WHITE PAPER: BEST PRACTICES

Confidence in a connected world.

Sizing and Scalability Recommendations

for Symantec Endpoint Protection

Rev 2.3

Symantec Enterprise Security Solutions Group

Contents

Introduction

Symantec Endpoint Protection provides best-of-breed endpoint security to enterprises of all sizes. Several decisions factor into correctly sizing and deploying the Symantec Endpoint Protection environment for optimum protection and serviceability. This white paper provides the following information:

- Detailed recommendations for single- and multiple-site environments
- Client-to-server ratios
- Database sizing recommendations
- Log-keeping and maintenance

Please note the following:

- The architectures, designs, and recommendations provided in this guide are based on metrics from internal testing of the product. These tests are performed in an isolated environment. Implementations in production environments may result in performance metrics that vary from the testing scenarios. These variations can alter the recommended sizing and architecture.
- This guide references possible changes and modifications to Symantec Endpoint Protection capability, functions, metrics, and features. These changes are subject to ongoing evaluation and should not be considered as firm commitments by Symantec.

The challenge of sizing security protection in the enterprise

Successful Symantec Endpoint Protection configurations and deployments depend on several variables, including the following:

- The Symantec Endpoint Protection technologies to be deployed
- Whether different security policies are needed for users in different locations
- Whether different policies are needed for desktops, servers, laptops, users, and departments
- The number of geographic locations within the company
- The frequency at which content updates are applied
- Whether Symantec Endpoint Protection patches should be automatically deployed
- The desired method of content distribution
- Whether High Availability infrastructure is present or desired
- Log retention times

- The frequency of requests for log or reporting data older than one week, one month, and one year
- Frequently gathered metrics
- Who and where people are that need access to the data
- Whether multiple administrative groups exist within the organization (for example, IT, Security, Desktop, Server)
- Requirements to tie into an existing third-party tool or authentication scheme

Knowing how to evaluate these variables is crucial to establishing an effective, efficient, and sustainable endpoint protection solution.

System design and planning

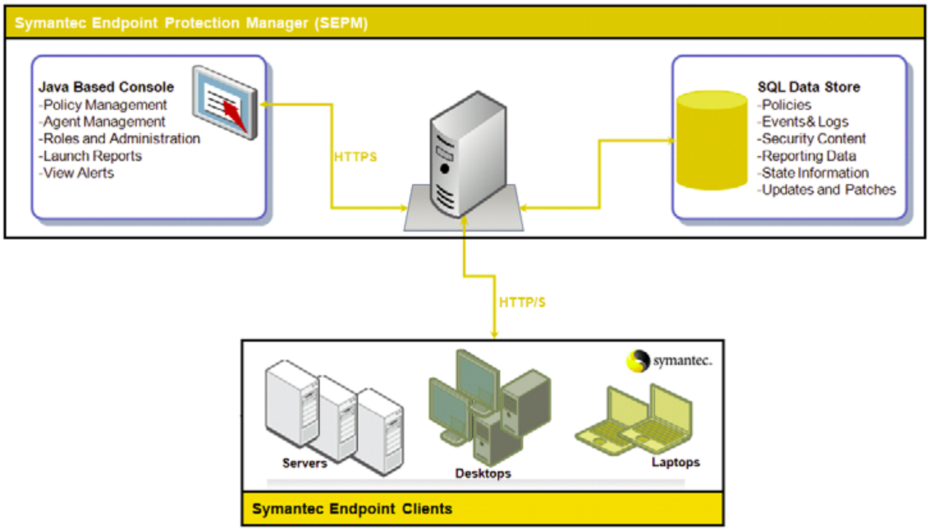
Effective and efficient endpoint security requires a balance of protection technologies, a manageable infrastructure, and adequate forensic data to properly monitor network security activities. Before the solution is deployed, several decisions need to be made about the best ways to configure the Symantec Endpoint Protection components for your particular environment.

Architecture

Symantec Endpoint Protection contains four main architectural components that work together to protect your company from security threats:

- Symantec Endpoint Protection Manager ("SEPM" or "manager")– The management server that is used to configure clients, reports, and alerts.
- Symantec Endpoint Protection SQL Data Store ("database") – The database that stores all configuration, updates, and reporting information.
- Symantec Endpoint Protection Client ("client")— Software that is deployed to networked computers. The client is used to monitor policies and automate policy compliance activities.
- Symantec Protection Center (formerly, the Symantec Endpoint Protection console)— A lightweight user interface that is used to access the Symantec Endpoint Protection Manager. The Symantec Protection Center is used to manage and view deployment activity, configurations, updates, and Symantec Endpoint Protection client reports.

Basic Symantec Endpoint Protection Architecture

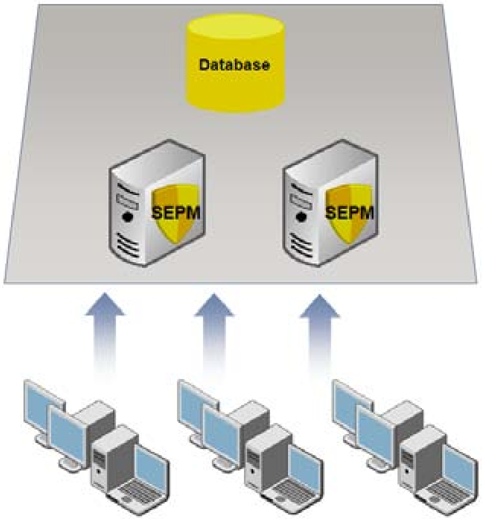


Site Design

A Symantec Endpoint Protection site design begins with the choice of the basic site architecture.

At the highest level, designs are divided between single-site designs and multiple-site designs.

