LiveUpdate Administrator Architecture, Sizing, and Performance Recommendations

Legal Notice

Architecture, sizing, and performance recommendations

This document includes the following topics:

Introduction

The Symantec LiveUpdate Administrator (LUA) can be configured and deployed in several different configurations. The purpose of this document is to outline Symantec recommended architectures for the Symantec LiveUpdate Administrator version 2.2, and to describe the recommendations for single and multiple site

environments. For the purposes of this document, a site is defined as a physical location that contains a group of clients that need to be kept up-to-date.

The following architectures and designs are based on metrics from internal product testing done in a closed environment. Implementation in production environments may encounter different metrics that would affect the recommended sizing and architecture.

Any changes or planned modifications to product capability, function, metrics, and/or features discussed are subject to ongoing evaluation by Symantec, and should not be considered as final recommendations by Symantec.

Background

The Symantec LiveUpdate Administrator is an enterprise Web application that lets you manage Symantec product updates on multiple internal LiveUpdate servers. Using the Symantec LiveUpdate Administrator, you download product updates to a local machine, and then distribute the updates to production servers for LiveUpdate clients to download, or to testing servers, so that the updates can be tested before they are distributed to a production system. You can download and distribute updates on schedule, allowing you to create a low maintenance, reliable system that can be set up once, and then run automatically. Updates can also be manually downloaded and published as needed.

Note: The LiveUpdate Administrator can download and distribute content for a wide variety of Symantec products. The content is dynamic, and the size and frequency of available content can change daily.

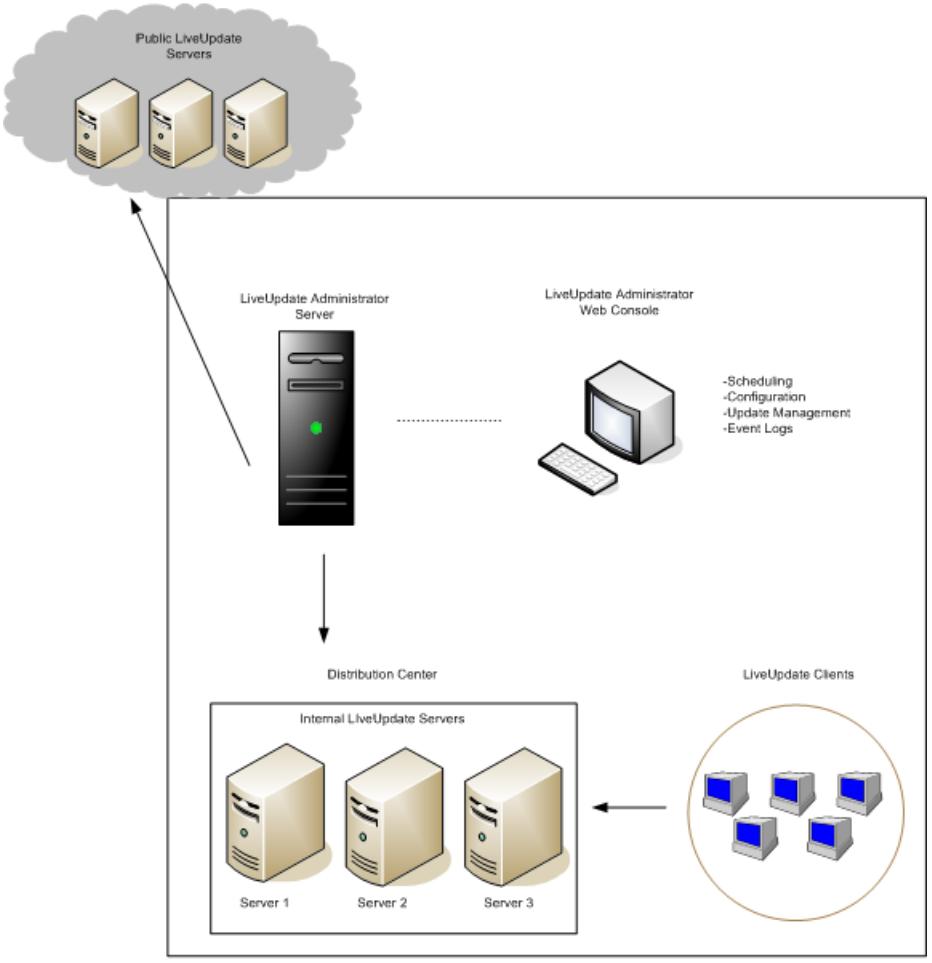
The following are some common scenarios where you would consider leveraging LiveUpdate Administrator in your environment:

