11. In the Browse for Organizational Units dialog box, on the Found tab, select the organizational unit to which the computer or computers belong, and then click **OK**.
12. Repeat steps 10 and 11 as necessary.
13. Click **Next**.
14. Click **Next**.
15. Review the Configuration summary, and then click **Finish**.
16. Click **Close**.

Editing Windows LiveUpdate configuration properties

You must add the computers that will use the Windows LiveUpdate configuration before you can distribute the configuration. At a minimum, you must specify the computer names and associated organizational units.

To edit Windows LiveUpdate configuration properties

1. In the Symantec management console, on the Configuration view tab, in the left pane, under the top-level SESA domain, expand **LiveUpdate** > **Windows LiveUpdate**.
2. Under Windows LiveUpdate, right-click the configuration that you want to modify, and then click **Properties**.
3. In the Configuration Properties dialog box, on the Computers tab, to add a computer, click **Add**.
4. In the Searching for Computers dialog box, in the Computer name text box, type a specific computer name or a combination of letters and an asterisk, and then click **Search**.

   By default, the Computer name text box contains an asterisk (*), which serves as a wildcard character, displaying all computers that have been defined.
5. On the Found tab, select one or more computers, and then click **OK**.
6. If your computer is associated with a configuration group, on the Configuration Groups tab, click **Add**.
7. In the Find Configuration Groups dialog box, on the Found tab, select the configuration group to which the computer belongs, and then click **OK**.
8. On the Organizational Units tab, to associate an organizational unit with the selected computer, click **Add**.
9. In the Browse for Organizational Units dialog box, on the Found tab, select the organizational unit to which the computer belongs, and then click **OK**.
10. Repeat steps 4 through 9 as necessary.
11. In the Configuration Properties dialog box, click **OK**.

Modifying a Windows LiveUpdate configuration

You can change an existing Windows LiveUpdate configuration.

To modify a Windows LiveUpdate configuration

1. In the Symantec management console, on the Configurations view tab, in the left pane, under the top-level SESA domain, expand **LiveUpdate** > **Windows LiveUpdate**.
2. Under Windows LiveUpdate, select the configuration that you want to modify.
3. In the right pane, modify the configurations on the following tabs as necessary:
   - General configuration settings
   - Windows LiveUpdate configuration settings
   - Custom content Settings
   - LiveUpdate Other Settings

Distributing a Windows LiveUpdate configuration

To successfully distribute a Windows LiveUpdate configuration, you must have specified the target computers and organizational units when you created or modified the Windows LiveUpdate configuration.

To distribute a Windows LiveUpdate configuration

1. In the Symantec management console, on the Configurations view tab, in the left pane, under the top-level SESA domain, expand **LiveUpdate** > **Windows LiveUpdate**.
2. Under Windows LiveUpdate, right-click a configuration, and then click **Distribute**.
3. When you are prompted to distribute the configuration, click **Yes**.
   A message is sent to the computers that are associated with the Windows LiveUpdate configuration, which instructs them to contact the SESA Manager for a new configuration.

Chapter 7

Using Java LiveUpdate

This chapter includes the following topics:

About Java LiveUpdate

Java LiveUpdate is the Symantec technology that provides LiveUpdate services on Windows and non-Win32 platforms such as AS/400, UNIX, Solaris, and Macintosh. Java LiveUpdate is automatically installed with Symantec products on these platforms.

Java LiveUpdate functions similarly to the Win32 version of LiveUpdate. When Java LiveUpdate runs, it connects to the server that is specified in the host file or in liveupdate.conf. The zipped catalog file (livetri.zip) is downloaded into the local package directory and the LiveUpdt.tri files are extracted. The files are authenticated to ensure that they originated from Symantec.

Java LiveUpdate determines if there are updates available for the specified products. For each update that is found, a temporary directory is created under the local package directory into which the zipped files are copied. The packages are authenticated, unzipped, and installed. The temporary directory and files are then removed.

Java LiveUpdate tracks configuration information about multiple LiveUpdate servers or hosts. It tries each of the servers in the order in which they are listed in the Java LiveUpdate configuration file and automatically fails over to the next host if it finds that the server is unreachable.

Java LiveUpdate also integrates into the Symantec Enterprise Security Architecture (SESA™) event management system. SESA employs data collection services for events that Symantec security products generate. For more

information on SESA, see the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator's Guide.*

Java LiveUpdate requires Java Runtime version 1.1.8 or later.

Java LiveUpdate configuration

By default, Java LiveUpdate gets its configuration information from the liveupdate.conf file. You can specify a different configuration file with the `-c` command-line switch. For example:

```
java -classpath jlu.jar LiveUpdate -c /home/james/liveupdate.conf
<parameters>
```

See "Java LiveUpdate command-line switches" on page 102.

The locations of liveupdate.conf are as follows:

UNIX	/etc/liveupdate.conf
Win32	<Common Apps Folder>\Symantec\Java LiveUpdate\liveupdate.conf

When you configure Java LiveUpdate, you can set the parameters in Table 7-1.

Table 7-1 liveupdate.conf parameters

Parameter	Description
workdir	The working directory on the client computer. This entry is required. Java LiveUpdate creates a local package directory under the specified working directory. If the working directory doesn't exist, Java LiveUpdate creates it and uses the working directory as the local package directory. The local package directory is removed when Java LiveUpdate exits unless the `-k` command-line switch is specified. See "Java LiveUpdate command-line switches" on page 102.
hostfile	The full path to a legacy host file (Liveupdt.hst) that is generated by the LiveUpdate Administration Utility. If a host file is specified, all of the transport-related entries in liveupdate.conf are ignored, and the information from the specified host file is used instead.

Table 7-1 liveupdate.conf parameters

Parameter	Description
logfile	The full path to the log file that Java LiveUpdate uses to log events and errors. If this setting is omitted, no log file is created.
jar	The full path to the jlu.jar file. If this file is omitted, Java LiveUpdate looks for its JAR file in the LiveUpdate subdirectory immediately under the Symantec directory. The location of the Symantec directory is specified by the BaseDir parameter in the Symantec Shared section of the Symantec global configuration file /etc/Symantec.conf. Java LiveUpdate returns an error immediately if it can't locate its JAR file.
urls	External Symantec server support. By default, Java LiveUpdate ignores the URL= lines in the TRI file. If this parameter is 1 (true), Java LiveUpdate uses the URL= lines in the TRI when it uses HTTP to download packages. This parameter and the URL= lines are ignored if FTP is specified as the protocol.
proxy	The name of a proxy server. For example: proxy=addr:port, where the port number is optional. Addr is the TCP/IP address of the proxy server and :port is the TCP/IP port on which the proxy server is listening (optional). This setting is not supported for FTP.
proxyusername	The user name to use when you log on to the specified proxy server. This setting is only needed if your proxy server requires a logon. This setting is not supported for FTP.
proxypassword	The password that is associated with the specified proxyusername account. This setting is only needed if your proxy server requires a logon. This setting is not supported for FTP.
maximumLogFileSize	The maximum allowed log file size in KBs. Java LiveUpdate discards older log entries once the log file exceeds the specified maximum size. The default log file size is 1024 KB.

Table 7-1 liveupdate.conf parameters

Parameter	Description
AllowConfigurationOverride	The setting that is used to tell Java LiveUpdate to use the -c command-line switch and hostfile setting. If this is set to anything other than True in the shared liveupdate.conf file, Java LiveUpdate ignores the -c switch and hostfile setting.
hosts/<host#>/url	The URL of a LiveUpdate server. You may specify a non-standard port for HTTP servers and a package directory for both FTP and HTTP servers. Java LiveUpdate supports up to 10 servers starting with 0 through 9. This setting replaces the following Java LiveUpdate 1.10 settings: ■ protocol ■ host ■ packagedir ■ login ■ password

You must specify the working directory on the client computer using the workdir parameter.

Java LiveUpdate must also be able to find its JAR file. For UNIX platforms, Java LiveUpdate searches for jlu.jar in the LiveUpdate subdirectory immediately under the Symantec directory that is specified in /etc/Symantec.conf.

For Win32 platforms, Java LiveUpdate searches for jlu.jar in <Program Files Folder>\<Common Files Folder>\Symantec Shared\Java LiveUpdate. If the jlu.jar file does not exist in the directory, you must specify its location using the jar parameter.

If you want to use a legacy host file, you must type the full path to the host file. The only parameters that are required in the configuration file are the workdir and the hostfile settings. If you are not using a legacy host file, the workdir and the hosts/<host#>/url setting must be specified.

If a setting is followed by :ENC, the value has been encrypted by Java LiveUpdate. The settings that may be encrypted are as follows:

- login
- password
- proxyusername
- proxypassword

- hosts/<host#>/login
- hosts/<host#>/password

Java LiveUpdate 2.0 and later automatically encrypts the login and password settings each time that Java LiveUpdate runs if the :ENC tag is missing.

Sample liveupdate.conf files

Following is an example of a liveupdate.conf file on UNIX using Java LiveUpdate 2.0:

```
;hostfile=opt/Symantec/LiveUpdate/liveupdt.hst
hosts/0/url=http://liveupdate.symantecliveupdate.com:80
hosts/1/url=http://liveupdate.symantec.com:80
hosts/2/login:ENC=b3effee10d982d2c7449c810c
hosts/2/password:ENC=19d3d3v3c123333898dcf293d
hosts/2/url=ftp://update.symantec.com/opt/content/onramp
workdir=/tmp
logfile=/opt/Symantec/LiveUpdate/liveupdt.log
jar=/opt/Symantec/LiveUpdate/jlu.jar
urls=1
proxy=proxy.yourcompany.com:8080
proxyusername=joe
proxypassword=geer132
maximumLogFileSize=512
AllowConfigurationOverride=true
```

Following is an example of a liveupdate.conf file on Win32 using Java LiveUpdate 2.0:

```
hostfile=/opt/symantec/LiveUpdate/liveupdt.hst
hosts/0/url=http://liveupdate.symantecliveupdate.com:80
hosts/1/url=http://liveupdate.symantec.com:80
hosts/2/login:ENC=b3effee10d982d2c7449c810c
hosts/2/password:ENC=19d3d3v3c123333898dcf293d
hosts/2/url=ftp://update.symantec.com/opt/content/onramp
logfile=C:\Documents and Settings\All Users\Application
Data\Symantec\Java LiveUpdate\liveupdt.log
workdir=C:\Documents and Settings\All Users\Application
Data\Symantec\Java LiveUpdate\Downloads
jar=c:\Program Files\Common Files\Symantec Shared\Java
LiveUpdate\jlu.jar
```

```
urls=1
proxy=proxy.yourcompany.com:8080
proxyusername=joe
proxypassword=geer132
maximumLogFileSize=512
AllowConfigurationOverride=true
```

Following is an example of a liveupdate.conf file on UNIX using Java LiveUpdate 1.10.

Note: Java LiveUpdate 1.10 is not supported on Windows.

```
protocol=HTTP
host=liveupdate.symantecliveupdate.com
workdir=/tmp
jar=/opt/Symantec/LiveUpdate/jlu.jar
logfile=/opt/Symantec/LiveUpdate/liveupdt.log
proxy=proxy.proxy.yourcompany.com:8080
proxyusername=joe
proxypassword=geer132
urls=1
```

Configuring Java LiveUpdate to use a Central LiveUpdate server

LiveUpdate operation is controlled by settings in the liveupdate.conf file. By default, an HTTP connection is made to the Symantec server. You can change the settings to point to an internal Central LiveUpdate server using either an FTP or HTTP protocol connection. The Central LiveUpdate server is created using the separately supplied and installed LiveUpdate Administration Utility.

Configure LiveUpdate to use a Central LiveUpdate server

You can configure liveupdate.conf to use a host (.hst) file that was created to use a Central LiveUpdate server. You can also create a new host file.