Single-site design



An organization with one datacenter can generally use a single-site design with the following attributes:

- Two Symantec Endpoint Protection Managers (for redundancy and load balancing)
- Database clustering (to support high availability)

Multiple-site design

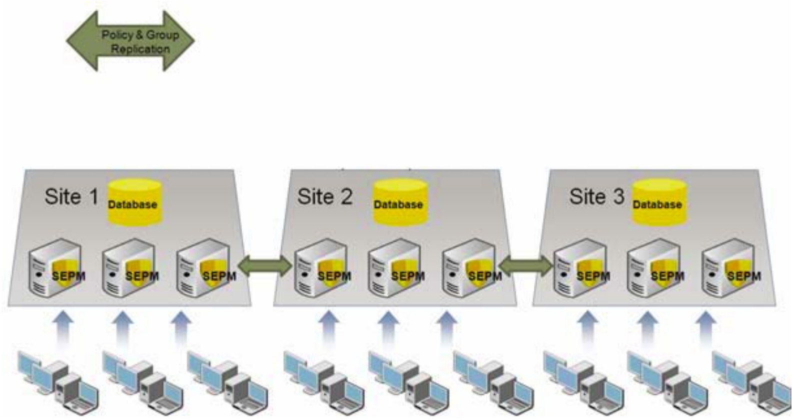
An organization with more than one datacenter or with multiple large physical locations should use a multiple-site design. There are three primary designs for a multiple-site environment:

- Distributed
- Central Logging
- High Availability

Distributed

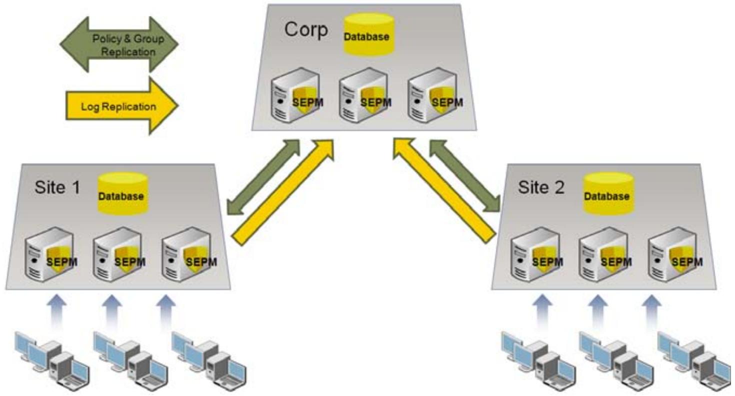
The Distributed design is recommended when immediate access to remote site data is not critical. This design has the following attributes:

- Each site performs bi-directional replication of Groups and Policies.
- Logs and content are not replicated by default.
- To view the site reports, administrators use the console to connect to the Symantec Endpoint Protection Manager at each remote site.



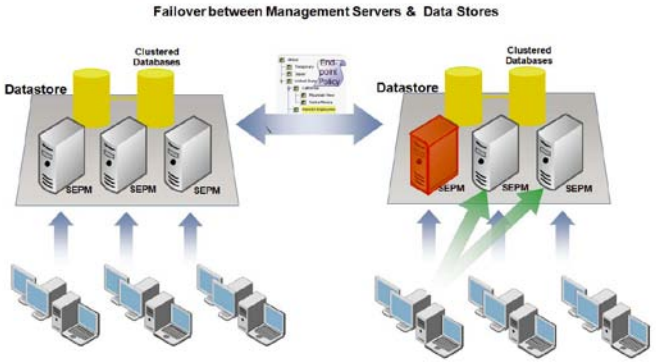
Central Logging

The Central Logging design is recommended when centralized reporting is required. The principal feature of this design is log forwarding to a centralized repository. In the following example, the Corporate Headquarters site is the central repository for logs forwarded from Corporate Sites 1 and 2.



High Availability

High Availability (HA) designs take advantage of multiple Symantec Endpoint Protection Manager installations and multiple, clustered databases to provide redundancy, failover, and disaster recovery. Several options are available to optimize performance, fail-over, and recovery. For instance, the HA design can be configured to have client computers automatically switch to an alternate Symantec Endpoint Protection Manager server should the primary server become unavailable.



Determining Client-to-server Ratios

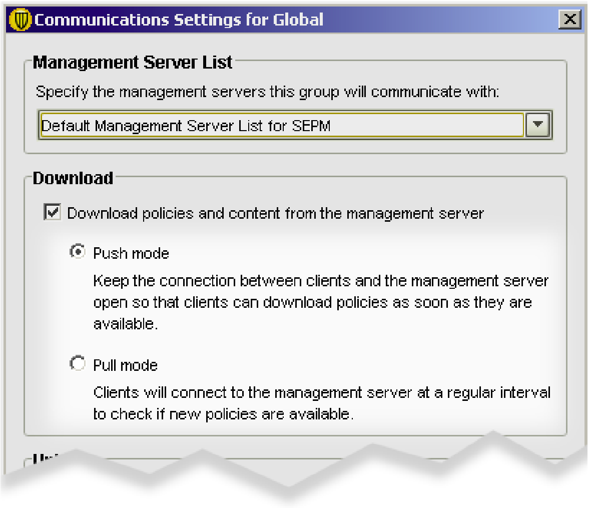
Deploying Symantec Endpoint Protection with the proper client-to-server ratio is crucial to providing a high performance endpoint security environment. Chief among the parameters that affect the client-to-server ratio are client-server communication, desired update speeds, and the security technologies deployed in the network environment.

Client-Server Communication

Symantec Endpoint Protection clients and managers exchange status information and content data. Clients initiate this communication with the Symantec Endpoint Protection Manager from an ephemeral port to the Symantec Endpoint Protection Manager server on TCP port 8014 (or 443 if using SSL). In the event of a conflict, this port is configurable. The frequency of communication depends on the heartbeat (also called "polling interval") and communication configuration.