- You are responsible for managing multiple Symantec products in your environment and you want to point all these products to one internal source for update.
- You want to test the content before rolling it out to the production system.
- You want a backup update mechanism for your endpoints in case content update using management servers (for example, a Symantec Endpoint Protection Manager server) is unavailable for some reason (hardware failure, and so on).
- Your management server (for example, a SYMANTEC ENDPOINT PROTECTION MANAGER server) does not have direct access to the internet.
- In a large scale deployment of Symantec Endpoint Protection:

- You want to remove load from the SYMANTEC ENDPOINT PROTECTION MANAGER servers of regular content processing and provision, so they can swiftly and efficiently provide policies, deliver reporting, and so on.
- You want absolute scheduling control of when updates are distributed from central server to endpoints at remote sites (across WAN Links).
- You have a large number of remote sites with more than 200 endpoints per site.

Architecture

The Symantec LiveUpdate Administrator (LUA) contains four main architectural components that work together to allow you to download LiveUpdate content to the computers in your environment.



LUA Server	The LiveUpdate server that facilitates the download and distribution of content to multiple locations, called distribution centers.

LUA Distribution Center	A group of internal LiveUpdate (LU) servers (test or production) where the content is distributed for LiveUpdate clients to download. An internal LU server (sometimes referred to as Central LiveUpdate server) can be a file share, an FTP server, or a Web server.
LiveUpdate Client	Software that you deploy to company computers to download Symantec content from either a public LiveUpdate Server or LUA Distribution Centers.
LUA Console	A console that provides the ability to configure test and production distribution centers, schedule download and distribution of content, and to review event logs.

When you plan for LUA in your environment, several design decisions must be considered, for example:

- How many geographic locations are there within the company?
- How frequently does Symantec publish content for product(s) that you are managing in your environment?
- How often do you want to provide content updates?
- Which method of content distribution do you want to use (third party vs. the LUA distribution feature)?
- How many end points (desktops, laptops, servers, and so on) exist at each location?

