

# Symantec™ LiveUpdate™ Administrator 2.3.3 User's Guide



# Symantec LiveUpdate Administrator 2.3.3 User's Guide

Product version: 2.3.3

Documentation version: 1

This document was last updated on: June 25, 2014

## Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>

# Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online 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 and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

## Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

## Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

Customer Service is available to assist with non-technical questions, such as 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 about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

## Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan [customercare\\_apac@symantec.com](mailto:customercare_apac@symantec.com)

Europe, Middle-East, and Africa [semea@symantec.com](mailto:semea@symantec.com)

North America and Latin America [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

# Contents

Technical Support .....	4	
Chapter 1	Introducing LiveUpdate Administrator .....	9
	About LiveUpdate Administrator .....	9
	What's new in LiveUpdate Administrator 2.3.3 .....	10
	Where to get more information about LiveUpdate Administrator .....	11
Chapter 2	Installing and running LiveUpdate Administrator .....	12
	Before you install .....	12
	System requirements for LiveUpdate Administrator .....	13
	Installing LiveUpdate Administrator .....	15
	Uninstalling LiveUpdate Administrator .....	16
	Logging on to LiveUpdate Administrator .....	16
	Connecting to LiveUpdate Administrator remotely .....	17
Chapter 3	Setting up LiveUpdate Administrator .....	18
	Getting started on LiveUpdate Administrator .....	18
	What you can do from the LiveUpdate Administrator Home page .....	20
	About the LiveUpdate Administrator icons .....	21
	Updating the Symantec Product Catalog .....	22
	Adding Symantec products to the product list .....	22
	Configuring Source Servers .....	23
	Working with failover servers .....	24
	Adding distribution centers .....	25
	Creating host files for LiveUpdate clients to receive updates .....	27
Chapter 4	Managing download and distribution schedules .....	28
	Scheduling downloads .....	28
	Running distribution schedules automatically after the completion of a download .....	30
	Scheduling distribution .....	30

	Viewing the download tasks and distribution tasks .....	32
Chapter 5	Configuring LiveUpdate Administrator .....	33
	Configuring LiveUpdate Administrator preferences .....	33
	Managing updates for products .....	35
	Deleting revisions .....	36
	Locking and unlocking revisions .....	36
	Adding or modifying user accounts .....	38
	Forcing a user to log off LiveUpdate Administrator .....	39
	Backing up and restoring your LiveUpdate Administrator configuration .....	39
	Best practices for increasing security in LiveUpdate Administrator .....	42
Chapter 6	Viewing events and troubleshooting information .....	44
	Viewing information in the Event Log .....	44
	About the troubleshooting file .....	45
	Generating the troubleshooting file .....	45
Index .....		47

# Introducing LiveUpdate Administrator

This chapter includes the following topics:

- [About LiveUpdate Administrator](#)
- [What's new in LiveUpdate Administrator 2.3.3](#)
- [Where to get more information about LiveUpdate Administrator](#)

## About LiveUpdate Administrator

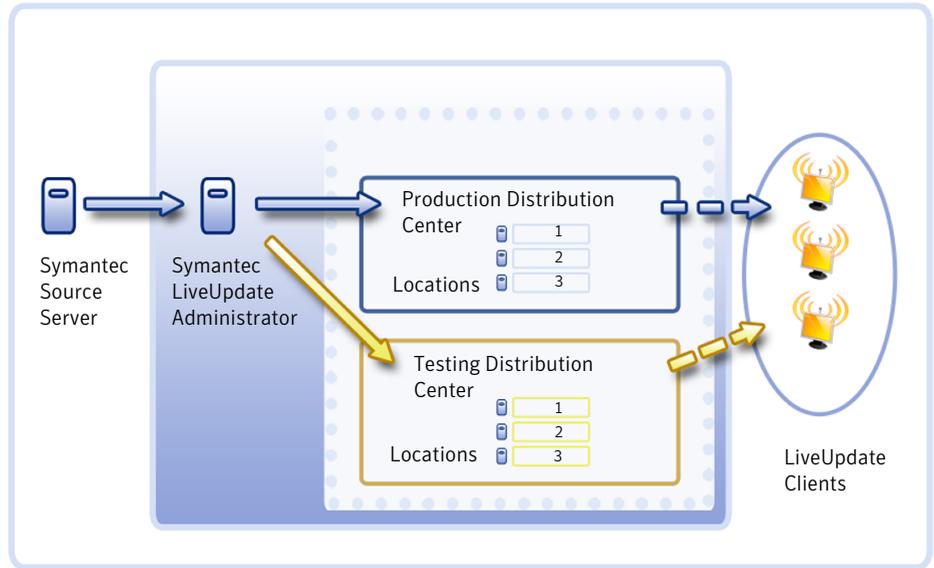
Symantec LiveUpdate Administrator is an enterprise web application that lets you manage Symantec updates on multiple internal LiveUpdate servers.

You download the updates from an external site to the internal LiveUpdate Administrator server, called Distribution Centers. You send the updates either immediately to a production distribution center for LiveUpdate clients to download, or to a testing center, so that you can test the updates. Once the updates have passed your testing requirements, they are sent to the production distribution center.

You distribute the updates on a schedule, letting you create a low maintenance, reliable system that can be set up once, and then run automatically. Updates can also be manually downloaded and distributed as needed.

[Figure 1-1](#) illustrates a typical LiveUpdate Administrator environment.

**Figure 1-1** Symantec LiveUpdate Administrator environment



## What's new in LiveUpdate Administrator 2.3.3

LiveUpdate Administrator includes the following new features and enhancements:

**Table 1-1** What's new in LiveUpdate Administrator 2.3.3

Feature	Benefit
System requirements	<ul style="list-style-type: none"> <li>You can upgrade from 2.2.2.9 through 2.3.2 to 2.3.3.</li> <li>LiveUpdate is packaged with Apache Tomcat version 7.0.54 and PostgreSQL version 9.3.1.</li> </ul> <p>See <a href="#">"System requirements for LiveUpdate Administrator"</a> on page 13.</p>
Installation changes	<p>When you install LiveUpdate Administrator, the installation folder, temporary folder, and download folder cannot be empty. Also, the root drive (such as C:\ or D:\) must use a subfolder that does not contain other files. The subfolder should use a local path, as network paths are not allowed.</p>