When there are no new client-side logs to upload to the management server, or policy or content to download from the server, the size of the Symantec Endpoint Protection client heartbeat is between 3KB and 5KB. When all client protection technologies are enabled and the maximum level of client logging is enabled (with the exception of packet-level firewall logging, which is not recommended in production environments), the size of a typical heartbeat is between 200 KB and 300 KB.

Symantec Endpoint Protection clients can be configured to communicate with the Symantec Endpoint Manager using either push mode or pull mode. For best performance, keep the Symantec Endpoint Protection database close to the Symantec Endpoint Protection Manager server, and use pull mode.



Communications Settings for Global

Management Server List

Specify the management servers this group will communicate with:

Default Management Server List for SEPM

Download

☑ Download policies and content from the management server

● Push mode

Keep the connection between clients and the management server open so that clients can download policies as soon as they are available.

○ Pull mode

Clients will connect to the management server at a regular interval to check if new policies are available.

Communication modes

Each communication mode has advantages and disadvantages that need to be assessed for each environment.

Pull mode

In pull mode, the client connects to the manager according to the heartbeat frequency. This procedure repeats indefinitely. The number of clients that can be supported in pull mode depend on the following conditions:

- Server performance
- Network bandwidth used for clients
- Server communication
- Heartbeat (polling) frequency

In general, the less frequent the heartbeat, the more clients a server can support. There is no maximum number of clients that can connect to a particular Management Server.

Push mode

In push mode, the client establishes a persistent TCP connection to the server. If a client cannot connect to the management server, it retries periodically, depending on the heartbeat frequency. The following conditions apply to push-mode communication:

- The server notifies the client whenever the server changes status

- Logs are sent from the client to the Symantec Endpoint Protection Manager server at the heartbeat interval
- Push mode is more resource intensive than pull mode because of the persistent TCP connection

In push mode, the theoretical maximum ratio of clients to Symantec Endpoint Protection Manager servers is 50,000:1. However, Symantec generally recommends a maximum ratio of 5000:1 for push mode communication.

Heartbeat Interval

The performance figures provided in tables 1-5 are based on testing performed in a controlled environment using servers with the following specifications and configured as a single site. All times are measured in minutes.

Symantec Endpoint Protection Server

- CPU: Intel® Core™2 Duo E6600 , 2.40 GHz
- Physical Memory (RAM): 4 GB
- Operating System: Microsoft Windows Server® 2008, 64-bit.

Microsoft SQL Server

- CPU: Intel® Xeon® E5420 2.5 GHz (see below for CPU core performance)
- Physical Memory (RAM): 64GB
- Operating System: Microsoft Windows Server® 2008, 64-bit
- Database Software: Microsoft SQL Server® 2008

Table 1- 5000 Clients

SQL Server CPU	1 Symantec Endpoint Protection Manager	2 Symantec Endpoint Protection Managers
Single Core	50	30
Dual core	20	15
Quad core	15	10
2x Quad core	10	10

Table 2- 15,000 Clients

SQL Server CPU	1 Symantec Endpoint Protection Manager	2 Symantec Endpoint Protection Managers	3 Symantec Endpoint Protection Managers
Dual core	50	35	25
Quad core	20	15	10
2x Quad core	20	10	10

Table 3- 25,000 Clients

SQL Server CPU	1 Symantec Endpoint Protection Manager	2 Symantec Endpoint Protection Managers	3 Symantec Endpoint Protection Managers	4 Symantec Endpoint Protection Managers	5 Symantec Endpoint Protection Managers
Dual core	85	55	45	35	30
Quad core	30	20	20	15	10
2x Quad core	30	20	15	10	10

Table 4- 50,000 Clients

SQL Server CPU	2 Symantec Endpoint Protection Managers	3 Symantec Endpoint Protection Managers	4 Symantec Endpoint Protection Managers	5 Symantec Endpoint Protection Managers
Dual core	80	65	50	40
Quad core	30	25	20	15
2x Quad core	25	20	15	10

Table 5- 100, 000 Clients

SQL Server CPU	2 Symantec Endpoint Protection Managers	3 Symantec Endpoint Protection Managers	4 Symantec Endpoint Protection Managers	5 Symantec Endpoint Protection Managers
Quad core	50	40	35	30
2x Quad core	40	35	30	20

Note: The heartbeat intervals listed in the preceding tables do not include the performance overhead introduced by actions such as site-to-site database replication or reporting activity. Other factors such as lower hardware specifications, available network bandwidth, or network congestion can adversely affect performance numbers and will require increasing the heartbeat intervals to achieve the desired performance in your environment. Test data provided in this document is based on performance in a physical environment. Do to the nature of resource allocation in a virtual environment you should added 25-30% more time to your calculation of the heartbeat interval setting.

Heartbeat Sizing Example

The following examples assume the Symantec Endpoint Protection Manager specifications shown on page 11:

Number of total Clients	Number of Symantec Endpoint Protection Managers	SQL Server CPU	Shortest recommended heartbeat interval
50,000	2 (25,000 Clients per manager)	Dual core (2 CPU)	80 minutes
50,000	2 (25,000 Clients per manager)	Quad core (4 CPU)	30 minutes

Calculating Content Distribution Time

A key metric for provisioning a Symantec Endpoint Protection environment is the time it takes to distribute content updates to an organization. Content updates can include:

- Antivirus definitions
- Intrusion Prevention signatures
- Symantec Endpoint Protection engines updates

Content updates vary in size and frequency depending upon content types and content update availability. The time required to perform a content distribution update in a best-case scenario can be calculated with the following formula:

Concurrent Connections X Average Content Size ÷ Available Bandwidth = Content Distribution Time, where Average Content Size = 70-100KB*