See "Configuring clients to use a Central LiveUpdate server" on page 36.

Warning: Make a backup copy of liveupdate.conf before you modify it.

To use an existing Liveupdt.hst file

- Add the following line to the liveupdate.conf file:

  ```
  hostfile=<full path to the .hst file on the server>
  ```

  If the hostfile= parameter is included in liveupdate.conf, all of the settings that relate to transport (host, protocol, logon, password, and proxy) are ignored and data from the .hst file is used instead.

To create a new Liveupdt.hst file

- Use the LiveUpdate Administration Utility (LUAdmin), which runs under Windows.

  See "Creating a LiveUpdate host file for clients" on page 36.

Running Java LiveUpdate from the command line

At times, it may be necessary to manually run Java LiveUpdate from the command line.

Warning: Do not run Java LiveUpdate from the command line unless you have been instructed to do so by Symantec Technical Support.

To run Java LiveUpdate from the command line

- At the command prompt, type the following:

  ```
  java <classpath> jlu.jar LiveUpdate<options>
  ```

  In order to run Java LiveUpdate, the classpath must be set by typing the full path to jlu.jar and the Java runtime classes. The Java runtime classes are usually in a file named either classes.zip or rt.jar.

Java LiveUpdate command-line switches

Table 7-2 lists the command-line options that are available for Java LiveUpdate.

Table 7-2 Java LiveUpdate command-line options

Option	Description

-version	This switch prints information about the version of Java LiveUpdate to stdout. Java LiveUpdate exits immediately after printing the version information. For example:
	`java -classpath jlu.jar LiveUpdate -version`
	`The output is similar to the following:`
	`JLU Windows 1.1 9`
	A general description of the operating system is printed, followed by the version number (1.1) and the build number (9).
	Possible values for the operating system are Windows, Macintosh, AS/400, S/390, Linux, Solaris, and AIX.

-c <full path to configuration file>	This switch is used to specify a configuration file other than the default (/etc/liveupdate.conf). For example: `java -classpath jlu.jar LiveUpdate -c /home/lufiles/liveupdate.conf`
-r	This switch is used to encrypt the logon, password, proxyusername, and proxypassword settings. The encrypted version of the configuration file is copied over the existing liveupdate.conf file. Use the -c switch to encrypt a specific configuration file other than default /etc/liveupdate.conf. Java LiveUpdate exits immediately after creating the encrypted configuration file. For example: `java -classpath jlu.jar LiveUpdate -c /home/lufiles/liveupdate.conf -r /home/lufiles/liveupdate_enc.conf` On S/390 and AS/400, the -e switch should also be used to specify a specific character encoding.

Table 7-2 Java LiveUpdate command-line options

Option	Description
-d	This switch enables debug mode with trace output to stdout.
-e <character encoding>	This switch is used to specify a character encoding for the configuration file. The default when this parameter is not used is ISO-8859-1, the ASCII character encoding. See "Support for EBCDIC character encoding" on page 103.
-k	This switch is used to prevent the deletion of the temporary files that are retrieved from the LiveUpdate server and stored in the package directory that is specified by the workdir setting. Otherwise, these files are deleted.

Support for EBCDIC character encoding

You must pass the command-line parameter -e <encoding> to indicate the character encoding of the CONF files on your platform to Java LiveUpdate. For AS/400, the name of the encoding is CP307. For S/390, the name of the encoding is CP1047. For example:

```
java -classpath jlu.jar LiveUpdate -e CP037 -c \etc\liveupdate.conf
```

If the -e parameter is not specified, the default ASCII character encoding is used for all files. If you use debug mode, Java LiveUpdate indicates which code page is being used.

Chapter 8

Working with custom content

This chapter includes the following topics:

About LiveUpdate custom content publishing

LiveUpdate custom content publishing lets you use the security features of LiveUpdate to allow client computers to receive custom content. Custom content is any type of Symantec product file that you want your clients to receive, including firewall rules for the Symantec Desktop Firewall products, settings for Symantec products, and virus and worm removal tools.

Using the Custom Content Publishing Application (CCPA), you create, modify, and publish updates that are uploaded to the Central LiveUpdate server. When the LiveUpdate client runs, it looks for custom content packages, in addition to LiveUpdate virus definitions and product updates, and authenticates the package to determine if it can be trusted. The custom content publishing process consists of users with clearly defined roles.

Roles and users

The CCPA Administrator assigns a role to each system user. Roles determine abilities and responsibilities within CCPA. CCPA roles are shown in Table 8-1.

Table 8-1 CCPA user roles

Role	Description
Administrator	CCPA comes pre-configured with one administrative user. The user name for this predefined Administrator is admin. The Administrator can create user profiles and assign roles to all other CCPA users.
Submitter	A Submitter can define, edit, and submit product updates to be tested by a Tester and published by a Signer.
Tester	A Tester can accept or reject product updates that are uploaded to the test LiveUpdate server, depending on the outcome of the testing process. The testing process is optional.
Signer	A Signer can approve product updates for publishing to a test server, approve publishing to the production server, or reject the updates.

Working with the Custom Content Publishing Application

The Custom Content Publishing Application (CCPA) is a self-contained, stand-alone Web application that can be run on any Windows computer. The CCPA server itself must be a computer that is running Windows 2000 Server SP3 or later. CCPA requires Java Development Kit (JDK) version 1.4.x or later. You must also have a code-signing certificate for each trusted Signer. You can provide this Signer certificate in the form of either a standard DER-encoded X.509 certificate file, or the actual PKCS #12 keystore file that is used by the Signer. (In this case, you will need the password that was used to create the PKCS #12 file.)

In addition, you will need a certificate to sign the LOTS file. This certificate must chain up to a trusted root certificate authority (CA) that is listed as a trusted root in the system certificate store. This certificate can be a PKCS #12 keystore file, or it can be selected from the local system certificate store.

CCPA and LOTS file locations and Windows Start menu shortcuts

By default, CCPA files are installed in the following location:

C:\Program Files\Symantec\CCPA

By default, LOTS Manager files are installed in the following location:

C:\Program Files\Symantec\LiveUpdate Publishing

The following shortcuts are placed under LiveUpdate Publishing on the Windows Start menu:

LOTS Manager	Launch the LOTS Manager application. See "Using the LOTS Manager" on page 110.
Login to CCPA	Log onto the CCPA Web interface.
Readme	Read important information not included in this manual.
Start CCPA	Launch the Apache Tomcat service.
Stop CCPA	Stop the Apache Tomcat service.

Planning for content publishing

Before you can publish content using the Custom Content Publishing Application (CCPA), you must perform the following tasks:

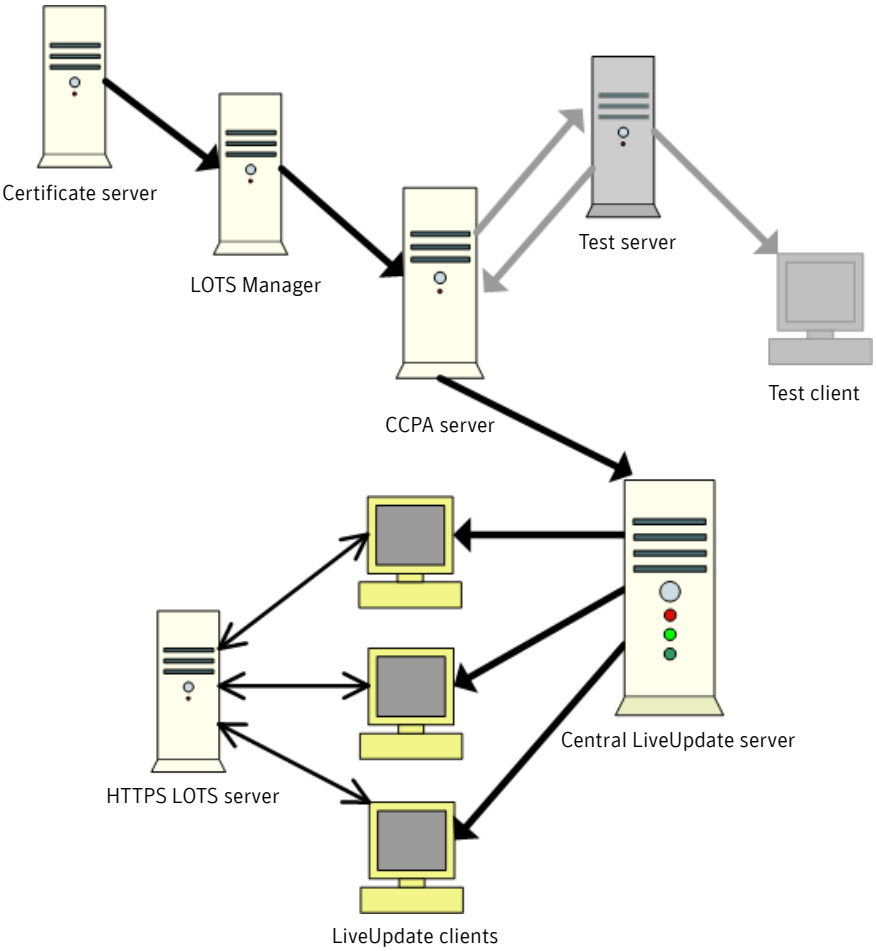
- Upload the List of Trusted Signers (LOTS) file: The LOTS file validates the signature certificates that are uploaded by CCPA Signers from the User Profile page.
- Ensure that you have an HTTPS server for storing the LOTS file that is used by LiveUpdate clients: When the LiveUpdate client runs, it first checks for an updated LOTS file. It compares the LOTS file on the HTTPS server with the copy of the file on the local computer.
- Designate a server to be used for your CCPA production server.

You must install CCPA to a server that is running HTTPS to ensure secure transmissions. When CCPA is installed to an HTTPS server, all communication to and from the server is encrypted. When CCPA is installed to an HTTP server, all communication (including user names and paswords) is transferred in clear text.

See "Enabling SSL support over HTTPS" on page 112.

A typical CCPA environment is shown in Figure 8-1.

Figure 8-1 A CCPA environment



The computer that is running the LOTS Manager obtains certificates from the Certificate server. For security, the server running the Custom Content Publishing Application is brought up only when it is needed to publish updates. A separate server is used to test the Update Packages before they are published to the Central LiveUpdate production server. When LiveUpdate is run on the client computers, it first checks with the LOTS server to verify that the clients' LOTS file is the most current. If the client LOTS is older, a current file is downloaded. Symantec content and custom content are then downloaded from the Central LiveUpdate server and applied to the client.

Installing the Custom Content Publishing Application

The Custom Content Publishing Application and the LOTS Manager are installed separately. While they can be installed on the same computer, as a best practice, it is recommended that you install them on different computers. You will need to install the LOTS Manager and upload a LOTS file before you configure user roles.

See "Using the LOTS Manager" on page 110.

If you install the Custom Content Publishing Application to an SSL server, there are additional steps that you must perform to enable SSL support for CCPA.

See "Enabling SSL support over HTTPS" on page 112.

To install the Custom Content Publishing Application

1. Review the pre-installation information.
   See "Planning for content publishing" on page 107.
2. Start the Custom Content Publishing Application setup program (LiveUpdate CCPA.msi).
3. In the LiveUpdate CCPA InstallShield Wizard window, click **Next**.
4. In the Destination Folder window, do one of the following:
   - Verify that the default destination folder is appropriate (C:\Program Files\Symantec\CCPA\).
   - Click **Change**, and then select a different destination folder.
5. Click **Next**.
6. Click **Install** to start the installation, and then follow the on-screen instructions.

To install the LOTS Manager

1. Start the LOTS Manager setup program (Symantec LiveUpdate LOTS Manager.msi).
2. In the Symantec LiveUpdate LOTS Manager InstallShield Wizard window, click **Next**.
3. Click **Install** to start the installation, and then follow the on-screen instructions.