**Table 1-1** What's new in LiveUpdate Administrator 2.3.3 (*continued*)

Feature	Benefit
Removing old product versions from the <b>Symantec Product Catalog</b>	<p>LiveUpdate Administrator now removes old, unsupported versions of products from the <b>Symantec Product Catalog</b> and the Distribution Centers. After Symantec no longer supports a specific version, LiveUpdate Administrator removes the older versions based on the purge schedule for updates.</p> <p>You can change the purge schedule on the <b>Configure &gt; Preferences</b> tab.</p> <p>See “<a href="#">Configuring LiveUpdate Administrator preferences</a>” on page 33.</p> <p>See “<a href="#">Updating the Symantec Product Catalog</a>” on page 22.</p>
Use of HTTPS protocol	<p>The URLs within LiveUpdate Administrator now use the HTTPS protocol instead of the HTTP protocol. HTTPS is more secure than HTTP, which is subject to eavesdropping attacks and can let attackers gain access to website accounts and sensitive information.</p>
Password requirements	<p>To increase security, all administrator passwords to log on to LiveUpdate Administrator must be a minimum of 8 characters, be alphanumeric, and include one special character</p> <p>You can increase the minimum number of characters that are required on the <b>Preferences</b> page.</p> <p>See “<a href="#">Configuring LiveUpdate Administrator preferences</a>” on page 33.</p> <p>See “<a href="#">Adding or modifying user accounts</a>” on page 38.</p>
Importing the configuration file	<p>To restore the LiveUpdate Administrator configuration to 2.3.3 from an earlier version, you do not export the recovery backup file and then import it. Instead of exporting and importing the recovery backup file, you import a compressed file that you create from two other backup files.</p> <p>See “<a href="#">Backing up and restoring your LiveUpdate Administrator configuration</a>” on page 39.</p>

## Where to get more information about LiveUpdate Administrator

The Symantec Web site provides regularly updated information on LiveUpdate Administrator. This information includes product updates, user forums, tutorial videos, troubleshooting guidelines, and knowledge base articles.

On the Web, go to the following URLs:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

[www.symantec.com/connect](http://www.symantec.com/connect)

# Installing and running LiveUpdate Administrator

This chapter includes the following topics:

- [Before you install](#)
- [System requirements for LiveUpdate Administrator](#)
- [Installing LiveUpdate Administrator](#)
- [Uninstalling LiveUpdate Administrator](#)
- [Logging on to LiveUpdate Administrator](#)
- [Connecting to LiveUpdate Administrator remotely](#)

## Before you install

Before you install LiveUpdate Administrator, you should become familiar with where the installation program installs the software. Also ensure that your environment meets the system requirements.

The installation program installs the software in the following default locations:

64-bit	C:\Program Files (x86)\Symantec\LiveUpdate Administrator
32-bit	C:\Program Files\Symantec\LiveUpdate Administrator

[Table 2-1](#) lists the installed components for LiveUpdate Administrator and their installation location.

**Table 2-1** LiveUpdate Administrator components

Component name	Install location
PostgreSQL DBMS	<install path>\pgsql
Database	<install path>\pgsql\data
Tomcat servlet engine	<install path>\tomcat
LiveUpdate Administrator Web application	<install path>\tomcat\webapps\lua
Manage Updates folder	<ul style="list-style-type: none"> <li>■ Windows 2008, Windows 7, and Windows Vista:            &lt;App_data_path&gt;\ProgramData\Symantec\LiveUpdate Administrator\Downloads  <b>For example,</b>            C:\ProgramData\Symantec\LiveUpdate Administrator\Downloads</li> <li>■ Windows 2003, XP, and Windows 2000:            &lt;App_data_path&gt;\Documents and Settings\All Users\Application Data\Symantec\LiveUpdate Administrator\Downloads  <b>For example,</b> C:\Documents and Settings\All Users\Application Data\Symantec\LiveUpdate Administrator\Downloads</li> </ul>

See “[System requirements for LiveUpdate Administrator](#)” on page 13.

## System requirements for LiveUpdate Administrator

[Table 2-2](#) lists the system requirements for the main LiveUpdate Administrator components.

**Table 2-2** System requirements

Requirement	Description
Software	<p>Operating systems:</p> <ul style="list-style-type: none"> <li>■ Window XP Professional with Service Pack 3 or later</li> <li>■ Windows Vista with Service Pack 1 or later</li> <li>■ Windows 7</li> <li>■ Windows 2008 Server</li> <li>■ Windows 2003 Server with Service Pack 2 or later</li> <li>■ Windows 2000 Server with Service Pack 4 or later</li> </ul> <p>Browsers:</p> <ul style="list-style-type: none"> <li>■ Internet Explorer 6.x through 10.x</li> <li>■ Mozilla Firefox 3.x and later</li> <li>■ Google Chrome 31 and later</li> <li>■ Safari 5.x and later</li> </ul> <p>Other:</p> <ul style="list-style-type: none"> <li>■ TCP/IP network protocol enabled</li> </ul> <p><b>Note:</b> Windows 64-bit versions are supported, except for Windows XP.</p> <p><b>Note:</b> To ensure optimal LiveUpdate Administrator operations, Symantec recommends that you use a Server operating system.</p>
Hardware	<ul style="list-style-type: none"> <li>■ 650 MB hard disk space for LiveUpdate Administrator, the JRE, and third-party tools. The LiveUpdate Administrator installer package is approximately 200 MB, which includes the JRE that is required for LiveUpdate Administrator to function.</li> <li>■ A minimum of 10 GB hard disk space each for the updates in the following folders: <ul style="list-style-type: none"> <li>■ Manage Updates folder</li> <li>■ Temporary download folder: C:\TempDownload</li> <li>■ Permanent download folder: C:\ProgramData\Symantec\LiveUpdate Administrator\Downloads</li> </ul> </li> </ul> <p>LiveUpdate Administrator copies the updates to these folders for distribution.</p>

Symantec recommends using either IIS or Apache Server for hosting your remote distribution center locations. Refer to your operating system's documentation for additional information.

[Table 2-3](#) lists the default ports that LiveUpdate Administrator uses:

**Table 2-3** Ports

Port	Used by
7070	Default Distribution Center
7071	Tomcat for shutdown commands. While LiveUpdate Administrator works if this port is closed, Tomcat shutdown operations do not.
7072	PostgreSQL database
7073	LiveUpdate Administrator

If other applications use these ports when you install LiveUpdate Administrator, you are prompted to enter alternate port numbers.

LiveUpdate Administrator communicates with the distribution centers using the destination ports HTTP (80), HTTPS (443), and FTP (21). If the LiveUpdate clients run a firewall, verify that the firewall allows these destination ports.

Problems may occur when you use a terminal service for installation. You should install LiveUpdate Administrator directly from the console.

To install LiveUpdate Administrator, you must log on as at least a power user with Administrator privileges. You must be able to create new local users and to create new services.

## Installing LiveUpdate Administrator

To install LiveUpdate Administrator, you must log on as at least a power user with Administrator privileges. You must be able to create new local users and to create new services.

When you install LiveUpdate Administrator, the Java Runtime Environment (JRE), Apache Tomcat, and PostgreSQL database applications are also installed. The Apache Tomcat and PostgreSQL services are started automatically.

### To install LiveUpdate Administrator

- 1 Download the installer file from one of the following locations:
  - <http://www.symantec.com/docs/TECH134809>
  - [ftp://ftp.symantec.com/public/english\\_us\\_canada/liveupdate](ftp://ftp.symantec.com/public/english_us_canada/liveupdate)
- 2 Run the executable, and then follow the on-screen instructions.
- 3 In the **Destination Folder** window, do one of the following tasks:
  - To accept the default folders for the LiveUpdate Administrator files, click **Next**.