*Note that latency is also affected by network utilization and protocol overhead

Example Content Distribution Time using 70KB update

The example assumes the use of the entire bandwidth

Bandwidth	Number of Clients	Time
T1 (1.54 Mbps)	• 5000 • 15,000	• 30 Minutes • 2 Hours
10 Mbps	• 5000 • 15,000	• 4 Minutes • 14 Minutes
100 Mbps	• 5000 • 15,000	• 30 Seconds • 2 Minutes
1 Gbps	• 5000 • 15,000	• 3 Seconds • 9 Seconds

To decrease the time required to distribute content distribution updates, do one or more of the following:

- Distribute the client load across multiple managers
- Deploy Group Update Providers
- Use alternative methods to distribute the content such as LiveUpdate Servers or third-party distribution tools

About Group Update Providers

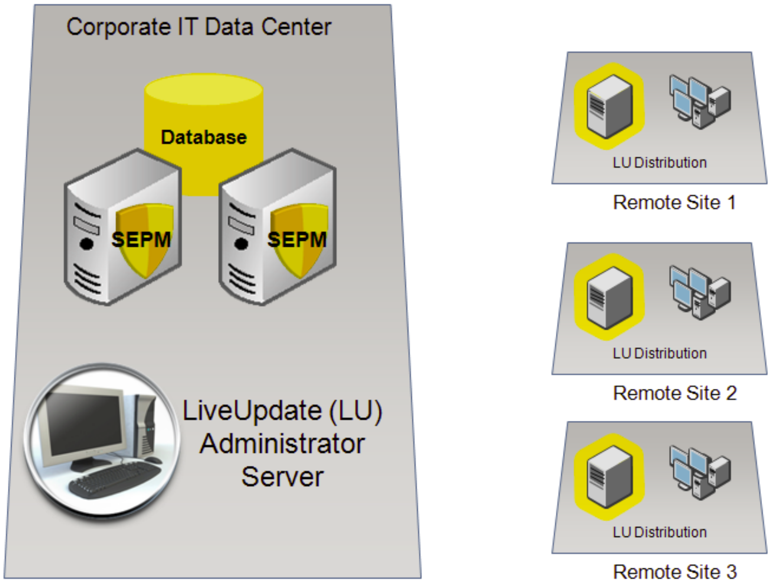
The Group Update Provider (GUP) provides updates to clients belonging to a Group, and any subgroups that are configured to inherit Group policies as set on the Clients tab. If there is a concern of multiple updates occurring across a given connection, then Administrators should consider deploying a GUP. With the release of Symantec Endpoint Protection MR3, the GUP can support up to 10,000 clients. The performance of the GUP is dictated by the throughput of the hardware for the system that is designated as a GUP. Typically, a client configured as a GUP will require an additional 50MB of disk space to store content updates. This number can vary depending upon the age of the clients connecting for updates, and the size of the delta created to update them.

If you need to deploy updates to more than 10,000 nodes, Symantec recommends you consider an alternative update method, such as:

- Additional GUPs
- Additional Symantec Endpoint Protection Managers
- A Symantec LiveUpdate Server

About LiveUpdate Servers

Environments that provide content updates to more than 10,000 nodes, but cannot provide an additional Symantec Endpoint Protection Manager or additional GUPs can use a Symantec LiveUpdate Server. The following graphic depicts an architecture design that uses a LiveUpdate Server to provide content updates:



This design features a LiveUpdate Server at the Corporate Site (HQ) which redistributes content to LiveUpdate Servers at each remote site. LiveUpdate distribution servers act as simple re-distribution points and use HTTP, FTP, or Network Shares to distribute content updates. LiveUpdate Distribution Servers add very little overhead to an existing server, and so have negligible impact on server resources. For a complete list of hardware and software requirements for the Symantec Endpoint Protection components, see the *Installation Guide for Symantec Endpoint Protection and Network Access Control*.

Application learning and impact to the database

Application Learning allows Symantec Endpoint Protection (SEP) clients to report information and statistics about the executables that are run on them. This information is provided to the Symantec Endpoint Protection Manager (SEPM) and aggregated into the SEPM database. The purpose of this information is to build a list of known applications in an environment to create Application-based firewall rules, Host Integrity (HI) rules and can be used as a reference for developing Application Control rules and Centralized Exceptions.

If left to run indefinitely, the database can grow considerably and eventually slow processing or cause other database problems. For this reason, it is strongly recommended for systems using the embedded database, that application learning is turned off.

For more information, see the Symantec Technical Support knowledge base article, **“Best Practices Guide to Application Learning in Symantec Endpoint Protection Manager”**

Symantec Endpoint Protection Manager Server and Database Sizing

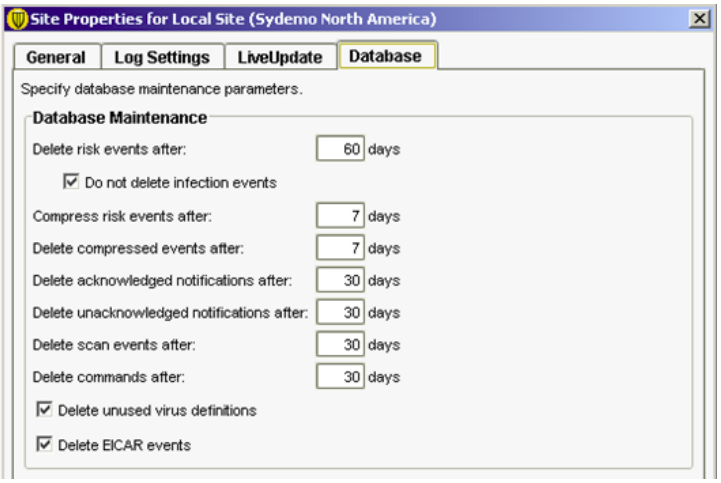
Several factors influence the size of the Symantec Endpoint Protection database and the storage space required on a Symantec Endpoint Protection Manager server. These factors include the following variables:

- Database maintenance settings
- Log size and expiration timeframes
- Content update sizes
- Client installation package sizes
- Backup information requirements

Database maintenance settings

Administrators can configure database maintenance options for the data that are stored in the database. Database maintenance options help you to manage the size of your database by specifying compression settings and how long to keep data.