After you install

After you've installed the Custom Content Publishing Application (CCPA) and the LOTS Manager, you should perform the following basic administrative tasks:

- Create a LOTS file.
  See "Working with certificates" on page 112.
- Specify update servers.
  See "Working with CCPA servers" on page 116.
- Configure users and roles.
  See "Performing administrative tasks" on page 114.
- Specify products and languages.
  See "Browsing audit log entries" on page 128.
- Enable LiveUpdate clients to retrieve custom content.
  See "Enabling LiveUpdate clients to retrieve custom content" on page 129.

Uninstalling the Custom Content Publishing Application

Both CCPA and the LOTS Manager can be uninstalled using Add/Remove Programs in the Windows Control Panel.

The uninstall program for CCPA is located in Add/Remove Programs under LiveUpdate CCPA.

The uninstall program for the LOTS Manager is located in Add/Remove Programs under Symantec LiveUpdate LOTS Manager.

Using the LOTS Manager

The LOTS Manager lets you create and maintain a LOTS (List of Trusted Signers) file, which contains a list of every Signer certificate that LiveUpdate can trust. Multiple certificate file formats are supported, including X.509 (.cer and .crt) and PKCS #7 and PKCS #12 (.pfx and .p12).

Using the LOTS Manager, you can do the following:

- Add new certificates.
- View details of existing certificates.
- Remove certificates.

The LOTS Manager maintains the LOTS internally as an in-memory certificate store through CAPICOM. When you add a certificate to the LOTS, it is added to the in-memory certificate store. When you save the LOTS file to disk, the LOTS Manager retrieves the certificate store in PKCS #7 format. You cannot save the

LOTS file to disk unless you have specified a certificate for signing the LOTS. This certificate, which must be associated with a private key, can either be selected from the Microsoft local certificate store, or you can specify one from an external file (only PKCS #12 password-protected keystores are supported). You can always view the details of a certificate, even if it is not trusted.

If Custom Content has been enabled, the LiveUpdate client automatically looks for a local copy of the LOTS file. It uses the information in this file to authenticate the custom content that is pulled from the Central LiveUpdate server much in the same way that Symantec LiveUpdate verifies and secures the content that is downloaded from the Symantec LiveUpdate site or from the Central LiveUpdate server.

LiveUpdate can be configured to attempt to retrieve a LOTS file from an HTTPS server (the LOTS server). The LiveUpdate client only downloads this LOTS file from the LOTS server in the event that the LOTS file on the local computer is older than the one on the LOTS server.

LiveUpdate verifies that the signature on the LOTS file chains to a trusted root certificate such as Verisign, and checks that the Signer certificate from the Signature File has a matching certificate in the LOTS database. It then checks to see if the Signer certificate has expired and verifies that the format of the Signer certificate is valid. The LiveUpdate client trusts the LOTS server only if its server certificate was issued by a ROOT CA that is identified as a Trusted Root in Internet Explorer.

To start the LOTS Manager

- On the Windows taskbar, click **Start** > **Programs** > **LiveUpdate Publishing** > **LOTS Manager**.

How the LOTS file is used in the custom content publishing process

Before custom content can be downloaded to a client computer, the LiveUpdate client verifies that the content is secure by using the LOTS file.

Custom content is specified and secured in the custtri.zip file, rather than livetri.zip. The custtri.zip file also contains a Guard and Signature file. The only certificate in the Custom Content Signature file is the one that belongs to the user (the Signer) who generated the Signature file. Even if the Signer's certificate has a chain of CAs and a trusted root, those certificates are not included in the Custom Content Signature file, because they are ignored by LiveUpdate. LiveUpdate trusts this Signature file as long as the Signer's certificate can be found in the local LOTS file. The Administrator is responsible for managing the deployment of the LOTS file to the LiveUpdate clients.

The LOTS file can be redeployed if any of its Signer certificates need to be revoked, for example if the private key is compromised or if the Signer leaves the company.

Working with certificates

You use the LOTS Manager to create a LOTS file, which contains a copy of the code-signing certificates that are used by Signers when publishing custom content within the CCPA. The LOTS file is used by the CCPA and by LiveUpdate clients that have been enabled to receive custom content from a Central LiveUpdate server. The LiveUpdate client uses the LOTS file to determine if it can trust the custom content that it downloads from the Central LiveUpdate server.

To work with certificates

1. In the LOTS Manager window, select any of the following:
   - Add Certificate From File: Add a signing certificate.
   - View: View the details of a signing certificate.
   - Remove Certificate: Delete a certificate.
2. To save the LOTS file, under Certificate for signing the LOTS, click **Select**, and then select a certificate for signing the LOTS.
   You can select a certificate from either the System Certificate Store or from an External PKCS #12 File.
3. Click **Select**.
4. If you select a certificate from an external PKCS #12 file, type the password for the certificate, and then click **OK**.
   The LOTS file cannot be saved to disk unless a LOTS-signing certificate has been specified.

Enabling SSL support over HTTPS

To enable SSL support over HTTPS for the Custom Content Publishing Application using a PKCS #12 keystore, you must perform some additional steps. SSL support in CCPA is turned off by default.

Before you begin this procedure, you must have a Web server certificate. You can create your own server certificate using Microsoft Certificate Services or you can create a self-signed certificate using the keytool utility included with the Java Runtime Environment and JDK. Web server certificates can also be obtained from third-party certificate authorities (CA) such as Verisign.

Obtaining a certificate from such a CA will allow your clients to trust the CCPA server implicitly when connecting over HTTPS.

The certificate request should indicate that the private key is exportable and that the intended purpose is Server Authentication. The certificate must also chain to a trusted root.

The certificate issued common name must be the same as the name you are using to connect to the CCPA server. For example, for the CCPA server https://ccpaserver:8443, the name is ccpaserver.

To enable SSL support in CCPA

1. Locate the Server Authentication Certificate file that you want to use from the Certificate Store, and export it to the \webapps directory where the CCPA program files are installed.
   By default, this location is C:\Program Files\Symantec\CCPA\webapps.
2. Edit the server.xml file.
   By default, this is located in C:\Program Files\Symantec\CCPA\conf.
3. Under the section <!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->, do the following:
   - Delete the following: <!-- ** No SSL support, by default ***
   - Delete the following: *** NO SSL support, by default *** -->
   - Locate keystoreFile="c:/ccpa/webapps/.ccpakeystore" and replace it with the path to the certificate that you are using. For example: keystoreFile="C:/Program Files/Symantec/CCPA/webapps/[certificate filename]"
   - Locate keystorePass="ccpa42" and replace ccpa42 with the password used when you exported the PKCS #12 certificate.
   - Add the attribute keystoreType="PKCS12" before /> at the end of the section.