- To change the default folders, click **Change**, change the folder, and then click **Next**.

---

**Note:** The LiveUpdate Administrator files, the JRE, Tomcat, the PostgreSQL database, and the documentation are installed in the first folder.

---

You can change the default folder for the updates after installation.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

- 4 At the **LiveUpdate Administrator User Setup** window, type your user name, password, and email address, and then click **Next**.

- 5 Click **Install**.

If any or all of the default ports are currently used, you are prompted. You can then specify alternate ports for LiveUpdate Administrator to use.

You must restart LiveUpdate Administrator services after you stop the programs that use these ports. You do not need to stop the service if you use a port other than the default.

- 6 Click **Finish**.

## Uninstalling LiveUpdate Administrator

You can uninstall LiveUpdate Administrator using Add/Remove Programs in the Control Panel.

## Logging on to LiveUpdate Administrator

LiveUpdate Administrator installation program adds a shortcut in the **Programs** menu under **LiveUpdate Administrator > LiveUpdate Administrator**. The installation also adds a shortcut to the desktop.

---

**Note:** The inactivity timeout for LiveUpdate Administrator is 120 minutes, after which you need to log back on. If you do not log on with the correct credentials after five attempts, the account locks you out. You must wait 15 minutes before the account unlocks.

---

---

**Note:** LiveUpdate Administrator user interface is best viewed using a screen resolution of 1024 x 768 or higher.

---

### To log on to LiveUpdate Administrator

- 1 Do one of the following tasks:
  - Click Start, and go to **Programs > LiveUpdate Administrator**, and then click **LiveUpdate Administrator**.
  - Double-click LiveUpdate Administrator icon on the desktop.
- 2 On the **LiveUpdate Administrator** window, enter your user name and password and click **Log On**.

If you forget your password, click **Forget your password?** to request that an email message with a link be sent to the email address that you specified during installation. Use this link to change your password. Use the changed password to log on to LiveUpdate Administrator. For security, the link is valid for a limited time only.

To receive the email message, you must first configure the mail server.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

## Connecting to LiveUpdate Administrator remotely

You can connect to LiveUpdate Administrator (LUA) computer remotely. To connect, use the following command structure:

```
https://Hostname_of_LUA_computer:7073/lua
```

or

```
https://IP_address_of_LUA_computer:7073/lua
```

If you have specified a different port number during installation, use that port number instead of 7073.

# Setting up LiveUpdate Administrator

This chapter includes the following topics:

- [Getting started on LiveUpdate Administrator](#)
- [What you can do from the LiveUpdate Administrator Home page](#)
- [Updating the Symantec Product Catalog](#)
- [Adding Symantec products to the product list](#)
- [Configuring Source Servers](#)
- [Adding distribution centers](#)
- [Creating host files for LiveUpdate clients to receive updates](#)

## Getting started on LiveUpdate Administrator

LiveUpdate Administrator is set up to enable you to download and distribute updates to LiveUpdate clients quickly.

[Table 3-1](#) displays the tasks that you must perform after installation. By default, most of the tasks are already configured for you.

**Table 3-1** Steps to get up and running on LiveUpdate Administrator

Step	Task	Description
Step 1	Update the Symantec product catalog (optional)	<p>LiveUpdate Administrator adds the latest products and versions of Symantec products to the Symantec product catalog on a weekly basis by default. If you want to update the catalog more frequently, you can do it manually.</p> <p>See <a href="#">“Updating the Symantec Product Catalog”</a> on page 22.</p>
Step 2	Add the products and versions from the product catalog to the product list	<p>Add products and versions from the Symantec product catalog to the product list. From the product list, you choose which product updates to download to the clients.</p> <p>See <a href="#">“Adding Symantec products to the product list”</a> on page 22.</p>
Step 3	Identify the source server from which to download updates to LiveUpdate Administrator	<p>By default, LiveUpdate Administrator downloads and receives updates from one of the LiveUpdate servers at the following location:  <a href="http://liveupdate.symantecliveupdate.com">http://liveupdate.symantecliveupdate.com</a></p> <p>If you do not want to use the default server, you can configure one or more local servers.</p> <p>You should also configure a failover server in case the primary server fails.</p> <p>See <a href="#">“Configuring Source Servers”</a> on page 23.  See <a href="#">“Working with failover servers”</a> on page 24.</p>
Step 4	Add test and production distribution centers to distribute updates	<p>To download updates to LiveUpdate clients, LiveUpdate Administrator uses a distribution center. Each distribution center uses a server, or location, to distribute the updates.</p> <p>LiveUpdate Administrator uses the following types of distribution centers:</p> <ul style="list-style-type: none"> <li>■ A Testing Distribution Center to test the updates before you download them to the clients.</li> <li>■ A Production Distribution Center to download the updates using a schedule you determine.</li> </ul> <p>For each distribution center, you select the products and components that the distribution center downloads to the clients.</p> <p>By default, LiveUpdate Administrator installs a testing distribution center and a production distribution center. You can also add your own distribution centers.</p> <p>See <a href="#">“Adding distribution centers”</a> on page 25.</p>

**Table 3-1** Steps to get up and running on LiveUpdate Administrator (*continued*)

Step	Task	Description
Step 5	Schedule updates to automatically download and distribute updates to clients	<p>You set up one schedule to download updates to LiveUpdate Administrator, and a second schedule to distribute updates to the clients.</p> <p>See <a href="#">“Scheduling downloads”</a> on page 28.</p> <p>See <a href="#">“Scheduling distribution”</a> on page 30.</p>
Step 6	Create a host file so that LiveUpdate clients retrieve updates from a specific server (optional)	<p>When a LiveUpdate client is installed, by default it is configured to connect to a Symantec LiveUpdate server to retrieve updates. To direct LiveUpdate clients to retrieve updates from a specific distribution server instead, you must modify the configuration of the LiveUpdate client.</p> <p>See <a href="#">“Creating host files for LiveUpdate clients to receive updates”</a> on page 27.</p>

After you get up and running, you can perform other configuration tasks as needed.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

## What you can do from the LiveUpdate Administrator Home page

The LiveUpdate Administrator **Home** page displays the status and links to the most common tasks that LiveUpdate Administrator performs.