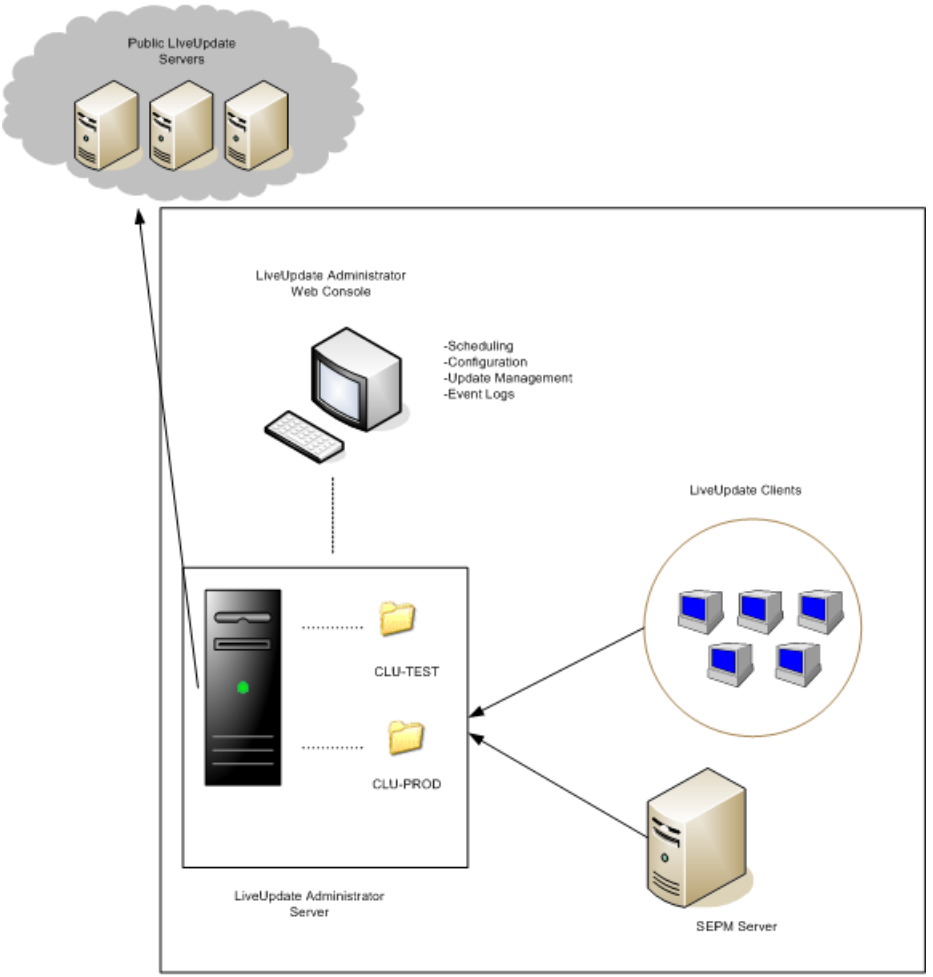
Single site design

In the situations where LUA is used to host content at one site, Symantec recommends the single site design.

This design is typically applicable but not limited to the following scenarios:

- If you want to test the content before the management server (for example, SYMANTEC ENDPOINT PROTECTION MANAGER server) pushes the content to endpoints. Once the content is tested, LiveUpdate clients can be pointed to the internal management server for updates, instead of going to the public LU servers.

- If your management server (for example, SYMANTEC ENDPOINT PROTECTION MANAGER server) does not have direct access to the internet.
- If you are using the LUA server as a back up update mechanism.



Single Site Design

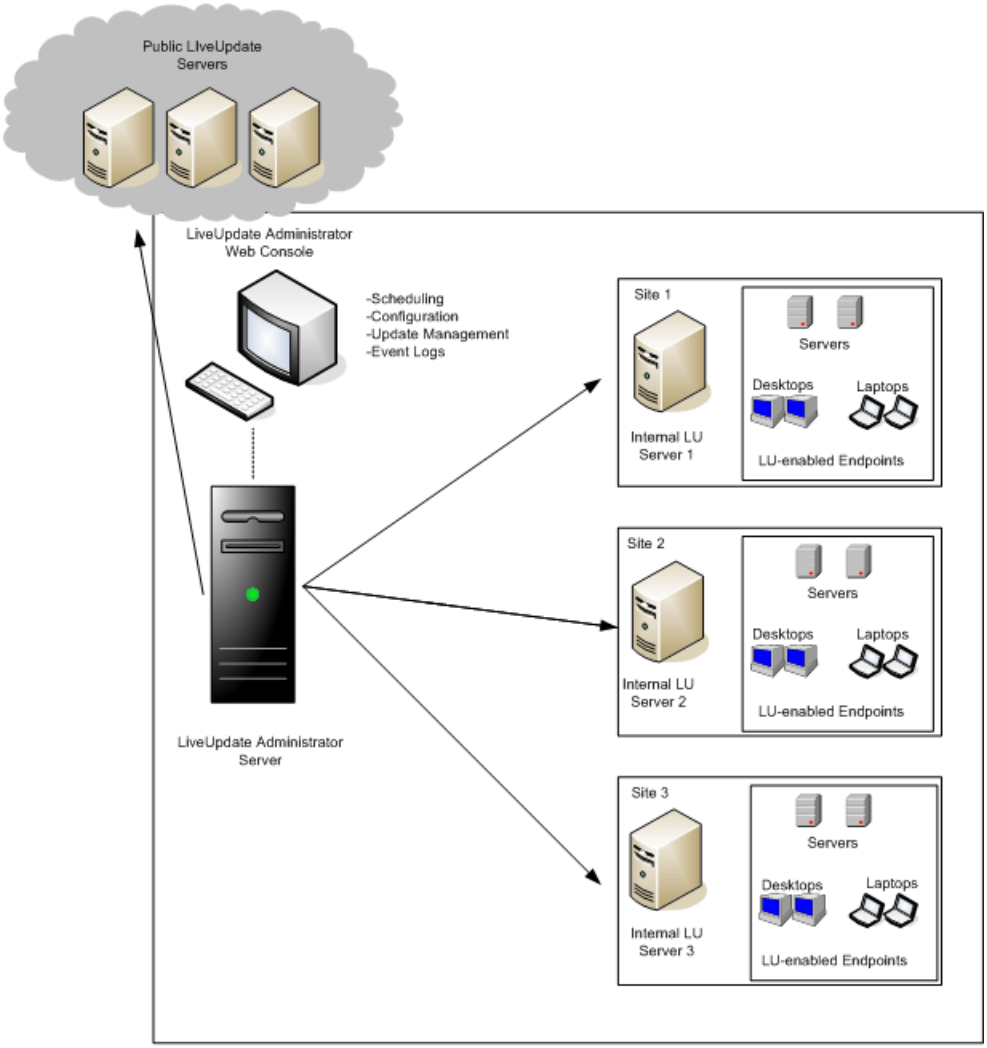
In the single site scenario, it is recommended that one LUA server be used. The distribution center that is created during installation (production and test) on the same computer can be leveraged to host the content. Additional internal LU servers