   The resulting section should be similar to the following:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
           port="8443" minProcessors="5" maxProcessors="75"
           enableLookups="true"
           acceptCount="10" debug="0" scheme="https" secure="true"
           useURIValidationHack="false">
  <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
           clientAuth="false" protocol="TLS" keystoreFile="C:\Program
    Files\Symantec\CCPA\webapps\myPKCScert.pfx"
           keystorePass="mypassword" "keystoreType='PKCS12" />
</Connector>
```

4 Save **server.xml**.

5 Restart the CCPA service.
See “Starting and logging on to CCPA” on page 114.

6 Open your browser and type the name of the server that is running CCPA and then append :8443.
For example, https://ccpaserver:8443

To enable SSL on your server using the JKS format instead of PKCS #12, please refer to the Apache Jakarta Web site at http://jakarta.apache.org/tomcat/tomcat-5.0-doc/ssl-howto.html.

Performing administrative tasks

The CCPA Administrator is responsible for configuring CCPA, managing users and update production servers, monitoring audit logs, and maintaining data about the products, languages, and update types that are addressed in CCPA product updates.

When you are logged on as the Administrator, click **Admin** on the main navigation menu to display the administration menu. This menu enables you to navigate through the pages that are used for CCPA administration.

As an Administrator, you can do the following tasks:

- Add and manage users.
- Manage servers.
- Review history.
- Browse audit logs.
- Work with Products, Languages, and Update Types.
- Edit configuration settings.
- Manage publishing sessions.

Starting and logging on to CCPA

Once you start the CCPA service, you can log on to CCPA from the computer that is running the service, or from a remote workstation.

To start the CCPA service

- On the Windows taskbar, click **Start** > **Programs** > **LiveUpdate Publishing** > **Start CCPA**.

To log on to the CCPA Web interface

- Do one of the following:
  - On the local CCPA computer, on the Windows taskbar, click **Start** > **Programs** > **LiveUpdate Publishing** > **Login to CCPA**.
  - On the remote workstation, open a Web browser, type the name of the server that is running CCPA, and then append :8080.
    For example, https://remotetest:8080

  The first time that you log on to CCPA, the default user name and password is admin. You will be required to type a new password before you can proceed.

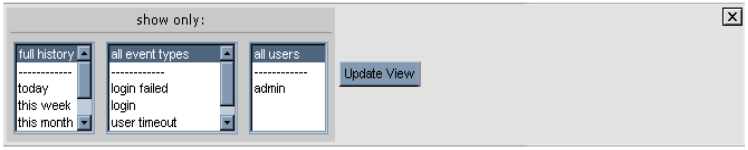
Navigating the Custom Content Publishing Application

The CCPA user interface displays a trail below the menu to keep you informed of where you are and how you got there. Each time that you go to a page, the name of that page appears under the menu in the left side of the browser window. As you continue to other pages under that menu item, CCPA adds a link for each page that you've accessed. You return to the previous page within a menu selection by clicking the link for that page.

Do not use the Back arrow to navigate to the previous page.

On pages that display lists of items, such as updates, users, and servers, you can filter the display using the show only feature in the filter bar above the list. The filter bar is collapsed by default, and you can expand it by clicking the expand icon at the right end of the bar.

When you expand the filter bar, you can select your filtering criteria.



By selecting attributes and clicking **Update View**, you can filter the display to show only those items that are relevant to your task. For example, when browsing the product updates list, you can select products in specific languages and click the update view button to display only those updates that match your selection.

Uploading the LOTS file

You should upload a LOTS file before you configure user roles.

See "Using the LOTS Manager" on page 110.

To upload the LOTS file

1. In the main LiveUpdate - Custom Content window, click **admin**.
2. In the LOTS file status window, click **Upload LOTS**.
3. Click **Browse**, select the LOTS file, and then click **Open**.
4. Click **submit** to upload the file to the CCPA.
5. To cancel your action, click **cancel**.

Working with CCPA servers

You can define your CCPA servers, browse the server list, and establish test and production servers. Initially, you'll define each of your servers as either inactive or test servers. You can then specify an inactive server as the production server.

Work with CCPA servers

The Update View button updates the list according to your selection. You can add or delete servers as necessary, and you can edit the profile of any of your servers. The show only drop-down menu lets you select all types, production, inactive, or test servers.

To add a new server

1. Start CCPA and log on as an administrator.
   See "Starting and logging on to CCPA" on page 114.
2. Click **admin**.
3. Click **LU servers**, and then click **New**.
4. In the add server window, do the following:
   - In the nickname box, type a name for the server.

- In the URL box, type the URL of the server.
- In the Protocol box, select the protocol that is used by the server to transfer data.
  For all protocols, write access must be enabled. You should password-protect the document root where you save the files.
- Select the server to add as either a test server or an inactive server.
  An inactive server can be changed to a production server.
  See "To set an inactive server to a production server" on page 117.
- Optionally, you can specify a user name and password for the server, in case authentication is required to access the server.
  If the server requires a user name and a password, and if you do not provide them as a part of the server profile, the Signer will be prompted to type the user name and password at publishing time.

5 Click **Add Server**.

6 To cancel and reload the default form, click **Reset Form**.

To delete a server

1 In the LU servers window, select the server that you want to delete, and then click **Delete**.

2 Click **Confirm Delete** to delete the server.
You cannot delete a production server nor can you delete a test server that is being used for a publishing session that is currently in progress.

To set an inactive server to a production server

1 In the LU servers window, select the server that you want to change, and then click **Set as production**.

2 In the Confirm Production window, do the following:

- If necessary, type the user name and password.
- Click **Confirm Switch**.

When you set a server as the production server, CCPA goes into a maintenance state until it is synchronized with the new production server. All users that are logged on are prevented from accessing CCPA functions.

You can only have one production server. To set a server as a production server, its current type must be set to inactive. To set a test server to production, you must first change its type to inactive, and then set it to production.

CCPA validates the server, and if it is verified, it switches the inactive server to a production server.

Synchronizing the CCPA database with the production server

The Synchronize option appears only when the selected server is the current Production server.

Once you confirm the synchronize, CCPA goes into the maintenance state. While in maintenance state, all logged on users are prevented from accessing any CCPA functions.

When synchronizing servers, CCPA performs the following actions:

- The production server contacts the remote LiveUpdate server using the selected server protocol.
- The production server downloads update details (TRI file) from the remote server.
- All existing update details (TRI records) are removed from the CCPA database.
- The CCPA database is populated with the new update details.
- CCPA enters the available state, and users can access all CCPA functions.

To synchronize the CCPA database with the production server

- Click **Synchronize**.

Working with User Profiles

You can view and update the information that identifies your CCPA users. With the exception of user name, you can change the information as needed to update the user's profile information.

Note: Once you establish each user's user name, it cannot be changed. To change a user name, you must first delete the user record and then create a new one.

You create a password for each user. Passwords can be edited by users at any time. You also type the first name, last name, and email address of each user. Users can also edit this information.

The role(s) box is available only to CCPA Administrators. This is where you assign each user one or more user roles. User roles determine permissions and work flow in CCPA.

See "Roles and users" on page 106.

Note: If you change a user's role while the user is logged on, the change does not take effect until that user's next log on.

CCPA users who are assigned the role of Signer must have a signing certificate uploaded to the system. When you set up or update a user with the role of Signer, the value of this box is missing. You can upload the Signer's certificate or allow the individual Signers to upload and manage their own signing certificates.

See "Uploading a signing certificate" on page 159.

Adding new users

When you add new users and the information that identifies them to the CCPA system, you assign roles to them according to the tasks that they perform. You can also change the roles of your users as needed.

See"Roles and users" on page 106.

Some information can be edited only by CCPA Administrators. However, all users can update their own personal information.

To add a new user

1. Start CCPA and log on as an administrator.
   See "Starting and logging on to CCPA" on page 114.
2. Click **admin**.
3. Click **users**, and then click **New**.
4. To add a new user, do the following:
   - In the username box, type the name of the user.
   - In the password box, type the password for the user.
     Users can change their passwords by accessing their profiles on the My Profile window.
   - In the verify password box, re-type the password.
   - In the first name box, type the first name of the user.
   - In the last name box, type the last name of the user.
   - In the email address box, type the email address for the user.
     Users can edit their first and last names and their email addresses in the My Profile window.
   - In the role(s) box, define the user's role. The roles are Administrator, Signer, Submitter, and Tester.

Users who are assigned to the Signer role must upload their signing certificates to validate their authority to publish product updates.
See "Uploading a signing certificate" on page 159.

5 Click **Save**.

6 To cancel your changes without saving, click **Reset Form**.

Managing User Profiles

The user list is accessible only to CCPA Administrators. You can sort, filter, and display all current users. In addition, you can add new users, delete users, and force users to log off. When you click a user name, you will see the User Profile page where you can maintain and update the information that identifies your CCPA users. Current profile for... displays the name of the user that you selected on the Users page. With the exception of user name, you can change the information as needed to update the user's profile information.

Note: To save your changes, click **update profile**. Otherwise, your changes will be lost.

Working with products and languages

You can view all of the product names and languages in the CCPA database. These are the lists that Submitters use when they select product names and languages to define or modify product updates. You can add, delete, import, or export product names and languages.

CCPA includes a default list of Symantec products and languages. You can select the products and languages that you want Submitters to select from when they work with Symantec content.

To work with products and languages

1 Start CCPA and log on as an administrator.
See "Starting and logging on to CCPA" on page 114.

2 Click **admin**.

3 Select one of the following

- products: Work with products
- languages: Work with languages

4 To add a new product or language, in the new box type the name of the custom content product or language, and then click **Add**.

5 To delete a listed product or language, select it, and then click **Delete**.

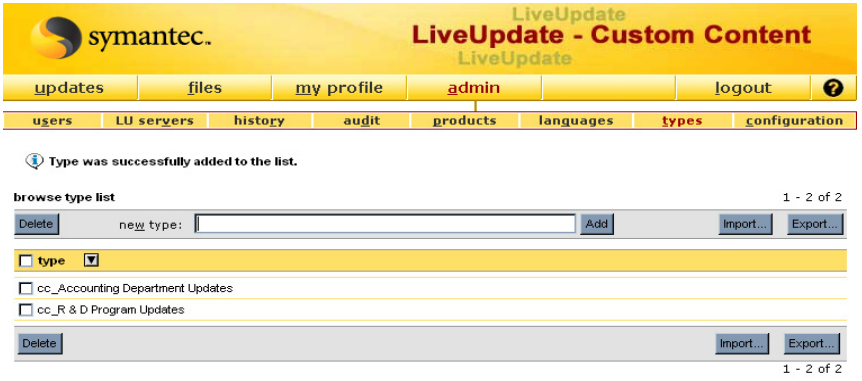
6 To import a list of products or languages, click **Import**.
The list should be a flat text file with a single product or language on each line. When the import process has completed, a message confirms the import, along with a summary of how many records in the import file were processed, how many were imported, how many were duplicates of existing records, and how many were rejected. Records are rejected if they are too long or if they contain non-printable characters. The maximum length is 250 characters.

7 To export a list of products or languages, click **Export**.
You can export a flat text file that lists all of the products or languages to a location that you select.

Working with update types

You can categorize custom content updates by giving them distinctive names. For example, if you have custom content updates for your accounting department, you could create a type called Accounting Department Updates. When this is added to the types list, CCPA adds cc_ to let users know that this update contains custom content. The type appears in the list as cc_Accounting Department Updates (Figure 8-2).

Figure 8-2 CCPA product type list



You can browse the update type list, delete existing types, and add new types of custom content updates. You can also import and export the list of file types. The list consists of the types of updates that are available for a Submitter to select from when defining a new update or modifying an existing product update.

A Submitter can also add updates to this list by entering them during a publishing session.

To work with update types

1. Start CCPA and log on as an administrator.
   See "Starting and logging on to CCPA" on page 114.
2. Click **admin**.
3. Click **types**.
4. To add a new update type, in the new type box, type the name and then click **Add**.
   The update type is added to the list, and cc_ is added to the beginning of the name.
5. To delete a listed update type, select it, and then click **Delete**.
6. To import a list of update types, click **Import**.
   The list should be a flat text file, with a single product or language name on each line. When the import process has completed, a message confirms the import, along with a summary of how many records in the import file were processed, how many were imported, how many were duplicates of existing records, and how many were rejected. Records are rejected if they are too long or if they contain non-printable characters. The maximum length is 250 characters.
7. To export a list of update types, click **Export**.
   You can export a flat text file that lists all of the products or languages to a location that you select.

Setting the System Configuration