---

**Note:** The inactivity timeout for LiveUpdate Administrator is 120 minutes, after which you need to log back on.

---

**Table 3-2** Home page

Page	Description
<b>Download and Distribution Activity</b>	<p>Displays the ten most current requests. You can view a full list of requests by clicking the full request report link. The report link displays the <b>Download &amp; Distribute &gt; Activity Monitor</b> page.</p> <p>Events on the <b>Activity Monitor</b> page filter by type, status, and time. You can sort the events by type, when the event was started, changed, or by event status.</p> <p>See <a href="#">“Viewing the download tasks and distribution tasks”</a> on page 32.</p>

**Table 3-2** Home page (continued)

Page	Description
<b>Event Log</b>	Displays the 10 most recent critical events that LiveUpdate Administrator generates. See " <a href="#">Viewing information in the Event Log</a> " on page 44.
<b>Configuration Restore</b>	Enables you to import an exported configuration file if you need to reinstall LiveUpdate Administrator.  <b>Note: Configuration Restore</b> is only available after you log on to LiveUpdate Administrator and click the <b>Home</b> page for the first time. After you navigate away from the <b>Home</b> page, this option is no longer available unless you reinstall LiveUpdate Administrator.  See " <a href="#">Backing up and restoring your LiveUpdate Administrator configuration</a> " on page 39.
<b>System Statistics</b>	Displays the amount of space that LiveUpdate Administrator and its database uses.
<b>Quick Links</b>	Displays the links to where you can add a new distribution center, distribution schedule, or download schedule. You can access these pages by clicking <b>Configure &gt; Distribution Centers</b> or <b>Download &amp; Distribute &gt; Schedules</b> .  See " <a href="#">Adding distribution centers</a> " on page 25.  See " <a href="#">Scheduling downloads</a> " on page 28.  See " <a href="#">Scheduling distribution</a> " on page 30.
<b>My Symantec Products Overview</b>	Displays the icons that show whether all of the products in your Site List are assigned to distribution centers and have been associated with distribution and download schedules.

## About the LiveUpdate Administrator icons

LiveUpdate Administrator uses the following icons to assist you in determining if all updates are scheduled for download and distribution. The icons also indicate when more information is available:

-  Displays detailed information about the item.
-  Displays that all products in the **My Symantec Product** list are covered in Distribution, Download schedules, and centers.
-  Displays that some of the products in the **My Symantec Product** list are covered in Distribution, Download schedules, and centers.

-  Displays that none of the products in the **My Symantec Product** list are covered by Distribution, Download schedules, and centers.

See [“Viewing the download tasks and distribution tasks”](#) on page 32.

## Updating the Symantec Product Catalog

To download Symantec products to distribute, you must first display the latest available products, which you can then add to your product list.

By default, LiveUpdate Administrator is configured to automatically update the product catalog each week. If your product does not appear in the list of available products, you may need to update the product catalog manually.

If you do not want the automatic product catalog updates, you can disable it.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

### To update the Symantec Product Catalog

- 1 Click the **Configure** tab.
- 2 On the left pane in the **My Symantec Products** window, under **My Symantec Products Tasks**, click **Update Symantec Product Catalog**.

## Adding Symantec products to the product list

You can add and delete the products for which you want LiveUpdate Administrator to download updates. You can also view the coverage details for each product.

### To add a product to the product list

- 1 On the **Configure** page, click **My Symantec Products**, and then click **Add New Products**.
- 2 Under **Product line**, select the name of the product that you want to add from the list.
- 3 Click **OK**.

Products are automatically updated to the Symantec product catalog on a weekly basis. If your product is not listed, you can update the product catalog immediately.

See [“Updating the Symantec Product Catalog”](#) on page 22.

### To delete a product from the product list

- 1 On the **My Symantec Products** window, click the check box next to the product that you want to delete from the product list.
- 2 Click **Delete Selected Products**.
- 3 Click **Confirm Delete**.

## Configuring Source Servers

When you download updates, LiveUpdate Administrator attempts to download from a source server. By default, LiveUpdate Administrator uses the server at: <http://liveupdate.symantecliveupdate.com>. You can optionally add more source servers. LiveUpdate Administrator tries to connect to these servers in the order in which they appear in the user interface.

If the server is not available, LiveUpdate Administrator attempts to download from the failover server. You can designate a list of failover servers that can be used in cases where the primary server is not available.

See [“Working with failover servers”](#) on page 24.

### To add a Source Server

- 1 On the **Configure** tab, under **Source Servers**, click **Add**.
- 2 In the **New Source Server** window, enter the information for the server.
- 3 Do one of the following:
  - To save the new source server, click **OK**.
  - To save the new source server, and add a failover server for the new source server, click **Save and Add Failover**.
  - Click **Cancel** to cancel adding a new server.

### To edit a Source Server

- 1 On the **Configure** tab, under **Source Servers**, select the server you want to edit, and then click **Edit**.
- 2 When you have finished editing the information for the server, do one of the following:
  - Click **OK** to save your changes.
  - Click **Apply** to save the changes and continue editing.
  - Click **Test** to test the server connection.

### To delete a Source Server

- 1 In the **Configure** tab, under **Source Servers**, select the server you want to delete, and then click **Delete**.
- 2 Click **Cancel** to cancel the deletion.
- 3 Click **Confirm Delete** to delete the language from the site list.

### To reset to defaults

- 1 In the **Configure** tab, under **Source Servers**, in the left pane, click **Reset to defaults**.
- 2 Do one of the following:
  - Click **Cancel** to cancel resetting to the defaults.
  - Click **Confirm reset** to confirm resetting to the defaults.

The source servers and failover servers are removed.

## Working with failover servers

A failover server is used when a connection to the source server fails. LiveUpdate Administrator then attempts to download from a failover server that you designate. If that connection also fails, LiveUpdate Administrator retries downloading from the source server.

LiveUpdate Administrator makes three attempts by default. You can change the number of times LiveUpdate Administrator attempts to connect in the **Configure > Preferences > Server Connection** option.

### To add a failover server

- 1 Select the source server that you want to associate with a failover server by doing one of the following:
  - In the **Configure/Source Servers** window, on the left pane, click **Add Failover Server**. Then, in the drop-down list, select the source server that you want to add a failover server for.
  - In right pane, under **Source Servers**, click on the server that you want to add a failover server for, and then click **Add**.
  - If you are in the process of adding a new Source Server, in the **New Source Server** window, click **Add** next to the Failover Servers box.
- 2 Enter the information for the server.
- 3 Do one of the following:
  - Click **OK** to add the failover server.

- Click **Save and Add Another** to continue adding additional failover servers.
- Click **Cancel** to cancel the addition of the failover server.

#### To change the order of a failover server

- 1 On the **Source Servers** window, click the name of the source server, and then click **Edit**.
- 2 Click the name of the failover server that you want to move, and then click **Move Up** or **Move Down**.

#### To promote a failover server to primary server

- 1 Click **Configure > Source Servers**.
- 2 In the **Source Servers** list, click the name of the Source Server to which the failover server belongs, and then click **Edit**.
- 3 On the **Edit Source Server** window, in the **Failover Servers** box, click on the failover server that you want to promote, and then click **Primary**.
- 4 Click **Confirm make primary**.

This promotes the failover server to be the primary Source Server. The previous primary Source Server becomes a new failover server.

See [“Configuring Source Servers”](#) on page 23.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

## Adding distribution centers

A Distribution Center represents a single server or group of servers to which updates are distributed from a LiveUpdate Administrator.