(called Location in LUA configuration) can be added to the distribution center if required.

Please note that the LUA server and the SYMANTEC ENDPOINT PROTECTION MANAGER server can be installed on the same computer if required.

Multiple site design

In scenarios where the LiveUpdate Administrator is used to host content at more than one site, typically in an organization that has multiple large physical locations, Symantec recommends a multiple site design. In the multiple site design, Symantec recommends at least one internal LU server per site for the local caching of the content, in order to conserve WAN bandwidth. Each site may require more than one internal LU server for proper load balancing, depending on the number of end points that need to be kept up-to-date.



Multiple Site Design

Scalability guidelines for LiveUpdate Administrator

Symantec recommends no more than 100 distribution center locations for a single LiveUpdate Administrator server.

If your organization needs to support more than 100 internal LiveUpdate servers, then it is recommended that you use additional LiveUpdate Administrator servers.

These servers are managed independently. You will lose centralized management capability with multiple LiveUpdate Administrator servers, but you can use other methods for distributing content. Using this approach, you can download and distribute content to a single location using the LiveUpdate Administrator server (similar to the single site example), and leverage any file replication techniques for distribution to multiple locations.

Here are some alternatives that you may want to consider for distributing content:

- Microsoft ™ Robocopy to distribute content to a Windows share (recommended)
- VERITAS File Replicator (recommended)
- Microsoft DFS in a stable DNS environment
- Xcopy
- Easy File Sync ™
- ViceVersa
- PeerSync

Example: Content size for Symantec Endpoint Protection 11

The LiveUpdate Administrator is designed to download and distribute all available updates for a product. All updates are downloaded and distributed in their entirety. Virus definitions are published up to three times a day, and can make up nearly 90 percent of total data.

The following table displays the amount of data that is typically downloaded and distributed using the LiveUpdate Administrator for Symantec Endpoint Protection 11.x virus definitions.

Table 1-1 Data sizes for daily and once a month downloads

Product	Initial load	Average load size/daily session	Average load size/once a month session (when monthly hubs are published)
Symantec Endpoint Protection 11 32 Bit only	250-280 MB	25-30 MB	250-280 MB

Table 1-1 Data sizes for daily and once a month downloads *(continued)*

Product	Initial load	Average load size/daily session	Average load size/once a month session (when monthly hubs are published)
Symantec Endpoint Protection 11 32 and 64 Bit	425-450 MB	50 MB	425-450 MB

Even though the LiveUpdate Administrator downloads and distributes all of the permutations of virus definitions to distribution center locations (servers), end points that are updated on a regular basis download only the delta virus definitions packages. These packages are typically only a few Kbytes in size (<1MB).

As noted previously, Symantec recommends at least one internal LiveUpdate server for each site for local content caching. This conserves WAN bandwidth. However, if you are deploying Symantec Endpoint Protection 11.x, and you have less than 100 computers at a site, and if the WAN link is relatively slow, then you do not need to set up a distribution center at that location. The computers at such sites can be configured to get updates using the Group Update Provider, the Symantec Endpoint Protection Manager server, or download updates directly from public LiveUpdate servers.

Configuring distribution centers and schedules

A distribution center is a collection of locations (servers). Content distribution schedules are set at the distribution center level. You can have a single schedule for either one distribution center or for multiple distribution centers, but you cannot have a separate schedule for a location within a distribution center.