You can modify the application configuration parameters. These are system-wide settings that determine how information is presented and handled for all CCPA users.

Running LiveUpdate

You can download and apply updates for CCPA by running LiveUpdate from the configuration page. When you run LiveUpdate, you are logged off during the LiveUpdate session.

To run LiveUpdate from CCPA

1 Start CCPA and log on as an administrator.
See "Starting and logging on to CCPA" on page 114.

2 Click **admin**.

3 In the configuration window, under invoke LiveUpdate, click **LiveUpdate**.
All updates that apply to the Custom Content Publishing Application are downloaded from the LiveUpdate server.

Editing Application configuration settings

You can change the number of rows that appear on a page, the number of history records that are kept, the length of passwords and user names, log on and security settings, and email notification.

To edit application configuration settings

1 Start CCPA and log on as an administrator.
See "Starting and logging on to CCPA" on page 114.

2 Click **admin**, and then click **configuration**.

3 To change the general application configuration settings, do the following:

- In the maximum rows per page box, type the number of rows to display.
This determines the maximum number of rows per page for all lists.
- In the maximum session history records, type the number of records to be maintained in history.
You can review history on the History page.
- To enable debugging, click **Yes**.
This turns on verbose debugging information. This is disabled by default, and only error messages are displayed.
- To enable the progress page, click **Yes**.
A progress page is a way of showing the user that the system is executing the submitted action. If this is not enabled, users will see the process icon of their browser.
- To accept all LiveUpdate server certificates, click **Yes**.
If you click Yes, any HTTPS certificates that are installed on the server are accepted. If you click No, a trusted authority such as Verisign is required.

4 To change login and security settings, do the following:
   - In the minimum username length box, type the number that specifies the minimum number of characters that are required for a CCPA user's user name.
     The default is four.
   - In the minimum password length box, type the number that specifies the minimum number of characters that are required for a CCPA user's password.
     The default is four.
   - In the maximum number of unsuccessful login attempts box, type the number of times a user can attempt to log on before the user is locked out of CCPA.
   - In the login lockout duration in minutes box, type the number of minutes a user will be locked out of CCPA after the maximum number of log on attempts is reached.

5 To change email notification settings, do the following:
   - To enable notification messages, click **Yes**.
     Users will be notified by email when the status of a publishing session requires their attention. This is the default.
   - To disable notification, click **No**.
   - If you are enabling notification, type the name of the SMTP server.
     If SMTP server is not valid, this causes a significant slowdown.
   - Type the login ID for the SMTP server (optional).
   - Type the password for the SMTP server (optional).

6 To save the settings, click **Update**.

7 To cancel and reload the previous settings, click **Reload**.

8 To restore the default settings, click **Reset to Defaults**.
   The Confirm Reset to Defaults window displays the configuration parameters along with the default value for each one.

9 Click **Confirm** to accept the defaults, or click **Cancel** to continue editing the configuration.

Resetting the session timeout value

The session timeout value is the number of minutes CCPA is idle during a publishing session. When a user has a session open without activity for the specified timeout period, CCPA automatically logs that user off. The default session timeout period is 10 minutes.

You can reset the timeout value.

To reset the timeout value

1. Open the **web.xml** file located at:
   c:\ccpa\webapps\ccpa\web-inf\web.xml
2. Find the following line in the web.xml file:
   <session-config><session-timeout>10</session-timeout></session-config>
3. Change the <session-timeout> value to the number of minutes that are required.
4. Restart CCPA.

Managing publishing sessions

When the publishing session is locked, the LiveUpdate publish status box informs you of the current session type (add, delete, or modify) and whether the session is awaiting a Tester or a Signer.

You can do any of the following:

- Change the current state of the session.
- Change the session participants.
- Cancel a publishing session.
- Browse audit log entries.
- View session history.

Modifying the state of a publishing session

You can modify the current publishing session as long as a session is in process and not submitted. You can cancel the session and return it to the Available state so that a Submitter can begin a new publishing session, or you can return the session to the In Work state so that the current session Submitter can add

update definitions and re-submit the publishing session. The session attributes are listed in Table 8-2.

Table 8-2 Current session attributes

Attribute	Description
Session state	This is the current state of the session, which can be: ■ In Work: The current publishing session is locked by a submitter and is not yet submitted. ■ Submitted: The current publishing session is locked and has been submitted for signing and testing. ■ In Test: The current publishing session has been uploaded to the test LiveUpdate server by the Signer. ■ Approved: The current publishing session has been approved by the Tester and is ready to be published.
Submitter	The Submitter's name.
Signer	The Signer's name. If the session is in work, and the Submitter has not specified a Signer, this box displays not selected.
Tester	The Tester's name. If the session is in work, and the Submitter has not specified a Tester, this box displays not selected.
Test LU server	The name of the test LiveUpdate server. If the session is in work, and the Submitter has not specified a test server, this box displays not selected.
Select new session status	Select the new status that you want to set for the session. Only supported new session states are listed. The displayed session transitions depend on the current publishing session state.
Enter update message	If you want to write a message regarding the publishing session state change, you can type up to 500 characters in this text box. This text is included in the email notification message that is sent to all of the effected parties.
Cancel	Cancel your actions. You are returned to the Updates window. Nothing will be changed.
Modify session state	Confirm your modification of the session state.

To modify the state of a publishing session

1 Start CCPA and log on as an administrator.
See "Starting and logging on to CCPA" on page 114.

2 In the updates window, LiveUpdate publish status box, click **modify session state**.

3 Select a new session status.

4 In the enter update message box, type a message to send to session participants.
You can type up to 500 characters.

5 Click **modify session state**.

Modifying session participants

You can change the participants of the current publishing session. You can change the session's current Submitter, Signer, Tester, or test LiveUpdate server.

To modify session participants

1 Start CCPA and log on as an administrator.
See "Starting and logging on to CCPA" on page 114.

2 In the updates window, LiveUpdate publish status box, click **modify session participants**.

3 In the Current session participants window, in the select new submitter list, select a new Submitter for the current publishing session.

4 If a session has already been submitted, do any of the following:

- In the select new signer list, select a new Signer.
  All users who have been defined as Signers are listed.
- In the select new tester list, select a new Tester.
  All users who have been defined as Testers are listed.
- In the select test LU server list, select a new test LU server.
  This displays all of the servers that have been defined as test servers.
- In the enter an update message box, type a message of up to 500 characters.

5 Click **change**.
Any changes that you make immediately become effective.
CCPA generates email notifications to the users who are involved in the change.

6 To save your changes, click **modify**.

7 To cancel your changes, click **Cancel**.
The session attributes remain unchanged.

Canceling a publishing session

You can cancel a publishing session at any time.

To cancel a publishing session

1. On the updates page, in the LiveUpdate publish status box, click **cancel updates**.
   The Confirm Cancel Updates window warns you that your action will discard all changes defined in the session and asks you if you are sure you want to cancel the session.
2. Click **yes** to cancel.
   The session and all changes associated with it are canceled.

Browsing audit log entries

You can view the major events that are captured by the audit log. Major events are recorded for auditing purposes, such as user log ons, log offs, publishing session state changes, user and server modifications, unauthorized access attempts, and so on.

The following viewing and export options are available:

Show filter	The show only option allows you to filter and sort the display. You can select the length of history from current day to full history, select event types from specific events to all, and specify individual users or all users.
Update View	Updates the log according to the filtering criteria that you've selected.
Set audit log size	The audit log size specifies the number of records to be stored in the audit log. Once this limit is reached, records are removed starting with the oldest. On the drop-down menu, select a number of records to be stored in the log. Click **apply to** refresh the display.
Export	Exports the log to a CSV (Comma Separated Values) file.

To browse audit log entries

1. Start CCPA and log on as an administrator.
   See "Starting and logging on to CCPA" on page 114.
2. Click **admin**, and then click **audit**.

Viewing CCPA history

You can view details of completed CCPA publishing sessions. The number of sessions that are retained in history depends on the setting that is specified by the CCPA Administrator. For each completed session, the History page displays the following information:

Completed	The completion date and time of the publishing session
Started	The start date and time of the publishing session
Action	The action that was performed in the session: Insert, modify, or delete
Submitter	The Submitter's name (visible only to Administrators)
Signer	The Signer's name (visible only to Administrators)
Tester	The Tester's name (visible only to Administrators)
Test Server	The name of the test server that was used in the session
Production Server	The name of the production server that was used in the session
Product Update List	The product update list included in the publishing session For each session, the History window shows: ■ Product name ■ Version number ■ Language ■ Update type ■ Sequence ■ File

Enabling LiveUpdate clients to retrieve custom content

You must configure your LiveUpdate clients to automatically retrieve custom content. By default, custom content is disabled in the client's Settings.LiveUpdate file.

To enable LiveUpdate clients to retrieve custom content

1 On the client computer, open the Settings.LiveUpdate file.
See "About LiveUpdate client configuration files" on page 63.

2 Add the following settings:
- Enable custom content. Type **PREFERENCES\CUSTOM_CONTENT=1**

This enables the client to retrieve a custtri.zip file from the Central LiveUpdate server.

- Enable the LiveUpdate client to check for a new LOTS file. Type **LOTS\UPDATE_LOTS_FILE=YES/OPTIONAL/NO**
  If this is set to YES and the LOTS file retrieval fails, LiveUpdate disables custom content for that session.
  If this is set to OPTIONAL, the LiveUpdate client looks for a new LOTS file, but if the file retrieval fails, custom content is still downloaded.
  If this is set to NO, the LiveUpdate client does not look for a new LOTS file.
- **LOTS\LOTS_HTTPS_URL=**
  The URL of the HTTPS server hosting the LOTS file.
- **LOTS\LOGIN=**
  User name to use to log on to the HTTPS server hosting the LOTS file. LiveUpdate encrypts this automatically when it runs.
- **LOTS\PASSWORD=**
  Password to use to log on to the HTTPS server that is hosting the LOTS file. LiveUpdate encrypts this automatically when it runs.
- **LOTS\LOTS_FILE (<PER_MACHINE_FOLDER>\LIVEUPDT.LTS)=**
  The LOTS file name and path that are used instead of the default location.

If you do not specify a LOTS server, the LiveUpdate client can still retrieve custom content if it has been enabled, but you must have a copy of the LOTS liveupdt.lts file on the local computer. The liveupdt.lts file must be copied to the same folder as Product.Inventory.LiveUpdate.

See "LiveUpdate client file locations" on page 62.

For example, the following statements enable custom content, and specify a server, Symfiles, hosting the LOTS file in the LOTSDIR folder. The client looks for a new LOTS file each time that LiveUpdate runs. The client's LOTS file is called MYLOTSFILE.LTS and is in the C:\LOTSDIR\ folder.

LOTS\LOGIN:ENC=*P_A?Q0VSHE

LOTS\LOTS_HTTPS_URL=https://Symfiles/LOTSDIR

LOTS\PASSWORD:ENC=4V#GO=M=B\TC(%+!24M?+A

LOTS\UPDATE_LOTS_FILE=YES

LOTS\LOTS_FILE=C:\LOTSDIR\MYLOTSFILE.LTS

PREFERENCES\CUSTOM_CONTENT=1

When custom content has been enabled, LiveUpdate clients display Symantec LiveUpdate Custom Content updates in the LiveUpdate Status window when LiveUpdate is run (Figure 8-3).

Figure 8-3 LiveUpdate Status window with custom content enabled

Chapter 9

Publishing custom content

This chapter includes the following topics:

About the content publishing session

A content publishing session is the process of defining (adding, deleting, or modifying) a set of product updates, optionally testing the updates, and then publishing them to a Central LiveUpdate server. Only one publishing session can exist at any time and each publishing session can be used for only one action type: create new, delete, or modify product updates. Once a Submitter starts a publishing session, the publishing session process (workflow) is locked to all other users except the session participants and the CCPA Administrators.

At any given time, the current publishing session status is in one of the states shown in Table 9-1.

Table 9-1 CCPA publishing session status

State	Description
Available	When no product updates are in process, the publishing session is in the Available state and ready for a Submitter to start defining product updates. Any user can browse the Updates window and select and view the details of existing product updates. However, only a Submitter can start a product updates publishing session.

Table 9-1 CCPA publishing session status