Each single server within a Distribution Center is called a location. By default, updates are distributed to all locations in a distribution center. Once an update has been distributed to a location, it is not distributed again.

LiveUpdate Administrator has a default testing and production distribution center. For the default distribution centers, you add the list of products that are associated with the distribution center.

If you add your own distribution center, you add both the locations and the list of products. The product list applies to the entire distribution center. You can select an entire product line, or only add specific components, such as software updates or virus definitions. For example, to download only the virus definitions for all of your products, you can select the products, and then specify the virus definitions component.

All locations in the distribution center are in sync with the product updates of the products that are configured in the list.

To make sure that you selected all components, click **Home > My Symantec Products Overview**.

You can enable bandwidth throttling for each location. Bandwidth throttling lets you manage distribution in the environments that have both high-bandwidth and low-bandwidth networks. In addition to enabling bandwidth throttling for specific locations, you can enable it for all location servers on the **Configure > Preferences** page.

---

**Note:** Attackers can tamper with the contents in the distribution centers. Therefore, make sure that only authorized users can access the distribution centers.

---

#### To add a distribution center

- 1 On the **Configure** tab, in the **Distribution Centers** window, click **Add**.
- 2 Enter the following information for the distribution center:

<b>Distribution center name</b>	Type a unique name for this distribution center
<b>Distribution center type</b>	Select either <b>Production</b> or <b>Testing</b> from the drop-down menu.
<b>Description</b>	Type a meaningful description that helps you identify this distribution center.

- 3 To specify a server, in the **Locations** box, click **Add**.  
A distribution center must have at least one location.
- 4 In the **New location server** window, enter the information for the server.
- 5 Click **OK** to save the new location, or **Save and Add Another** to continue adding new locations.
- 6 In the **Edit Distribution Center** window, add products to this distribution center by clicking **Add** next to the **Product List** box.
- 7 Select the products you want to add, and then click **OK**.  
You can add all products or expand a product and select specific components, such as virus definitions.
- 8 In the **Edit Distribution Center** window, click **OK** to save the changes and leave this window, or **Apply** to continuing editing the Distribution Center.

See [“Scheduling distribution”](#) on page 30.

# Creating host files for LiveUpdate clients to receive updates

When a LiveUpdate client is installed, by default it is configured to connect to the Internet-based Symantec LiveUpdate server to retrieve updates. To direct LiveUpdate clients to retrieve updates from a specific distribution server instead, you must modify the configuration of the LiveUpdate client.

Users typically modify the client configuration through the administration console of the installed Symantec product, which is more convenient and the preferred method.

However, you can also create a custom LiveUpdate configuration file, called a LiveUpdate host file, through the LiveUpdate Administrator console. You can then copy this custom host file to client computers as required. When client computers run LiveUpdate, they connect to the server that is specified in the custom host file and download content from that location. To use this method, you must copy the custom host file to the LiveUpdate installation folder on client computers.

## To create a host file for LiveUpdate clients to receive updates

- 1 On the **Configure** tab, click **Client Settings**.
- 2 Select the client settings that you want to create a host file for, and then click either **Export Windows Settings** or **Export Java Settings**.
- 3 Click **Save**.
- 4 Select the location to save the file, and then click **Save**.

The file for Windows clients should be saved as `Settings.Hosts.LiveUpdate.`

The file for Java LiveUpdate clients should be saved as `liveupdt.hst`.

# Managing download and distribution schedules

This chapter includes the following topics:

- [Scheduling downloads](#)
- [Running distribution schedules automatically after the completion of a download](#)
- [Scheduling distribution](#)
- [Viewing the download tasks and distribution tasks](#)

## Scheduling downloads

You can configure LiveUpdate Administrator to download updates automatically. You specify how often you want to update and for which products you want to download updates for. You can also run manual download and distribution requests, and view the Activity Monitor, which lists LiveUpdate Administrator download and distribution requests.

You can download updates for all products and components. Or you can fine-tune downloads so that only virus definitions, or software updates, or other components are downloaded. For example, if you use Symantec Endpoint Protection, you may want to set up a schedule that downloads content updates three times a day. This schedule is typically how frequently Symantec Endpoint Protection clients receive content updates if they receive them directly from the Symantec Endpoint Protection Manager.

**To create a new download schedule**

- 1 On the **Download & Distribute** tab, in the **Schedules** window, click **Add Download**.
- 2 In the **Add Download Schedule** box, type the following:

<b>Download Schedule name</b>	Descriptive name for this schedule
<b>Status</b>	Enabled or Disabled
<b>Description</b>	Description for this schedule

- 3 In the **Select Products** box, click **Add**.
- 4 Select the products and components that you want to add to this schedule.  
 To expand the product list, click on the plus sign (+), and then select specific components. Or, check **All Products** to add all products and components to the download schedule.
- 5 Click **Add**.
- 6 Select the test status that you want to assign to the schedule.  
 By default, the test status is set to Skip Test. Set the status to Must Test to test the updates before you distribute them.
- 7 In the **Select Schedule** box, set the download schedule.
- 8 Click **OK** to save the schedule.

**To run a manual download request that is based on an existing schedule**

- ◆ In the right pane, under **Schedules**, select an existing Download Schedule, and then click **Run Now**.

**To run a new manual download request**

- 1 In the left pane, under **Scheduling Tasks**, click **Manual Download Request**.
- 2 In the **Manual Download Request - Step 1 of 2** window, select the products that you want to add to this request by clicking **Add**.
- 3 In the **Select products to be added** window, select the product or components that you want to add and then click **OK**.
- 4 Select the test status for this download request: **Skip Test** or **Must Test**.  
 The default is Skip Test.
- 5 Click **Next**.

- 6 In the **Manual Download Request - Step 2 of 2** window, select the updates that you want to download.

You can select all products and components, or you can select specific components, such as software updates or virus definitions.

- 7 Click **Next** to start the download request.

#### To delete a download schedule

- 1 On the **Download & Distribute/Schedules** list, click the box beside the schedule that you want to delete.
- 2 Click **Delete**.
- 3 Click **Confirm Delete** to finish deleting the schedule or click **Cancel** to cancel the deletion.

## Running distribution schedules automatically after the completion of a download

The Symantec LiveUpdate Administrator enables you to execute distribution schedules automatically as soon as the download is complete.

#### To execute distribution schedules automatically after the completion of a download

- 1 Perform the steps to create a new download.  
See [“Scheduling downloads”](#) on page 28.
- 2 Select **Run selected Distribution Schedules automatically after this download completes**.
- 3 Select distribution schedules from the **Available Distribution Schedules** list.
- 4 Click **Add** or **Add all**.
- 5 Click **Ok**.

## Scheduling distribution

After you download updates, they can be sent to a testing distribution server or to a production distribution server where your LiveUpdate clients can download them.

When you add a distribution schedule, you also select the products and components that you want to associate with the schedule. This list of products and components is compared with the updates in the Manage Updates folder. Any revisions that are not already distributed are then distributed in the current session.