Scheduled deletion of events ensures log entries are deleted regularly to prevent your database from growing too large. Event compression consolidates multiple "risk-found" events into a single security event. Over time, and especially during a security event, event compression can help keep the database size within manageable limits.



Specify database maintenance parameters.

Database Maintenance

Delete risk events after: 60 days

☑ Do not delete infection events

Compress risk events after: 7 days

Delete compressed events after: 7 days

Delete acknowledged notifications after: 30 days

Delete unacknowledged notifications after: 30 days

Delete scan events after: 30 days

Delete commands after: 30 days

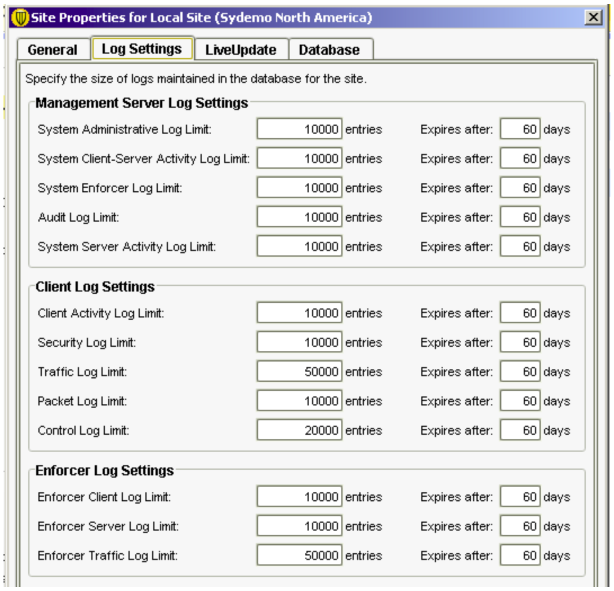
☑ Delete unused virus definitions

☑ Delete EICAR events

Logging options

Logging options are configured by the Administrator to optimize storage requirements and comply with company policies that control retention of logged data. The following parameters are commonly used to control logging activity:

- Maximum number of entries stored in the logs
- Length of time (days) to store log entries



Specify the size of logs maintained in the database for the site.

Management Server Log Settings

System Administrative Log Limit:	10000 entries	Expires after:	60	days
System Client-Server Activity Log Limit:	10000 entries	Expires after:	60	days
System Enforcer Log Limit:	10000 entries	Expires after:	60	days
Audit Log Limit:	10000 entries	Expires after:	60	days
System Server Activity Log Limit:	10000 entries	Expires after:	60	days

Client Log Settings

Client Activity Log Limit:	10000 entries	Expires after:	60	days
Security Log Limit:	10000 entries	Expires after:	60	days
Traffic Log Limit:	50000 entries	Expires after:	60	days
Packet Log Limit:	10000 entries	Expires after:	60	days
Control Log Limit:	20000 entries	Expires after:	60	days

Enforcer Log Settings

Enforcer Client Log Limit:	10000 entries	Expires after:	60	days
Enforcer Server Log Limit:	10000 entries	Expires after:	60	days
Enforcer Traffic Log Limit:	50000 entries	Expires after:	60	days

Log Size Examples

The following examples illustrate the key factors affecting log size and storage requirements:

Log data sizes

Log	Size per 10,000 log entries (MB)
System Admin	10
System Client Server Activity	9
System Enforcer	6
Audit Log	6
System Server Activity	66

Log	Size per 10,000 log entries (MB)
Client Activity	45
Security Log	45
Traffic Log	45
Packet	45
Control	45
Enforcer Client	16
Enforcer Server	14
Enforcer Traffic	9

Approximate detected/quarantined virus event sizes

Number of viruses in database	Approximate space (MB)
1,000	0.8
5,000	4.3
15,000	12.9
25,000	21.6
50,000	43.2

The average database requirements for a 17,000 node deployment is roughly 15,000 detected and quarantined virus events every 60 days.

Example of log data statistics for a 17,000 node environment*

Log	Avg. events per log
System Admin	10 events per day per admin
System Client Server Activity	9 events per day per machine
Audit Log	Usually very small
System Server Activity	650 events per server per day
Client Activity	120 events per machine per day
Security Log	1 event per day per machine

Log	Avg. events per log
Traffic Log	2400 events per machine per day
Packet	Could be extremely large depending on policies
Control	Could be extremely large depending on policies
Viruses	250 per month per 1000 Clients

*Log Metric Data will vary from customer to customer

Symantec Endpoint Protection Manager Hardware Recommendations

Hardware requirements vary depending on the number of clients served by the Symantec Endpoint Protection Manager. Symantec makes the following recommendations for Symantec Endpoint Protection Manager hardware:

Symantec Endpoint Protection Managers serving less than 10,000 clients:

- 2GB RAM minimum
- Single Processor

Symantec Endpoint Protection Managers serving more than 10,000 clients:

- 4GB RAM minimum
- Dual Processor

Database recommendations

For installations with a client-to-server ratio of 5,000 clients or less, using the default log settings, Symantec recommends using the embedded Sybase database. For installations with a client-to-server ratio greater than 5,000 clients, or using a higher level of log settings, Symantec recommends using a separate Microsoft SQL database. For SQL database sizing, Symantec recommends using the database vendor's recommended sizing tools or guides.