It's important to understand how the LiveUpdate Administrator distributes content before you configure your distribution centers. The LiveUpdate Administrator server has a built-in queuing mechanism for content distribution. It is capable of distributing content to a maximum of ten distribution center locations concurrently at any given time. If a schedule for one or more distribution centers has completely occupied the queue, subsequent schedules will have to wait. But the second schedule does not have to wait until the first is totally completed. As soon as distribution for one of the locations is complete, and if there are no additional locations awaiting distribution for the same schedule, then distribution for one location in the subsequent schedule will start immediately.

Configuring distribution centers for a high bandwidth network

The following configuration recommendations are for the environments where the majority of the links have high bandwidth (T1 or above.)

Configuring multiple servers into a single distribution center

This design is typically applicable, but not limited to, the following scenario:

- You have less than 100 locations and the update frequency is the same for all locations. For example, you have 100 servers that will be hosting Symantec Endpoint Protection content for 32-bit computers and you need to update those servers once a day. You can configure a single distribution center with 100 locations.

It is not required to configure 100 servers into a single distribution center. You can divide them into multiple distribution centers if you wish. The only real disadvantage in configuring multiple distribution centers is that it can be time-consuming.

Configuring multiple servers into multiple distribution centers

This design is typically applicable, but not limited to, the following scenarios:

- You have less than 100 locations, and the update frequency is different for all the locations. For example, you have 100 servers that will be hosting Symantec Endpoint Protection for 32-bit computers, and 50 of the servers are based in the United Kingdom. These 50 need to be updated once a day. The remaining 50 are located in Germany, and they need to be updated three times a day. You will need to create two distribution centers, one for the United Kingdom with 50 servers, and the other for Germany, also with 50 servers. Since both are split into two separate distribution centers, each can have its own schedule.
- You have less than 100 locations, and the update frequency is the same for all the locations, but you need to distribute content at different times. For example, you have 100 servers that will be hosting Symantec Endpoint Protection for 32-bit computers, and 50 of the servers are located in the United Kingdom. These are to be updated once a day. The remaining 50 are located in the United States. You also want to update them once a day, but you would prefer to distribute content during non-business hours. In this case, you would create two distribution centers, one for the United Kingdom servers, and one for the United States. Since you have created two separate distribution centers, each can have its own schedule.
- You have less than 100 locations, but you prefer to manage distribution centers per region or per country. For example, you have 100 servers that host Symantec Endpoint Protection for 32-bit computers. These servers are located

across the globe and you want to create one distribution per country. (This should not be considered to be a recommendation as such).

Configuring distribution centers for low to medium bandwidth networks

Designing content distribution architecture becomes challenging if you have large number of sites with medium or low bandwidth. The content distribution time becomes critical when designing LiveUpdate Administrator architecture in these scenarios.

The following are the key factors that contribute to content distribution time:

- The size of the content that is distributed.
- The total number of servers to which content is to be distributed.
- Networking parameters
  Network connection speed of LAN and WAN links, bandwidth availability during distribution, latency, bandwidth throttling settings, packet loss, and so on.

The following table is an example of content distribution times for different bandwidth for content size between 1 - 100 MB.

Table 1-2

	1 MB	30 MB	50 MB	100 MB
56.6 Kbps	142 seconds	71 minutes	120 minutes	238 minutes
64 Kbps	125 seconds	62 minutes	104 minutes	208 minutes
128 Kbps	62 seconds	31 minutes	52 minutes	104 minutes
T1 1.544 Mbps	5 seconds	3 minutes	5 minutes	10 minutes
T3 45 Mbps	< 1 second	10 seconds	10 seconds	20 seconds

The following table is an example of content distribution time for different bandwidth for the content size between 200 - 400 MB.