**To add a new distribution schedule**

- 1 On the **Download & Distribute** tab, in the **Schedules** window, click **Add Distribution**.
- 2 In the **Add Distribution Schedule** box, specify the following:
  - Distribution Schedule name
  - Status, either Enabled or Disabled
  - Description
- 3 Click **Add** to select the products and components for which updates are distributed.
- 4 Select the products and components that you want to add to this schedule.  
 To expand the product list, click on the plus sign (+), and then select specific components. Or, check **All Products** to add all products and components to the distribution schedule.
- 5 Click **Add**.
- 6 In the **Distribute Content To** box, select the distribution center type: **Testing**, **Production**, or both. Then, select the Distribution Centers.  
 You can select all Distribution Centers or a subset of the centers.
- 7 Select a distribution schedule.
- 8 Click **OK** to save the schedule or click **Cancel** to cancel this action.

**To run a manual distribution request based on an existing schedule**

- ◆ In the right pane under **Schedules**, select an existing Distribution Schedule, and then click **Run Now**.

**To run a new manual distribution request**

- 1 In the left pane under **Scheduling Tasks**, click **Manual Distribution Request**.
- 2 In the **Manual Distribution Request Step 1 of 2** window, click **Add** to select the products that you want to distribution with this request.
- 3 In the **Select products to be added** window, select the products or the components, then click **OK**.
- 4 In the **Manual Distribution Request Step 1 of 2** window, select the Distribution Center Type: **All**, **All Production Centers**, or **All Testing Centers**.
- 5 Select the Distribution Center: **All** or **Subset**.

- 6 Click **Next**.
- 7 In the **Manual Distribution Request Step 2 of 2** window, select the updates that you want to distribute, and then click **Next**.

## Viewing the download tasks and distribution tasks

You can find out the status of your download and distribution tasks in the Activity Monitor and by viewing the details of the task. The status that is displayed can help you determine if your task was successful, or help you to troubleshoot a problem.

The following types of status are displayed:

- Download task status: Displays the status of download requests.
- Download update status: Displays the status of the updates that are downloaded as a part of download request.
- Distribution task status: Displays the status of distribution requests.
- Distribution update status: Displays the status of the updates that are distributed as a part of distribution request. For example, you may want to verify that Symantec Endpoint Protection updates were successfully downloaded to client.

### To view the download tasks and distribution tasks

- 1 On the **Download & Distribute** page, click **Activity Monitor**.
- 2 To filter which events you want to see, click the Show Filters icon to the right of the Activity box.

You can filter activities by type, status, and time, either by the start time or by when the last change occurred.

### To view details for specific tasks

- ◆ Click on the ellipses option that appears to the right of the % column for the task that you want to view.

# Configuring LiveUpdate Administrator

This chapter includes the following topics:

- [Configuring LiveUpdate Administrator preferences](#)
- [Managing updates for products](#)
- [Adding or modifying user accounts](#)
- [Forcing a user to log off LiveUpdate Administrator](#)
- [Backing up and restoring your LiveUpdate Administrator configuration](#)
- [Best practices for increasing security in LiveUpdate Administrator](#)

## Configuring LiveUpdate Administrator preferences

[Table 5-1](#) displays the tasks for which you can configure settings on the **Preferences** page.

**Table 5-1** Preferences page settings

Task	Description
Specify the folders where updates are installed	You can change the default folder where downloaded content updates is stored temporarily and permanently.  See <a href="#">“Installing LiveUpdate Administrator”</a> on page 15.

**Table 5-1**      **Preferences** page settings (*continued*)

Task	Description
Set schedules for purging older updates	<p>You can set up a schedule and rules for purging older updates, in both the Manage Updates folder and the distribution centers.</p> <p>When you download updates, they are copied to the Manage Updates folder that you specified during installation. All updates in the Manage Updates folder, except for the latest three revisions, are set to be purged daily by default. You can specify rules to determine which updates to delete, based upon the age of the revision or when the updates were initially downloaded.</p> <p>See <a href="#">"Managing updates for products"</a> on page 35.</p>
Reduce the database size	<p>To save disk space, you can specify how often to reduce the data in the database and the Activity Monitor.</p> <p>See <a href="#">"Viewing the download tasks and distribution tasks"</a> on page 32.</p>
Enable bandwidth throttling for each location server	<p>Bandwidth throttling lets you manage distribution in the environments that have both high-bandwidth and low-bandwidth networks.</p> <p>See <a href="#">"Adding distribution centers"</a> on page 25.</p>
Specify the password length	<p>You can change of the minimum number of characters for user account passwords.</p> <p>See <a href="#">"Adding or modifying user accounts"</a> on page 38.</p>
Change the type of events that appear in the Event log	<p>See <a href="#">"Viewing information in the Event Log"</a> on page 44.</p>
Configure the source server connection	<p>You can configure connection settings from a source server to Symantec clients.</p> <p>See <a href="#">"Configuring Source Servers"</a> on page 23.</p>
Configure a mail server, email recipients, and notifications	<p>You can configure which mail server you want to use to send notifications. You also specify which email recipients get the notifications, and the type of notifications you want to send.</p>
Enable or disable automatic updates to the <b>Symantec Product Catalog</b>	<p>See <a href="#">"Updating the Symantec Product Catalog"</a> on page 22.</p>

**To configure LiveUpdate Administrator preferences**

- 1 Click the **Configure** tab, and then click **Preferences**.
- 2 Click **Update** to save your changes.

To restore default configuration settings

- 1 Click **Configure > Preferences**.
- 2 On the **Configure Application Preferences** window, click **Reset To Defaults**.
- 3 Click **Confirm**.

## Managing updates for products

**Manage Updates** is where you can manage all of the updates for the products you have selected in **My Symantec Products**.

- You can view, approve, distribute, and delete updates.
- You can define the types of updates that you want to download, and whether or not they need to be tested before they are distributed.

You can change the default location for updates after you install the LiveUpdate Administrator.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

To manage the updates for distribution

- 1 On the **Manage Updates** page, click **Show all updates**.

If you have not added any products to **My Symantec Products**, an error message appears, and you are prompted to create a list of your products.

See [“Updating the Symantec Product Catalog”](#) on page 22.

See [“Adding Symantec products to the product list”](#) on page 22.

Updates appear under **Product/Component**. **Product/Component** is the product name and component name for which updates are downloaded.

You can view the contents of the download folder using either the list view or the details view. The list view displays all of the current downloaded updates and definitions for all products. Updates from older revisions do not appear. However, you can use the detail view to view older updates.

- 2 If you want to filter the list to display fewer products, click **Select filter**.

You can show only updates for a specific product, or for updates based on criticality or by the date that the update was downloaded.

- 3 To view the revision details and the distribution status specific update component, click the ellipses option ([...]) that appears to the right of the **Distribution Coverage** column.
- 4 To start a manual distribution task for a selected product update, click **Distribute Content**.