Database performance enhancement recommendations

For added performance, Symantec recommends the following options:

- Use Microsoft Windows Server 2003 or 2008 64-bit operating system
- Microsoft SQL Server 2005 64-bit

- High-throughput hard drives with 10,000 RPM or higher drive speed.
- Install the different Symantec Endpoint Protection components (manager software, IIS server, and database) on different disk drives
- Use a SAN environment with a management product such as Symantec Storage Foundation

Additional optimization can be obtained for disk I/O performance on the Symantec Endpoint Protection Manager.

Database backups

Database backups create a copy of the database. In the event that data corruption or hardware failure occur, the Administrator can revert to a previous copy of a backup to restore lost data. A database backup is created using the Symantec Endpoint Protection Manager console or by using the Symantec Database Backup and Restore utility. The Symantec Database Backup and Restore utility is automatically installed during the installation of the Symantec Endpoint Protection Manager server. For more information, see the *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

Recommended SQL database maintenance

If you use a Microsoft SQL database, Symantec recommends that you periodically defragment and reindex the database. Reindexing can improve performance and ensure an optimal database structure, particularly in large environments. Reindexing and defragmenting should be included as part of the regular database maintenance plan that is described in the Symantec Support Knowledge Base article, *Create database maintenance plans in MS SQL Server 2005 using SQL Server Integration Services (SSIS)*

Recommended backup plans

Symantec recommends the following backup plans:

- Microsoft SQL database only: Use the Microsoft SQL Server Enterprise Manager to set up a maintenance plan that includes automatic backups.
- Embedded or an MS SQL database: Use the Symantec Endpoint Protection Manager console to perform on-demand backups and also schedule automatic backups.

Create backups regularly and store them on a separate disk drive, preferably at a secure off-site facility.

Backup storage requirement calculation

The size and number of retained backups impact the required disk space on the Symantec Endpoint Protection Manager server. The backup size is approximately 75% of the database size, multiplied by the number of copies being retained. For instance, 1GB database X 0.75 X 3 Copies = 2.3 GB of disc space.

Impact of Content Updates and Installation packages

Client update packages, patches, and content updates are also stored in the Symantec Endpoint Protection database and affect the storage requirements. Product updates and patches contain information for client packages and information for each language or locale. Note that patches also create new, full client builds. Full client builds are approximately 120 MB.

Content updates require approximately 300MB each. These updates contain information for the following technologies:

- Definitions and Eraser
- Intrusion Prevention Signatures
- Proactive Threat Scan Engine
- Proactive Threat Scan White Lists
- Decomposer

Calculating Total Disk Space Requirements

The following example scenario shows the space required for a Symantec Endpoint Protection implementation with 17,000 nodes. This example assumes the following metrics:

- An average 15,000 viruses over 60 days
- Retain 20,000 Events for each Log
- Retain five versions of each Symantec Endpoint Protection client (32/64 Bit, English and French language)
- Retain seven backups

Item	Space required (MB)
15,000 viruses detected/quarantined	12.9
20,000 events per log	722
20 Client versions	2400
Content updates	300

TOTAL Database Size = 4.80 GB*

*The database size of 3.43 GB must be multiplied by 1.4 to account for the overhead of indexes and other tables in the database.

The space required on the Symantec Endpoint Manager server to store seven backups is approximately 33.6 GB.

A key component of the Symantec Endpoint Protection Manager server is the Internet Information Server (IIS). IIS content requires approximately 4GB.

Symantec Network Access Control Enforcer Appliance Throughput

When the Symantec Network Access Control Enforcer Appliance is part of the security environment, use the following values to determine throughput rates:

- Gateway Enforcer: 25,000 concurrent sessions (1 Gbps throughput)
- DHCP Enforcer: 50,000 concurrent sessions
- LAN Enforcer: 10,000 concurrent sessions

Preventing and Correcting False-Positive Detections with Symantec Endpoint Protection 12.x

Security technology has always had the potential of identifying a good file as bad. Symantec works hard to balance this risk of a false positive versus the need for aggressive detection. Symantec Endpoint Protection 12.1 adds many features to reduce the risk of a false-positive detections (FPD). Among these are new security technologies that require some machine-learning to avoid false positives. As a result, during the initial testing and implementation of Symantec Endpoint Protection 12.1, some customers may initially see higher rates of FPD.

However, any disruption to the organization due to FPD can be avoided with some simple precautions. Additionally, improvements to the false positive workflow enable a false positive to be corrected quickly and with minimum disruption.

Symantec Insight technology uses file reputation data to recognize and block malicous code from running on protected computers. The following table describes the three bands of threshold sensitivity associated with Insight and the use-cases appropriate for each..

Range	Description
1-3	Appropriate for scenarios or for test environments that cannot tolerate false positive detections or the conviction of good files that are still building reputation. At these levels, malware that is still building reputation may evade detection, but the system is very unlikely to convict good files.
4-6	Appropriate for most desktop users running normal software. These bands balance false-positive (FP) risk and detection to capture most malware with low FPs. Based on Symantec's experience and understanding of the threat landscape, Level 5 is the appropriate threshold for the majority of the users. Symantec discourages users from changing the value unless advised by Symantec Technical Support personnel.
7-9	Appropriate for highly secure environments where you wish to "lock-down" a server or desktop that does not frequently install new or unproven software. False-positive detections will occur at this level, but very little malware will evade detection.

False Positive Prevention

Symantec Endpoint Protection 12.1 will not detect *known good files* as malware. There are several ways to make sure your good files are known as good. The following steps will help prevent false positives when installing Symantec Endpoint Protection 12.1.