Table 1-3

	250 MB	350 MB	400 MB	500 MB
56.6 Kbps	595 minutes	833 minutes	952 minutes	1190 minutes
64 Kbps	520 minutes	729 minutes	833 minutes	1041 minutes
128 Kbps	260 minutes	364 minutes	416 minutes	520 minutes

Table 1-3 *(continued)*

T1 1.544 Mbps	25 minutes	35 minutes	40 minutes	50 minutes
T3 45 Mbps	51 seconds	72 seconds	82 seconds	103 seconds

The LiveUpdate Administrator distributes on average 20 - 25 MB of data for 32-bit computers, and 50 MB of data for 32-bit and 64-bit computers combined, on a daily basis for virus definitions. The initial push, as well as a once a month push, can be as high as 250 - 300 MB for 32-bit computers, and 400 - 450 MB for 32-bit and 64-bit computers combined.

If you have a large number of medium or small bandwidth sites, then these sites will take up most of the distribution queue, since LiveUpdate Administrator only distributes content to ten servers at a time. This can potentially cause delays in distribution of content to the high bandwidth sites after the initial distribution.

For example, if you have 80 sites with high bandwidth (1.54 Mbps) and 20 sites with low bandwidth (56.6 Kbps), then you will run into a situation where the LiveUpdate Administrator will be distributing to all ten sites that are low bandwidth, regardless of how you configure and schedule distribution centers for those sites.

Symantec recommends that you measure content distribution time for average content size, as well as for maximum content size in your environment during the test cycle. The numbers gathered during such tests can be very critical when deciding your update architecture.

If you have a large number of low and medium bandwidth sites, then Symantec recommends that you either use the Group Update Provider feature of Symantec Endpoint Protection Manager, or configure additional LiveUpdate Administrator servers for distribution.

Use the following guidelines to help you when planning your LiveUpdate Administrator architecture in a large enterprise environment:

- For high bandwidth sites, you have a great deal of flexibility. You can either use the Symantec Endpoint Protection Manager server, a Group Update Provider, or a LiveUpdate Administrator distribution center. A LiveUpdate Administrator distribution center is recommended if you have a large number of computers at each site. A LiveUpdate Administrator server also reduces the load on Symantec Endpoint Protection Manager servers.
- For medium bandwidth sites, depending upon how many you have, you can use either a LiveUpdate Administrator distribution center, or Group Update Provider.

- For low bandwidth sites, LiveUpdate Administrator can be very ineffective due to the amount of data that is distributed. We strongly recommend that you use the Group Update Provider for such sites.

LUA server recommendations

2 GB minimum RAM

Single processor

The installed size for the LUA server is approximately 100 MB, which includes the Java Runtime Environment (JRE.) Approximately 5 GB hard disk space is required for the Manage Updates folder and for the temporary download folder.

Example: Calculating total disk space requirements

This scenario shows an example of the space consumed during a test implementation of LUA Server.

The example assumes the following metrics:

- Product: Symantec Endpoint Protection version 11
- Two distribution center locations (clu-prod and clu-test) on the same computer
- Continuous (every 15 minutes) download and distribution for 30 days
- Weekly purge for the Manage Updates folder
- Monthly purge for the distribution center locations
- Retention of the entire set of logs

Table 1-4 Space calculation examples

Item	Space required
Database	162 MB
Tomcat	566 MB
Events in log (400 entries)	47.8 MB
Manage Updates folder	997 MB
Temp Download folder	1.42 MB
Distribution center location 1 (clu-prod)	5.2 GB
Distribution center 1 (clu-test)	5.2 GB

Table 1-4 Space calculation examples *(continued)*

Item	Space required
Estimated total size	12 GB

Additional information

For more information on installing, configuring, and troubleshooting LiveUpdate Administrator, please see the following documents:

Title	After installing LiveUpdate Administrator 2.1 you have a new user account: LUASrvUser
Document ID	2007102610170548
URL	http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007102610170548?Open&seg=ent
Title	LiveUpdate Administrator 2.1 Distribution Scheduler does not execute distribution jobs as expected
Document ID	2008041114350748
URL	http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008041114350748?Open&seg=ent
Title	Installing and configuring LiveUpdate Administrator 2.1
Document ID	2007101913262648
URL	http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007101913262648?Open&seg=ent
Title	Symantec Endpoint Protection: Troubleshooting a failed installation of LiveUpdate Administrator 2.1
Document ID	2007101913464148
URL	http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007101913464148?Open&seg=ent
Title	Tips for Using Microsoft's Internet Information Services (IIS) 6.0 to host content for Server using HTTP
Document ID	2005051911001948

URL	http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2005051911001948?Open&seg=ent