State	Description
In Work	Once a Submitter has started a publishing session, the session status is In Work. While the session is In Work, it is locked to all other Submitters. Only the Submitter who started the session can define product update changes. All information in the current session is read-only to all other users. The In Work status remains unchanged until one of the following occurs: ■ The Submitter cancels the publishing session. ■ The Submitter submits the session for testing or publication. The Submitter can submit the defined product update changes for testing, or directly to production. The Submitter selects the Signer and optionally the Tester and test server, if testing is desired.
Submitted	When the Submitter submits product updates for testing or publication, the publishing session status goes to Submitted. The session remains locked in the Submitted state until the selected Signer either rejects the updates or signs and publishes them to either the selected test server or the production server. If the Signer rejects the updates, the publishing session returns to the In Work state and remains locked to all users except the originating Submitter. The Submitter can then make the needed changes and resubmit the updates.
In Test	When the Signer signs and publishes the product updates to the test server, the publishing session goes to In Test. The session remains locked in the In Test state until the Tester who performs the testing either rejects the updates or approves and passes them on to the Signer. If the Tester rejects the updates, the publishing session returns to the In Work state and remains locked to all users except the originating Submitter. The Submitter can then make the needed changes and resubmit the updates.
Approved	When the Tester approves the product updates on the test server, the publishing session goes to Approved. **Note:** If the originating Submitter did not select a Tester and test server, the publishing session goes directly to the approved state. The session remains locked in the Approved state until the Signer either publishes the updates to the production server or rejects them. If the Signer rejects the updates, the publishing session returns to the In Work state and remains locked to all users except the originating Submitter. The Submitter can then make the needed changes and resubmit the updates.

Once the publishing session is in the Approved state, the Signer signs and publishes the approved updates to the Central LiveUpdate server, and the publishing session returns to the unlocked Available state. The publishing session stays unlocked in the Available state until a Submitter starts another session.

To perform a publishing session

1. The Submitter starts a publishing session, selects and defines the updates to be included in the package, creates any necessary PreConditions, and then submits the update to either a test server or directly to a production server.
   See "Using PreConditions" on page 139.
   See "Submitting updates" on page 135.
2. The Signer publishes the submitted product updates to the test server, if one is used, and to the production server.
   See "Signing and publishing updates" on page 158.
3. The Tester tests the updates on a LiveUpdate test server. If the update passes testing, the Tester marks the update as Approved. If the test fails, it is marked Test Failed and sent back to the Submitter. This is an optional step, but it is recommended.
   See "Testing product updates" on page 161.
4. The Signer publishes the approved update to the production server.
   See "Signing and publishing updates" on page 158.

Submitting updates

CCPA allows only one publishing session at any time, and only one type of edit operation per session. The workflow process of submitting a product update begins with the publishing session in the Available state.

The options that are available are dependent upon the type of session that you have selected. For example, if you are defining new updates, the Delete option does not appear. If you are deleting updates, the New options do not appear. If you are modifying updates, neither the New nor the Delete options appear.

In addition to defining and submitting updates, you can manage the files (update packages) that are associated with the updates. You can modify the files as needed, and delete them when they become obsolete.

To submit updates

1. In the Updates window, in the LiveUpdate publish status box, click **Start Publishing Session**.
   This locks the session, which marks it In Work.

2 In the Start Session Confirm window, click **Define New Product Updates**.
The publishing session is locked once you confirm your selection. In this state, the publishing session is locked to other users, although they can browse updates.

CCPA displays a message stating that the publishing session has been locked. The Status box indicates your session type (New, Replace, or Delete) and identifies you as the Submitter of the current session.

Until you have completed or cancelled the session, you are not allowed to begin another session. The state of the publishing session persists between log ons. That is, when you initiate a publishing session, and log off of CCPA, the state of the publishing session is as you left it when you log back on. You are able to continue performing the previously selected type of edit operation (New, Replace, or Delete).

Once the session is started, the status of your session is In Work, and you are the only Submitter allowed to work with that publishing session. For example, if another Submitter has locked the publishing session, no matter what its current state, the publishing session is not available to you until the status of the publishing session returns to Available. Additionally, if you have a session in process, you cannot begin another session until the updates of your current session have been either published or cancelled.

Defining product updates

You can publish updates for Symantec products or for independent (non-Symantec) products.

Note: The maximum file size should not exceed 100 MB.

To define Symantec product updates

1 In the update window, click **New Symantec Update**.

2 In the Product box, select the product for which you are defining updates.

3 In the Version box, type the version number of the product for which you are defining updates.

4 In the Language box, select the language of the product for which you are defining updates.

5 Under Update Type, do one of the following to specify the Update Type that applies to your update.

- Select an Update Type: (ItemSeqName) from the list and then edit it in the text field.
- Type it directly.

6 Under Sequence Date: (ItemSeqDate), do one of the following:

- Accept the default.
- Type the current date.
  Initially, the current UTC time is displayed. If you enter a new date, you can return to the default value by clicking **Reset**.

7 Click **Edit** to define or edit PreConditions for your update.
For a new update, this box is not defined.
See "Using PreConditions" on page 139.

8 In the Item Name box, type a name for the update (up to 250 characters).

9 In the Description box, type a description for the update.
The File Name box displays the name of the update file, if one has been selected. You can select an update file from either a local directory, or from the list of currently used update files (GRD).

10 To select a file, do one of the following:

- To select a local file, click **New local file**, type the directory path of the local file that you want to use for your update, or click **Browse** to select the file. When you have specified which file you want, click **select**.
  You are returned to the New Product Update window.
- To select a new file from GRD, click **New file from GRD**, select a file from the list, and then click **select**.
  You are returned to the New Product Update window.
  The File Size box displays the size of the selected file.
  The SHA-1 box displays the sha-1 calculation of the file that you selected.

11 In the Action Item box, do the following:

- For a local file, select the executable or script to insert into the Action Item text box.
- For a GRD, the Action Item box displays the associated script or executable.
- Specify and edit the command-line parameters for the selected action item.
  Optionally, you can enter your command-line parameters in the text box.

12 To save the product update definition, click **Save Update**.
The session remains in the In Work state and returns to the Updates window.

13 To submit the update, click **Submit**.

Defining independent custom updates

An independent custom update consists of files that are not associated with Symantec products.

To define an independent product update

1 In the update window, click **New Custom Update**.

2 Under Update Type, specify the Update Type that applies to your update. You can select an Update Type: (ItemSeqName) and edit it in the text box, or enter it directly.

3 Under Sequence Date: (ItemSeqDate), accept the default or type the current date.
Initially, the current UTC time is displayed. If you enter a new date, you can return to the default value by clicking **Reset**.

4 To define or edit PreConditions for your update, click **Edit**.
For a new update, this box is not defined.
See "Using PreConditions" on page 139.

5 In the Item Name box, type a name for the update (up to 250 characters).

6 In the Description box, type a description for the update.
The File Name box displays the name of the update file, if one has been selected. You can select an update file from either a local directory, or from the list of currently used update files (GRD).

7 To select a file, do one of the following:

- To select a local file, click **New local file**. Type the directory path of the local file to use for your update, or click **Browse** to select the file, and then click **select**.
  You are returned to the New Product Update window.
- To select a new file from GRD, click **New file from GRD**, select a file, and then click **select**.
  You are returned to the New Product Update window.
  The File Size box displays the size of the selected file
  The SHA-1 box displays the sha-1 calculation of the file that you selected.

8 The Calculate Sha-1 hash box lets you calculate the SHA-1 of a local file. Enter the File Name or Browse to a file, and then, optionally, type the max bytes (Maximum Number of Bytes) to use.

9 Click the calculate sha-1 button to calculate the sha-1 for the selected file. Your output is displayed below the Calculate Sha-1 hash box.

10 In the Action Item box, do the following:

- For a local file, select the executable or script to insert into the Action Item text box.
  For a GRD, the Action Item box displays the associated script or executable.
- Specify and edit the command-line parameters for the selected action item.
  Optionally, you can type your command-line parameters in the text box.

11 To save the product update definition, click **Save Update**.
The session remains in the In Work state and returns you to the Updates page.

12 To submit the update, click **Submit**.

Using PreConditions

PreConditions offer you a powerful tool to target LiveUpdate content to specific computers. PreConditions allow updates to be filtered based on several different filtering operators. For example, you can filter updates based on the operating system of the target computer, the language of the operating system, LiveUpdate settings and more.

When PreConditions are not used, much of the logic as to whether or not an update should be installed is based on the sequence number found in the client's Product Inventory. LiveUpdate defines a new update as any update whose sequence number is higher than the installed product to which it is targeted. The logic for this process is within the update package itself, and the package must first be downloaded to evaluate the necessity of the update.

See "How LiveUpdate works" on page 21.

Using PreConditions, you can refine the update process so that LiveUpdate content is only downloaded by the client computer that actually needs the update. This not only conserves bandwidth, but it also minimizes network traffic.

For example, using PreConditions, you can specify that a particular update can only be applied if the update for another Symantec product or component has

already been retrieved and installed. Because PreConditions are specified in the .tri file, the LiveUpdate client can decide which updates are to be filtered out prior to retrieving the actual updates.

Because a PreCondition is used to either select an update for download or to reject the update, the PreCondition is specified as a Boolean expression, returning either True or False. When the expression evaluates to True, the update is flagged for downloading.

About PreCondition syntax

PreCondition expressions can range from simple to complex and they make calls to one or more predefined PreCondtion functions that query one or more attributes on the client computer. The PreCondition expression is assigned to the system variable called bSelect, and ends with a semi-colon:

bSelect = <PreCondition expression>;

PreConditions also support specifying function calls as parameters to other functions, which allows you to build more complex expressions;

bSelect = funct1(123, funct2(), “hello”);

A new line is not interpreted as the end of a statement. This allows you to separate long statements into multiple PreCondition lines. Like C language conditional expressions, you can create complex PreCondition expression using standard Boolean operators including “&&” (and) and “||” (or):

bSelect = funct1(123) && (funct2() || (funct3(“product”)<5));

PreCondition operators are based on C language syntax with a defined set of functions and variables. The available operators are infix, unary, and function (prefix) operators. PreCondition functions accept the following parameter and return values:

Data type	Range	Description
Bool	True/False	Boolean type
Long	-9223372036854775808 to 372036854775807	64-bit signed integer; any number value that doesn't use a decimal point.
Double	-1.7E=308 -2.7E+308	Double-precision floating point number; any number that uses a decimal point or is in the floating point format of 17E+20.
String		Unicode string; constants are specified by surrounding the string with double-quotes.

Syntax rules

When you use the Custom Content Publishing Application to create a LiveUpdate PreCondition, it ensures that the PreCondition expression is added to the .tri file in the correct format. The PreCondition Editor evaluates the PreCondition statement and verifies it for proper syntax.

The PreCondition syntax rules are as follows:

- PreCondition operators and function names are case-sensitive
- Whitespace outside of quoted strings is ignored
- The order of precedence for operators, from highest to lowest, is <, >, <=, >=, ==, !=, &, ›, |, &&, ||, prefix operators.
- The backslash "\" and period "." characters must be preceded by an escape character ("\") within any quoted strings. For example, if a string must be read as "Program Files\Symantec", then you would specify \"Program files\\Symantec\"