## Deleting revisions

You can delete revisions from the **Manage Updates** folder. All updates and TRI files are deleted. If you delete the current revision, any older revisions still in the folder become the current revision and are downloaded during the next download event. Locked revisions cannot be deleted.

### To delete an update revision

- 1 In the **Manage Update** window, expand the **Product / Component** list.
- 2 Select the revision that you want to delete.
- 3 Click **Delete**.

## Locking and unlocking revisions

You can lock an update revision to a specific distribution center. When the revision is locked, new revisions are downloaded, but they are not available to that distribution center. A padlock appears beside the distributed revision in the **Distribution Status** list.

### To lock a revision

- 1 In the **Manage Updates** window, expand the **Product/Component** list.
- 2 Click the ellipses option to the right of the **Distribution Coverage** column for the update that you want to lock.
- 3 In the **Update Details** window, in the **Distribution Status** box, select the Distribution Center that you want to lock, and then click **Lock To**.
- 4 In the **Manage Updates - Add Lock** window, select the revision you want to lock, and then click **OK**.
- 5 In the **Manage Updates - Confirm Add Lock** window, click **OK**.

### To unlock a revision

- ◆ In the **Manage Update** details window, click **Unlock**.

## Testing updates

When you create a download schedule or run a manual download request, you must set the testing status of the updates that you download. Updates can be marked as either Skip Test or Must Test. Updates that do not have to be tested can be sent directly to a production distribution center and are available for immediate downloading.

Each downloaded update has an associated testing state. The testing state lets you know whether the update has been tested and what stage the update is in.

The possible testing states are as follows:

Untested	The update has not been tested, but must be tested before it can be distributed to a production distribution center. This content has not yet been placed to a testing distribution server.
Passed	The update has been successfully tested and is ready to be sent to a production distribution center.
Failed	The update has failed testing. This update cannot be distributed to a production distribution center.
Test Not Required	The update does not require testing before being distributed to a production distribution center.
Faulty	The update initially passed testing, and was distributed to a production distribution center, but was later found to have problems.
Retest	The update that has been found to be faulty, or has failed testing, and you want to retest it.

You can view the test status of downloaded updates in Manage Updates. Updates that have been marked Untested can be sent to a testing distribution center, where they can then be distributed for further testing. After you have completed testing the updates, you can then mark them as Passed or Failed. Passed updates can then be sent to production distribution centers. Failed updated can be resent to the testing distribution center for further testing and the status changed to Retest.

Updates that you distribute to production distribution centers are either marked as Skip Test or Passed. If you find any issues with the updates after they have been distributed to a production center, you can mark them as Faulty and send them back to a testing center for further testing (the status is changed to Retest).

Only updates that are marked as Passed or Skip Test can be sent to a production distribution center. LiveUpdate Administrator will not allow updates marked Test Failed or Faulty to be sent to any production distribution center. Updates that are marked Untested will not be automatically sent to a production distribution center, but you can send them to a testing distribution center.

---

**Note:** Some update components are shared between products. If you have specified that updates for a particular product must be tested, any shared component updates will automatically be set to Must Test, and will display a status of Untested when they are downloaded.

---

If you set the status of an update to Must Test, but have not yet tested it, LiveUpdate Administrator sets the testing state to Untested. Otherwise, the status is set to Testing Not Required.

If the update state is Untested, LiveUpdate Administrator will send the update to the appropriate testing distribution center. This can happen automatically, based upon a schedule that you determine, or you can distribute the update for testing manually.

Once you have completed testing the update, you set the status to Test Passed or Test Failed. Updates marked as Test Passed will then be available to production distribution centers.

If the update has failed, you can retest the update, delete the update, or simply leave it in the Manage Updates folder.

If you have distributed an update to a production distribution center, and later determine that it is problematic, you can mark the update Test Faulty. This will prevent future operations from distributing the update to production distribution centers.

## Adding or modifying user accounts

You may want to add multiple logon accounts so that different users can manage different Symantec products.

You can add a user with either an administrator role or a user role. An administrator role has complete access to the system. The user role restricts users to the following tasks:

- Manually downloading updates
- Manually distributing updates
- Changing the status of updates in Manage Updates
- Changing user account information

---

**Note:** If users do not log on with the correct credentials after five attempts, the account locks them out. Users must wait 15 minutes before the account unlocks.

---

### To add a user account

- 1 On the **Manage Users** page, click **Add**.
- 2 Enter the information for the new user.
- 3 Click **OK**.

**To modify a user account**

- 1 On the **Manage Users** page, click the ellipse option to the right of the account name.
- 2 Change the password or user information.  
To change the password, first check **Change Password**.
- 3 Click **Update**.

See [“Forcing a user to log off LiveUpdate Administrator”](#) on page 39.

## Forcing a user to log off LiveUpdate Administrator

You can log off any administrator who is currently logged onto LiveUpdate Administrator.

**To force a user to log off**

- ◆ Check the box beside the user's name, and then click **Force Log Off**.

See [“Adding or modifying user accounts”](#) on page 38.

## Backing up and restoring your LiveUpdate Administrator configuration

If you need to reinstall LiveUpdate Administrator after a server failure, you use a recovery configuration file to restore the previously active configuration.

The configuration file includes:

- Products that you selected in the **My Symantec Products** list
- Custom Source Server information
- Distribution Centers
- Download schedules
- Distribution schedules
- Preferences

**Table 5-2** Steps to back up and restore the configuration

Steps	Description
Step 1	<p>Create and export a compressed recovery configuration file.</p> <ul style="list-style-type: none"> <li>■ Use the following method if you restore the configuration on the same version of LiveUpdate Administrator, such as 2.3.3 to 2.3.3. You also use this method to restore between versions earlier than 2.3.3, such as from 2.3.0 to 2.3.1 or from 2.3.1 to 2.3.2.  <a href="#">To create a recovery configuration file to and from the same version of LiveUpdate Administrator</a></li> <li>■ Use the following method if you restore the configuration from 2.3.0, 2.3.1, or 2.3.2 to 2.3.3.  <a href="#">To create a recovery configuration file from versions 2.3.0 through 2.3.2 to a later version</a></li> </ul>
Step 2	<p>Reinstall LiveUpdate Administrator.</p> <p>See <a href="#">“Installing LiveUpdate Administrator”</a> on page 15.</p>
Step 3	<p>Import the recovery configuration file into LiveUpdate Administrator.</p> <p><b>Warning:</b> The <b>Configuration Restore</b> page is only available after you log on to LiveUpdate Administrator and click the <b>Home</b> page for the first time. After you navigate away from the <b>Home</b> page, this option is no longer available and you must reinstall LiveUpdate Administrator to see the <b>Configuration Restore</b> page.</p> <p>See <a href="#">“To import the recovery configuration file”</a> on page 42.</p>

**To create a recovery configuration file to and from the same version of LiveUpdate Administrator**

- 1 On the **Configure** tab, click **Export**.
- 2 Click **Export configuration recovery file**.
- 3 In the **File Download** dialog box, click **Save**.
- 4 In the **Save As** dialog window, browse to the folder where you want the backup file saved.
- 5 In the **File name** box, specify a file name.  
 A default file name automatically appears, but you can change this name if you want. Ensure that the file extension remains .zip.
- 6 Click **Save**.  
 Save the compressed file to the computer where you install LiveUpdate Administrator and import this configuration file.