Step 1 – Using Digital Signatures

One of the easiest ways to identify that a file is good is to know where it came from and who created it. One of the most important factors in building a positive file reputation is to check its digital signature. Executable files without a digital signature are at risk of being identified as unknown.

- *Custom or home grown application should be digitally signed with class three digital certificates*
- *Customers should insist that their software vendors digitally sign their application*

Step 2 - Add to the Symantec White List

Symantec has a growing white list of over 25 million good files. These files are used to test signatures before the signatures are released to the public. The hash values of these files are also stored in the cloud and are used as a real time check to avoid FPD on the Symantec Endpoint Protection client. White-listing files provides a powerful method to avoid FPD. Customers and vendors can add files to this list.

- Software vendors: Submit executables for inclusion to the Symantec white list: ***https://submit.symantec.com/whitelist/***
- BCS Customers: Submit system images to the Symantec white list: ***https://submit.symantec.com/whitelist/bcs.cgi***

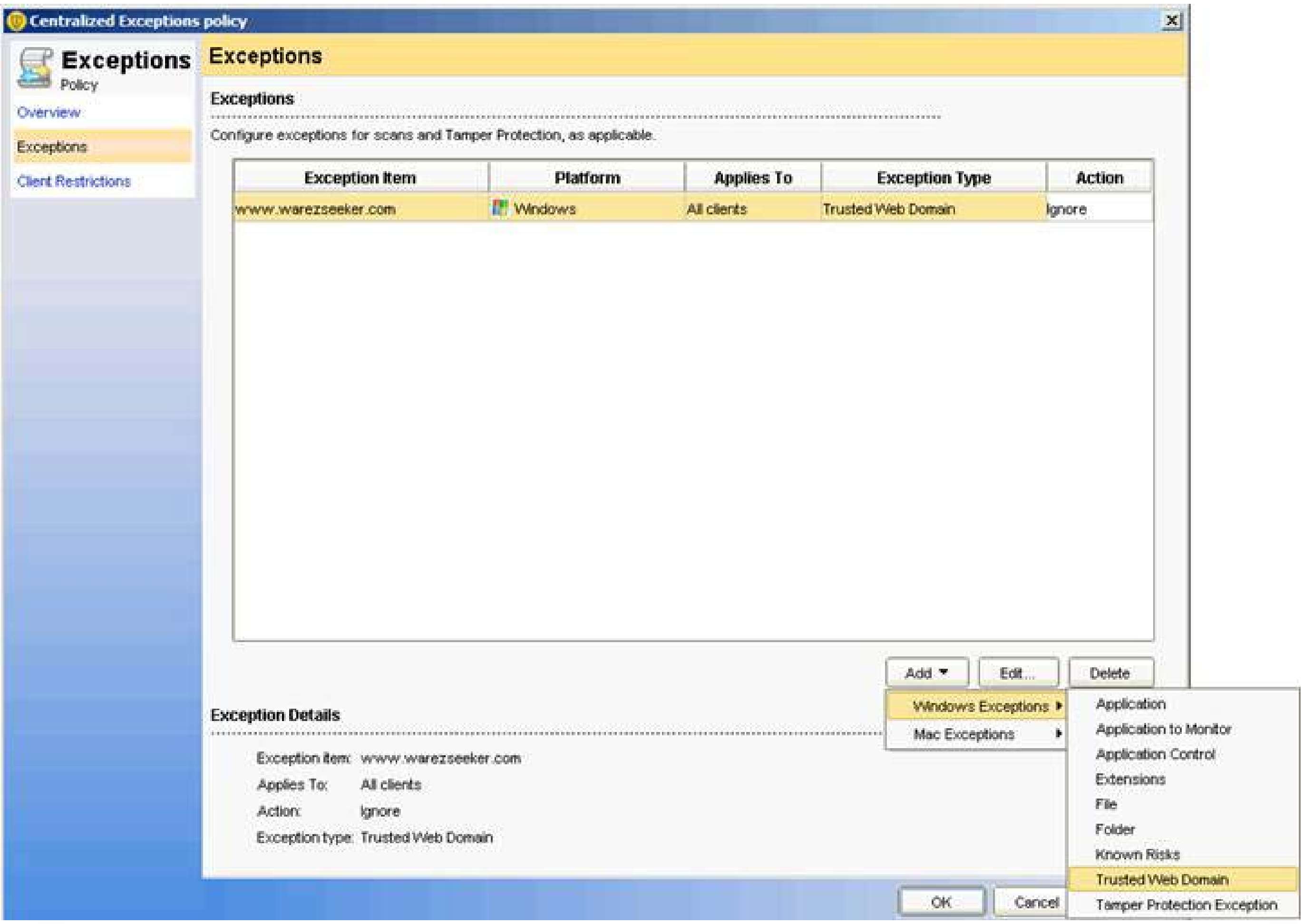
NOTES:

- Tools to help simplify the submission of files are available through the white listing program
- Do not use these web sites to correct a false positive. Instructions to correct a false positive are provided below.

Step 3 - Exclude

Symantec Endpoint Protection 12.1 provides multiple methods to exclude good files from detection. Exclusions can be added from within the Symantec Endpoint Protection Manager console to provide false-positive mitigation on the client.

- *Exclude your domain from Insight detections*



Exceptions

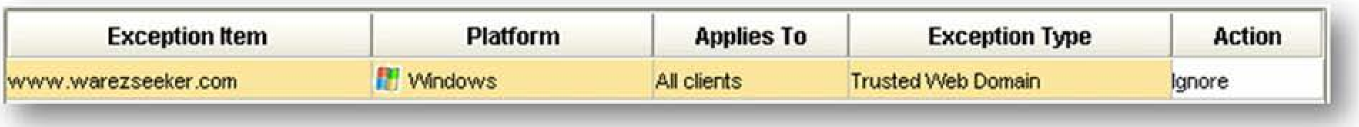
Exceptions

Configure exceptions for scans and Tamper Protection, as applicable.