Infix and unary operators

Table 9-2 and Table 9-3 describe the available infix and unary operators.

Table 9-2 Infix operators

Operator name	Description	Parameters	Return
<	Less than operator. Lexicographically compares arguments when parameters are strings.	<long | double | string><long | double | string> Strings can only be compared to strings.	<boolean>
<=	Less than or equal to operator. Lexicographically compares arguments when parameters are strings.	<long | double | string><long | double | string> Strings can only be compared to strings.	<boolean>
>	Greater than operator. Lexicographically compares arguments when parameters are strings.	<long | double | string><long | double | string> Strings can only be compared to strings.	<boolean>
>=	Greater than or equal to operator. Lexicographically compares arguments when parameters are strings.	<long | double | string><long | double | string> Strings can only be compared to strings.	<boolean>

Table 9-2 Infix operators

Operator name	Description	Parameters	Return
==	Equals operator.	<long | double | bool | string><long | double | bool | string> Boolean values can only be compared to boolean values, and strings can only be compared to strings.	<boolean>
!=	Not equal to operator.	<long | double | bool | string><long | double | bool | string> Boolean values can only be compared to boolean values, and strings can only be compared to strings.	<boolean>
&&	And operation on two boolean values. Returns true only when both input values are true.	<bool><bool>	<boolean>
||	Or operation on two boolean values. Returns true when at least one of the input values is true.	<bool><bool>	<bool>
^	Bitwise xor operation on two long values.	<long><long>	<long>
&	Bitwise And operation on two long values.	<long><long>	<long>
|	Bitwise Or operation on two long values.	<long><long>	<long>
+	String concatenation function. String2 is appended to string1. Does not work for numbers.	<string><string>	<string>

Table 9-3 describes the available unary operators.

Table 9-3 Unary operators

Operator name	Description	Parameters	Return
!	Takes in a boolean value and flips the value (true becomes false, false becomes true).	<bool>	<boolean>

Functions

Table 9-4 describes the available functions.

Table 9-4 Functions

Operator name	Description	Parameters	Return
StringIndexOf	Returns index of first instance of string1 in string2.	<string><string>	<long> -1 if substring is not found. Otherwise, returns the index of the substring.
AppendPath	An AppendString for two string values that represent parts of a path. The function ensures that a path separator is present in the returned string between string1 and string2.	<string><string>	<string>
ToLower	Convert string to lowercase.	<string>	<string>
ToUpper	Convert string to uppercase.	<string>	<string>
GetSettingsProp	Retrieves the value for a LiveUpdate setting.	<string>	<string> If the setting does not exist or is encryupted, <NULL> is returned.
GetSeqNum	Retrieves the sequence number for a given Product, Version, Language, and Type (PVLT).	Product Name <string> Version <string> Language <string> Type <string>	<long> If a PVLT does not exist, -1 is returned.
GetSeqNumby Moniker	Retrieves the sequence for a given LiveUpdate moniker.	Moniker <string> Type <string>	<long> If moniker does not exist, -1 will be returned.
GetProductProp	Retrieves the value of a property set for a given PVL.	Product Name <string> Version <string> Language <string> PropName <string>	<string> If property does not exist, <NULL> is returned.
GetProductPropBy Moniker	Retrieves the value of a property set for a given registered moniker.	Moniker {<string>} PropName <string>	<string> If property does not exist, <NULL> is returned.

Table 9-4 Functions

Operator name	Description	Parameters	Return
GetOSName	Retrieves a general name of the operating system.	<none>	<string> This version correctly identifies Window. Support for the following will be added later: ■ Macintosh ■ Linux ■ Solaris ■ AIX ■ S/390 ■ OS/400
GetOSVerMajor	Retrieves the major version number of the operating system.	<none>	<long>
GetOSVerMinor	Retrieves the minor version number of the operating system.	<none>	<long>
GetOSSPMajor	Retrieves the major version number of the Service Pack level of the operating system. Win32 specific.	<none>	<long>
GetOSSPMinor	Retrieves the minor version number of the Service Pack level of the operating system. Win32 specific. GetOSSPMinor cannot differentiate between Service Pack releases that differ at the letter version level. For example, the value 0 is returned on Windows XP computers that have SP 1.0 or SP 1.0a.	<none>	<long>

Table 9-4 Functions

Operator name	Description	Parameters	Return
GetOSSuiteMask	Retrieves the OS suite mask. Win32 specific.	<none>	<long> OS suite mask as used by the OSVERSIONINDEX struct. A bitwise & operation can be done on this mask to get more granular details about the operating system. The following values were defined in <winnt.h> and are possible numerical values that may be used: ■ VER_SUITE_BACKOFFICE 0x00000004 ■ VER_SUITE_DATACENTER 0x00000080 ■ VER_SUITE_ENTERPRISE 0x00000002 ■ VER_SUITE_SMALLBUSINESS 0x00000001 ■ VER_SUITE_TERMINAL 0x00000010 ■ VER_SUITE_BLADE 0x00000400 ■ VER_SUITE_PERSONAL 0x00000200 This function is unsupported on Windows 9x and versions prior to NT4 SP6. Zero is returned when this function is used on these platforms. The following MSDN link describes how to detect the different versions of Windows: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/getting_the_system_version.asp

Table 9-4 Functions

Operator name	Description	Parameters	Return
GetWinOSProduct Mask	Retrieves the operating system product mask. Win32 specific.	<none>	<long> OS product mask as used by the OSVERSIONINFOEX struct. A bitwise & operation can be done on this mask to get more granular details about the operating system. The following values were defined in <winnt.h> and are possible numerical values that may be used: ■ VER_NT_WORKSTATION 0x0000001 ■ VER_NT_CONTROLLER 0x0000002 ■ VER_NT_SERVER 0x0000003 This function is unsupported on Windows 9x and versions prior to NT4 SP6. Zero is returned when this function is used on these platforms.
GetHostName	Retrieves the name of the computer.	<none>	<string> <NULL> is returned if there is a problem determining the host name.
GetDomainName	Retrieves the domain name of the computer. This function only reliably returns the domain name on computers that are part of an NT or Active Directory domain. The domain name that is returned in this case is the name that is registered with the DNS servers.	<none>	<string> <NULL> is returned if there is a problem determining the domain name or none was set.
GetEnvVar	Retrieves the value of a given environment variable.	Param1: string (environment variable name)	<string>

Table 9-4 Functions

Operator name	Description	Parameters	Return
GetFileHash	Calculates the SHA-1 hash of a given file. The length of the hash is 20 bytes, therefore, this function returns a 40 character string of hexadecimal characters that represent the hash.	string (file name/path)	<string> If there are problems calculating the hash, <NULL> is returned.
GetPartialFileHash	Calculates the SHA-1 hash of the first n bytes of a given file. The length of the hash is 20 bytes, therefore, this function returns a 40 character string of hexadecimal characters that represent the hash.	Param 1: string (file name/path) Param 2: long (Number of bytes of the file to use for the hash)	<none> If there are problems calculating the hash, <NULL> is returned.
GetFileVer	Returns the file version string of a file.	Param 1: string (file name/path)	<string> Returns <NULL> if there is an error.
GetFileVerMajor	Returns the most significant version number (I.E. x.0.0.0).	Param 1: string (file name/path)	<long> Returns -1 if there is an error.
GetFileVerMinor	Returns the second most significant version number (I.E. 0.x.0.0).	Param 1: string (file name/path)	<long> Returns -1 if there is an error.
GetFileVerBuild	Returns the second least significant version number (I.E. 0.0.x.0).	Param 1: string (file name/path)	<long> Returns -1 if there is an error.
GetFileVerSub Build	Returns the least significant version number (I.E. 0.0.0.x).	Param 1: string (file name/path)	<long> Returns -1 if there is an error.
GetSystemDrive	Returns the system drive.	<none>	<string> Returns <NULL> if there is an error.
GetHomeDir	Returns the user's profile folder.	<none>	<string> Returns <NULL> if there is an error.

Table 9-4 Functions

Operator name	Description	Parameters	Return
GetProgFiles CommonDir	Returns the Program Files\Common Files folder.	<none>	<string> Returns <NULL> if there is an error.
GetCommonApp DataDir	Returns the common application data folder.	<none>	<string> Returns <NULL> if there is an error.
CheckFreeDisk Space	Checks to see if enough free space is available on a given drive or folder.	Param 1: string (drive/ folder) Param 2: long (disk space in KB)	<boolean>
CompareFile Versions		Param 1: string (version string) Param 2: string (version string)	<long> ■ <0 Version of Param 1 is less than Param 2. ■ 0 Version of Param 1 is equal to Param 2. ■ >0 Version of Param 1 is greater than Param 2.

Table 9-4 Functions

Operator name	Description	Parameters	Return
IsOSFamily	Tests to see if the operating system belongs to a particular family.	Param 1: constant ■ OS_SUITE_WIN95: Windows 95a or Windows 95b ■ OS_SUITE_WIN98: Windows 98 or Windows 98 SE ■ OS_SUITE_WINME: Windows Me ■ OS_SUITE_WINNT4: Winnt 4.0 Workstation, Server, Terminal Server & Enterprise ■ OS_SUITE_WIN2K: Windows 2000 Pro, Server, Advanced Server & Datacenter ■ OS_SUITE_WINXP: Windows XP Home and Pro ■ OS_SUITE_WIN2003: Windows 2003 Server, Web, Enterprise & Datacenter	<boolean>

Table 9-4 Functions

Operator name	Description	Parameters	Return
IsOSProduct	Tests to see if the computer is running a particular operating system.	Param 1: ■ OS_PRODUCT_WIN95A ■ OS_PRODUCT_WIN95B ■ OS_PRODUCT_WIN98 ■ OS_PRODUCT_WIN98SE ■ OS_PRODUCT_WINME ■ OS_PRODUCT_WINNT4_SRV ■ OS_PRODUCT_WINNT4_WRKSTN ■ OS_PRODUCT_WNNT4_ENTERPRISE ■ OS_PRODUCT_WINNT4_TERMINAL ■ OS_PRODUCT_WIN2K_DATACENTER ■ OS_PRODUCT_WIN2K_ADVSRV ■ OS_PRODUCT_WIN2K_SRV ■ OS_PRODUCT_WIN2K_PRO ■ OS_PRODUCT_WINXP_HOME ■ OS_PRODUCT_WINXP_PRO ■ OS_PRODUCT_WIN2003_DATACENTER ■ OS_PRODUCT_WIN2003_ENTERPRISE ■ OS_PRODUCT_WIN2003_WEB ■ OS_PRODUCT_WIN2003_SRV	<boolean>
IsAdminUser	Checks to see if the current user is part of the Administrators group. On Windows 9x platforms, this PreCondition always evaluates to true.	<none>	<boolean>

Table 9-4 Functions

Operator name	Description	Parameters	Return
IsPowerUser	Checks to see if the current user is part of the Power Users group. On Windows 9x platforms, this PreCondition always evaluates true.	<none>	<boolean>
IsWinnt	Determines whether the operating system is Windows NT-based (NT4, 2000, XP, etc.) Win32 specific.	<none>	<boolean>
IsWin9x	Determines whether the operating system is Windows 9x-based. Win32 specific.	<none>	<boolean>
GetOSLang	Retrieves the default language of the operating system.	<none>	<string>
GetWinDir	Retrieves the Windows directory as defined by the GetWindowsDirectory Win32 API call.	<none>	<string>
GetSystemDir	Retrieves the system directory as defined by the GetSystemDirectory Win32 API call.	<none>	<string>
GetProgFilesDir	Retrieves the Program Files directory as defined by the shfolder.dll.	<none>	<string>
IniSectionExists	Determines if a given ini section exists.	File name <string> Section name <string>: The section name that is used here should exclude the bracket characters [and].	<boolean> False is returned if the file does not exist.

Table 9-4 Functions

Operator name	Description	Parameters	Return
GetIniValue	Retrieves a setting in an ini file.	File name <stringL ■ Section name <string>: The section name that is used here should exclude the bracket characters [and]. ■ Setting name <string>	<string> <NULL> is returned if the setting or file does not exist.
RegKeyExists	Determines if a registry key exists.	Reg Hive <string> ■ “HKCR” ■ “HKCC” ■ “HKCU” ■ “HKLM” ■ “HKU” Reg Keyname <string>	<boolean>
GetRegValue	Retrieves a value from the registry.	Reg Hive <string> ■ “HKCR” ■ “HKCC” ■ “HKCU” ■ “HKLM” ■ “HKU” Reg Keyname <string> Reg Setting <string>: Pass in an empty string to get the default value for a regkey.	<string> If the value is a number, the base-10 representation of the number is returned in a string. If the value is binary, a hex-string is returned. <NULL> is returned if the setting doesn’t exist.
atoll	Converts a string that represents numbers into a long. It is assumed that the number that is represented in the string is base-10.	<string>	<long> Returns 0 if the input cannot be converted.
FileExists	Determines if a given file or folder exists.	<string>	<boolean>
MatchesSubnet	Determines whether one of the IP addresses of a computer matches a given IP address/ mask.	■ Param 1: string (IP Address) ■ Param 2: string (Mask)	<boolean>

Table 9-4 Functions

Operator name	Description	Parameters	Return
RegValExists	Determines if a registry value exists.	Param 1: string (Reg Hive) ■ "HKCR" ■ "HKCC" ■ "HKCU" ■ "HKLM" ■ "HKU" Param 2: string (Regkey name) Param 3: string (Regvalue): Use an empty string to get the default value for a regvalue	<boolean>
SetDebugMode	Turns on or off debug mode, which causes various PreCondition events to be logged to a known file location (c:\<windows dir>\LU_PC.log). For testing purposes only.	■ <long> Bit mask. ■ 0x0000000000000001: Log PreCondition debug lines ■ 0x0000000000000002: Log lex debug lines ■ 0x0000000000000004: Log yacc debug lines	<none>

PreCondition errors

A PreCondition terminates and evaluates to false if an error occurs. However, it can call the debug function to assist you in troubleshooting and testing update packages.

To enable the output of debug statements into the LiveUpdate log on the client (log.liveupdate), add the following PreCondition function:

SetDebugMode(1); bSelect=funct();

If debugging is turned on, the errors in Table 9-5 may be written to the log file.

Table 9-5 PreCondition errors

Error code	Description
-2	The PreCondition dll, LuPreCon.dll, failed to load.
1	General abort error.

Table 9-5 PreCondition errors

Error code	Description
2	Memory allocation error. This may occur under low memory situations.
3	Unsupported reserve word used.
4	Unknown operator used.
5	Unknown function used.
6	Invalid argument type was used for a given operation or function.
7	Invalid number of arguments was passed into a function.

Examples

You can create a PreCondition that lets you target product updates to specific computers in your environment. You can filter update packages based upon the operating system, LiveUpdate settings, registry settings, or product dependencies. The filtering takes place after LiveUpdate catalog files are retrieved, but before any updates are downloaded and installed.

In this example, LiveUpdate product updates are filtered based upon specific LiveUpdate properties found in the following Product.Catalog.LiveUpdate file:

```
[Product 0]

DESCRIPTIVENAME=SymEvent

LANGUAGE=English

MONIKER={6e34dcc1-b194-11D2-a11e-00409500ad7d}

PRODUCT=Symevent Installer

PRODUCTNAME=Symevent Installer

SEQ.UPDATE=20010917

SKU=123-4567

UPDATESTATUS=UPDATES:YES

VERSION=10.3
```

The following example filters updates based upon the sequence number of the Symantec SymEvent Installer. In order for the bSelect condition to be set to true, the sequence number must be 20010917 or higher.

```
bSelect = GetSeqNum (“Symevent Installer”, “10.3”, “English”,
“Update”) >= 20010917;
```

You can also use the registered product's moniker:

```
bSelect = GetSeqNumByMonider ("{6e34dcc1-b194-11D2-a11e-
00409500ad7d}","Update") >= 20010917;
```

In the following example, the PreCondition checks to see if the SKU value registered with the Symantec Installer is 123-4567:

```
bSelect = GetProductProp ("Symevent Installer", "10.3", "English",
"Update") = 123-4567;
```

In this example, the PreCondition checks the Settings.LiveUpdate file PREFERENCES\ENVIRONMENT line is set to retail mode:

```
bSelect = ToLower (GetSettingsProp ("PREFERENCES\ENVIRONMENT")) ==
"retail";
```

You can also create a PreCondition that filters based upon values that are in an INI file or in the registry. The following example checks the INI file in the <Program Files>\Symantec Client Security\Symantec AntiVirus\defloc.dat file to see if the Location setting from the DefBaseLocation section equals C:\Progra~1\COMMON~1\SYMANT~1\VIRUSD~1:

```
bSelect = GetIniValue (AppendPath (GetProgFilesDir (),
"Symantec_Client_Security\\Symantec AntiVirus\\defloc.dat"),
"DefBaseLocation", "Location") ==
"C:PROGRA~1\\COMMON~1\\SYMANT~1\\VIRUSD~1";
```

In this example, the PreCondition checks to see if the registry value of \\HKLM\SOFTWARE\SymantecSharedUsage\SAVCECLT_SymEvent is set to 1:

```
bSelect = GetRegValue ("HKLM", "SOFTWARE\\Symantec\SharedUsage",
"SAVCECLT_SymEvent") == "1";
```

You can string two or more PreConditions together. In the following example, bSelect will be True if the operating system is Windows XP and the environment setting is retail. The two PreConditions are combined using the && operator:

```
bSelect = (IsWinnt () && (GetOSVerMajor () == 5) && (GetOSVerMinor
() == 1) && ((GetWinOSProductMask () & 0x1) && (GetWinOSSuiteMask ()
& 0x200) != 0x200)) && (ToLower (GetSettingsProp
("PREFERENCES\\ENVIRONMENT")) == "retail";
```

Parentheses are used to group the statement that checks for Windows XP and the statement that checks for the environment setting. && (AND) is used to combine the two PreCondition statements, which evaluates to True only when both statements evaluate to True. To change the statement to evaluate to True if one or the other statement is True, use || (OR).

Using the PreCondition Editor

Initially, the PreCondition Editor is empty, but once you begin defining the PreCondition for your update, each statement of your PreCondition is listed.

Insert and modify PreCondition statements

You can insert a new PreCondition statement, use an existing PreCondition statement and modify it to create a new statement, modify an existing Precondition statement, cancel your edits, and save PreCondition statements.

Note: You are not able to exit the PreCondition Editor if any of your entries contain syntax errors.

To insert a PreCondition statement

1. In the new product update window, next to preconditions:, click **Edit**.
2. In the PreCondition Editor box, type a PreCondition statement.
3. Click **Insert**.
   Each time that you type a statement in the text box, click **Insert** to add it to the list in the PreCondition Editor.
4. To confirm the syntax of the PreCondition statement, click **Syntax**.
   Check the syntax of each statement you insert.

To use an existing PreCondition statement as a template for a new statement

1. Select the statement in the PreCondition Editor to use as a template.
2. Click **Select** to place the statement into the text box.
3. Modify the statement with your changes.
4. Click **Insert**.
   The original statement on which you based your new one remains unchanged.
5. To confirm the syntax of the PreCondition statement, click **Syntax**.

To modify a PreCondition statement

1. Select the statement to modify.
   It appears in the text box where you can make changes as needed.
2. When you have finished your changes, click **Modify**.
   The selected statement is replaced by your modified version.
3. To confirm the syntax of the PreCondition statement, click **Syntax**.

To cancel PreCondition statement edits

- Click **Cancel**.
  All changes that you have made to the PreCondition statements are discarded and you are returned to the New Updates window.

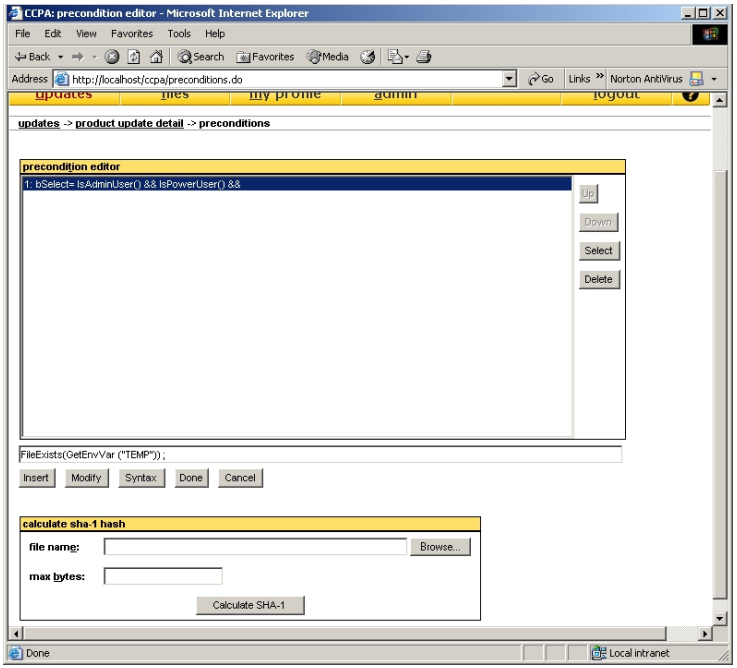
To save PreCondition statements

- Click **Done**.
  You are returned to the New Updates window.

Editing PreCondition statements

In the PreCondition Editor, you can revise the processing order and delete specific statements (Figure 9-1).

Figure 9-1 CCPA PreCondition Editor



To revise the processing order of the PreCondition statement

- Select the statement, and then click **Up** or **Down** to move the statement up or down in the processing order.

To delete a PreCondition statement

- Select the statement, and then click **Delete**.

Signing and publishing updates

Signers are responsible for performing the following tasks in the CCPA process:

- Signing submitted updates and publishing them to the test LiveUpdate server
- Signing submitted updates and publishing them to the production LiveUpdate server
- Rejecting submitted updates either before publishing to a test server, or before publishing to production
- Managing their own signing certificates (PKCS12 keystore)

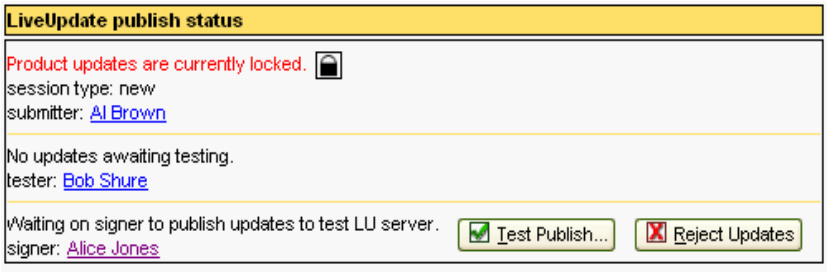
When a Submitter submits updates for which you are the designated Signer, the publishing session status goes to Submitted or Approved, depending on whether or not the Submitter selected a Tester. If email notification is enabled, CCPA notifies you by email. As the Signer, you review the updates and either publish them to the test or production server or reject them. If you publish the updates to the test server, the publishing session status changes to In Test, and CCPA notifies the Tester by email. If you reject the updates, the publishing session status returns to In Work, and CCPA notifies the Submitter by email.

After a Tester approves updates, or a Submitter submits updates without testing, and you are the designated Signer, the publishing session status goes to Approved, and CCPA notifies you by email if email notification has been enabled. As the Signer, you review the updates and either publish them to the production server or reject them. If you publish the updates to the production server, the publishing session status goes back to the initial state of Available, and CCPA notifies the Submitter and the Tester by email. If you reject the updates, the publishing session status returns to In Work, and CCPA notifies the Submitter by email.

Warning: You should test your updates before you publish them. Update packages can cause severe problems if they are not configured properly.

When a Submitter submits product updates for testing, the current publishing session status changes to Submitted, and the Publish Status box in the Updates window looks like the example shown in Figure 9-2.

Figure 9-2 CCPA Publish Status



The custom content is published first to a test server and once the Tester has approved the updates, you then publish the custom content to the production server.

Uploading a signing certificate

To publish product updates, you must first upload your signing certificate. You cannot publish updates to either the test server or the production server until your certificate has been uploaded.

To upload a signing certificate

1. Log onto CCPA.
2. In the main LiveUpdate - Custom Content window, click **My Profile**.
3. In the my profile window, click **Upload Certificate**.
4. Click **Browse**, and then select your signing certificate.
5. Click **submit**.

Publishing updates

If the Submitter has designated a Tester and testing server, the updates are ready to be published to that server for testing. If a testing server and Tester has not been designated, you can publish the updates directly to the production server after you approve them.

Once you confirm the publish to production action, the following takes place:

- The TRI file is assembled based on all of the product updates in the CCPA database. This includes the new updates that were just defined (added, deleted, or modified) as part of the current publishing session, as well as those that were not affected by the publishing session.

- The GRD file is assembled based on all of the files (Update Packages) defined in the CCPA database.
- The SIG file is created, which authenticates the GRD file using the Signer's certificate and password.
- The custtri.zip file is created with the TRI, GRD, and SIG files.
- The TRI file is transferred to the production server.
- Depending on the session type (new, replace, delete), the relevant files (Update Packages) are transferred to, or removed from, the production server.

Necessary cleanup operations are performed at the CCPA server and, finally, the publishing session goes into the Available state.

To publish updates to a test server

1. In the Updates > confirm test publish window, type the user name and password for the test server.
   This is only necessary if the user name and password were not entered in the server attributes during set up by the CCPA Administrator.
2. If email notification is enabled, type an email message regarding the update. You can add up to 500 characters. This email is sent to all session participants.
3. In the certificate password box, type your certificate password.
   A password is required for you to sign the GRD file, before the custtri file is assembled and transferred to the LiveUpdate test server.
4. Click **Confirm Test Publish**.
   This may take time to complete, depending on the size of the custtri.zip file.

To publish updates to a production server

1. In the Updates > Publish to Production window, enter the user name and password for the production server.
   This is only necessary if the user name and password were not entered in the server attributes during set up by the CCPA Administrator.
2. If email notification is enabled, type an email message regarding the update. You can add up to 500 characters. This email is sent to all session participants.

3 In the certificate password box, type your certificate password.
A password is required for you to sign the GRD file, before the custtri file is assembled and transferred to the Central LiveUpdate production server.

4 Click **Confirm Production Publish**.
A message confirms that the updates have been published to the production server.

Rejecting updates

When you reject an update for publishing, the publishing session remains locked and enters the In Work state. CCPA notifies the Submitter that the update has been rejected if email notification is enabled.

To reject an update

- In the LiveUpdate publish status window, click **Reject Updates**.

Testing product updates

The Tester is responsible for testing product updates on a LiveUpdate test server. CCPA notifies the Tester by email when updates have been submitted, if email notification has been enabled. The Tester is notified again when a Signer publishes the updates to a test server. This email provides the location of the test server where you can test the product updates, as well as the details regarding the changes that were defined by the Submitter in this publishing session.

When the publishing status is marked In Test, you can access the product updates on the test server to perform your verification test. It is the responsibility of the Submitter to ensure that the test server is in a ready state for testing the submitted updates.

When you have completed testing, you log on to CCPA and access the Updates window where you click Test Passed or Test Failed. CCPA notifies the Submitter and the Signer by email of the test results. If the test fails, the status of the publishing session returns to In Work, and it is the responsibility of the Submitter to perform the next step. If the test passes, the status of the publishing session changes to Approved and it is now the Signer's responsibility to perform the next step.

The products that are ready for testing are displayed in the list of product update entries in the LiveUpdate publish status window.

Index

T

U