**To create a recovery configuration file from versions 2.3.0 through 2.3.2 to a later version**

- 1 Do one of the following tasks:
  - If the computer that runs LiveUpdate Administrator does not have IPv6 support, go to step 4.
  - If the computer that runs LiveUpdate Administrator has IPv6 support, locate and open the following file in a text editor:

```
<install_path>\pgsql\data\pg_hba.conf
```

---

**Note:** You must uncomment IPv6 in the `hba` configuration file.

---

- 2 In the `pg_hba.conf` file, locate the following text:

```
# IPv6 local connections:
#host all all ::1/128 trust
```

Replace:

```
#host
```

With:

```
host
```

- 3 Save the file and close the text editor.
- 4 Open a command prompt window and navigate to: `<install_path>\pgsql\bin`
- 5 Type one of the following commands:

For 2.3.1 and 2.3.2, type: `pg_dumpall -U lua -p 7072 -f LUA_backup.sql`

For 2.3.0, type: `pg_dumpall -U lua -p 7072 > LUA_backup.sql`

---

**Note:** If you changed the PostgreSQL port when you installed LiveUpdate Administrator, use the modified port instead of 7072.

---

This step generates the `LUA_backup.sql` dump file in the `\pgsql\bin` directory.

- 6 Copy the `LUA_backup.sql` file to a temporary folder on your Desktop.
- 7 Navigate to: `<install_path>\tomcat\webapps\lua\WEB-INF\classes`.
- 8 Copy the file `lua.xml` to the same temporary folder that you created in step 6.

- 9 In the temporary folder, compress the following files together into a compressed file: `lua.xml` and `LUA_backup.sql`

Do not compress the temporary folder in which files reside, only the files themselves.

- 10 Save the compressed file to the computer where you install LiveUpdate Administrator and import this configuration file.

**To import the recovery configuration file**

- 1 Log on to LiveUpdate Administrator.
- 2 On the **Home** tab, in the **Configuration Restore** pane, click **here**.
- 3 In the **Configuration Restore** dialog box, browse to the compressed configuration backup file, and then click **OK**.
- 4 For version 2.3.3, restart the PostgreSQL and Tomcat services.

---

**Warning:** If you navigate away from the **Configuration Restore** page before you restart these services, you may corrupt the database.

---

A message appears indicating the configuration is successfully restored.

## Best practices for increasing security in LiveUpdate Administrator

You can protect your LiveUpdate Administrator data from outside attacks by implementing the following practices:

- Attackers can obtain information from the troubleshooting file, the exported configuration file, and the client settings file. Therefore, make sure that only authorized users can access these files.
- Attackers can tamper with the contents in the distribution centers. Therefore, make sure that only authorized users can access the distribution centers. See [“Adding distribution centers”](#) on page 25.
- Use an SMTP mail server that supports authentication schemes other than NTLM only.

LiveUpdate Administrator uses an SMTP server for the mail server, which requires you to add a user name and password if that particular SMTP server requires authentication. However, the NTLM authentication method does not require you to provide the user name and password because the Microsoft Windows single sign-on mechanism provides the necessary credentials.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

# Viewing events and troubleshooting information

This chapter includes the following topics:

- [Viewing information in the Event Log](#)
- [About the troubleshooting file](#)
- [Generating the troubleshooting file](#)

## Viewing information in the Event Log

The LiveUpdate Administrator Event Log records and displays information about the events that LiveUpdate Administrator generates. For example, you can view information about download and distribution, user accounts, schedules, and product updates.

You can filter the events by event type, users, and severity. You can also designate a specific date or a range of dates for the report and export the report to a comma-separated file. Events can also be deleted from the log.

You can change some log settings on the **Preferences** page.

See [“Configuring LiveUpdate Administrator preferences”](#) on page 33.

**To view the Event Log**

- 1 On the **Home** page, click **Event log**.
- 2 On the **Event Log** page, click **Select Filter** to specify which kinds of events you want to see.
- 3 To export the log to a comma-separated file, click the icon to the right of the **Description** field.

## About the troubleshooting file

The LiveUpdate Administrator can automatically collect environmental and troubleshooting data. This troubleshooting data may reduce the time that is taken for Symantec Technical Support to identify the cause for a LiveUpdate Administrator issue.

The following information is collected in the troubleshooting file for analysis:

- Current processes running
- Current services running
- Application logs
- Application configuration files
- Network configuration
- List of application files
- Application thread dump
- Updates being managed
- MSinfo - Windows information

See [“Generating the troubleshooting file”](#) on page 45.

## Generating the troubleshooting file

The LiveUpdate Administrator sometimes may not function as desired. To identify the exact issue, you require environmental and troubleshooting information. LiveUpdate Administrator enables you to collect the troubleshooting information in an `luadebuginfo.zip` file. You can generate this file and send it to Symantec Technical Support to identify the root cause of the issue.

**To generate the troubleshooting file**

- 1 On the LiveUpdate Administrator user interface, click **Troubleshoot**.
- 2 Click **Begin**.
- 3 Click **Save**.
- 4 Select the location in your system where you want to save this file, and then click **Save**.

# Index

## A

- accounts
  - adding 38
- Activity Monitor
  - viewing 32
- administrators
  - adding 38

## B

- bandwidth throttling
  - enabling 26

## C

- client settings 27

## D

- distribution
  - running 30
  - running a manual request 31
  - scheduling 30
- Distribution Centers
  - adding 25
- downloads
  - deleting schedule for 30
  - running a manual request 29
  - scheduling 28

## E

- Event Log
  - about 44

## F

- failover servers
  - configuring 24
  - promoting 24

## G

- getting started 18

## L

- LiveUpdate Administrator
  - home page 20
  - installing 15
  - requesting a temporary password for 16
  - system requirements 12
- liveupdt.hst 27
- locations 25
- logging off
  - other users 39
- LUA Startup
  - in Event Log user list 44

## M

- Manage Updates
  - about 35
- My Products
  - adding 22
  - deleting 22
- My Symantec Products
  - tasks 22

## N

- new features 10

## O

- overview 18

## P

- passwords
  - changing 38
- Product Catalog
  - updating 22

## R

- reports 44
- revisions
  - deleting from Manage Updates 36
  - locking and unlocking 36

**S**

Settings.Hosts.LiveUpdate 27

Source servers

- configuring 23

- default 23

- failover servers 23

- resetting to defaults 24

system requirements 13

**T**

testing

- states 36

- updates 36

troubleshooting file 45

**U**

updates

- default download location 35

users

- adding 38

- logging off 39