Exception Item	Platform	Applies To	Exception Type	Action
www.warezseeker.com	Windows	All clients	Trusted Web Domain	Ignore

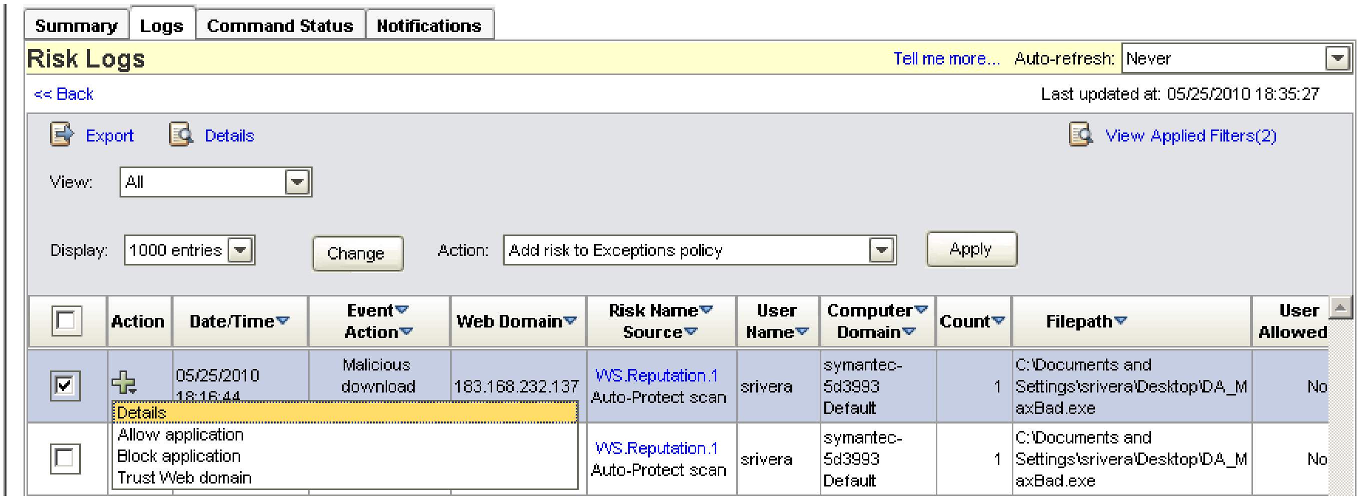
Exception Details

Exception item: www.warezseeker.com
Applies To: All clients
Action: Ignore
Exception type: Trusted Web Domain



Exception Item	Platform	Applies To	Exception Type	Action
www.warezseeker.com	Windows	All clients	Trusted Web Domain	Ignore

- *In the Symantec Endpoint Protection Manager, add exclusions or exceptions for critical files, directories, URLs, and IPs*



Risk Logs

Tell me more... Auto-refresh: Never

<< Back

Last updated at: 05/25/2010 18:35:27

View: All

Display: 1000 entries

Action: Add risk to Exceptions policy

☐	Action	Date/Time	Event Action	Web Domain	Risk Name Source	User Name	Computer Domain	Count	Filepath	User Allowed
☑	✚	05/25/2010 18:16:44	Malicious download	183.168.232.137	WS.Reputation.1 Auto-Protect scan	srivera	symantec-5d3993 Default	1	C:\Documents and Settings\srivera\Desktop\DA_MaxBad.exe	No
☐					WS.Reputation.1 Auto-Protect scan	srivera	symantec-5d3993 Default	1	C:\Documents and Settings\srivera\Desktop\DA_MaxBad.exe	No

A known-good application can appear in the Risk Logs as a false-positive. You can configure log settings to allow the application to be ignored, which prevents it from appearing in the Risk Log. This same functionality is also present in the SONAR Logs.

NOTES:

- You can select more than one application, file, URL, or IP at a time.
- You can use **Trust Web domain** to add a Web Domain to the Exceptions policy.
- For more information, see the *Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide*.

Step 4 - Test

The initial deployment of Symantec Endpoint Protection 12.1 during testing should include test machines with representative images of the software you run in your environment, including common 3rd party applications

- *Monitor for potential issues during testing*

Step 5 - Feedback

Each security technology in Symantec Endpoint Protection 12.1 can collect and send file metadata to Symantec. These submissions are used to identify and mitigate false positives through forensic analysis, heuristic training against collected data sets, and custom and generic white-listing.

- *Enable automated submission of metadata on detections.*

Correcting a False-Positive Detection

During the testing, Symantec wants to know about false-positive detections on customer systems:

- To identify the causes of false-positive detections.
- To make adjustments to the detection subsystem that reduce the number of future false-positive detections.

Step 1 - Submit

False positives submissions can be made immediately to Symantec via a web form.

- *For SONAR, Reputation (Download Insight), CloudScan, Canary and any other suspected false positive detection, use:* ***https://submit.symantec.com/false_positive/***
  NOTE: It is critical for resolution of false positives that the SHA256 value of the file be included with the submission.[1]
- *During the beta-testing, for false positives caused by antivirus technologies, continue to make submission at* ***https://submit.symantec.com/websubmit/bcs.cgi***

Once the submission has been processed and the file is white-listed by Symantec, the quarantine rescan feature will automatically restore files detected as heuristic false-positives.

Step 2 - Exclude

Symantec Endpoint Protection 12.1 provides multiple methods to exclude good files from detection. Exclusions can be added from within the Symantec Endpoint Protection Manager console to provide false-positive mitigation on the client.

[1] The hash value of a file is presented in a notice on the client. Third-party tools are also available

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com