



Symantec Protection Suite 4.0

Enterprise Edition

Best Practices

Symantec Protection Suite 4.0

Enterprise Edition

Best Practices

Content

Introduction	6
Symantec Protection Suite Enterprise Edition.....	6
Architecture.....	12
Database Considerations for the Suite	14
Virtualization	14
Symantec Endpoint Protection	15
Components	15
Planning and Preparation	15
Symantec Endpoint Protection Management Server	16
Best Practices on a Windows Small Business Server	18
Symantec Endpoint Protection Client Best Practices	24
Virtualization Support	25
Where to get more information.....	26
Symantec Network Access Control Self-Enforcement	26
Components	26
Planning and Preparation	26
Performance	27
Installation	27
Where to get more information.....	27
Symantec Messaging Gateway	28

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Components	28
Planning and Preparation	29
Recommended Hardware Allocation.....	29
Spam Control and Mail Considerations	30
Configuration	31
Spam Policies.....	33
Using Both Messaging Gateway and SMS for Exchange	35
Where to get more information.....	36
Symantec Mail Security for Exchange	36
Components	36
Planning and Preparation	37
Symantec Mail Security for Microsoft Exchange Port requirements.....	39
Installation	40
Performance	41
Administration	41
Mail Security for Exchange and Symantec Endpoint Protection	41
Mail Security for Exchange on Microsoft Exchange 2007.....	41
Setting Exclusions for Microsoft Exchange 2010.....	42
Mail Security for Exchange on a Microsoft Small Business Server	43
Where to get more information.....	44

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Mail Security for Lotus Domino	44
Planning and Preparation	45
Deployment Best Practices	46
Configuration Best Practices.....	47
Recommended Maintenance.....	49
Where to get more information.....	49
Symantec Web Gateway.....	49
Components.....	50
Deployment Best Practices	50
Configuration Best Practices.....	56
Recommended Maintenance.....	61
Where to get more information.....	65
Symantec Workflow.....	65
Components.....	65
Deployment Best Practices	67
Where to get more information.....	68
Symantec System Recovery	68
Components.....	68
Performance	75
Best Practices before a backup.....	77

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Best Practices during a backup.....	78
Best Practices after a backup.....	78
Where to get more information.....	79
IT Analytics for Symantec Endpoint Protection	79
Reporting	80

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Introduction

Symantec Protection Suite Enterprise Edition

Symantec Protection Suite Enterprise Edition (SPS EE) includes comprehensive, powerful endpoint, messaging, and web protection for less money and provides security management, data protection and business continuity beyond basic security. SPS EE includes Endpoint Protection, Messaging Gateway, Mail Security for Exchange and Domino, Web Gateway and Symantec System Recovery to quickly get back up and running in case of disaster.

Symantec Endpoint Protection

Powered by *Insight*, Symantec Endpoint Protection (SEP) is the fastest, most powerful endpoint protection security solution money can buy. Symantec Endpoint Protection provides state-of-the-art defense against all types of attacks for both physical and virtual systems. Seamlessly integrating the essential security tools you need into a single, high performance agent with a single management console, Symantec Endpoint Protection provides leading protection without slowing you down.

What is Symantec Insight?

Insight detects new and unknown threats that are missed by other approaches. Black-listing and white-listing only work when there are thousands of copies of a known file. But the majority of malware today mutates to hide from black lists and white lists. Insight correlates tens of billions of linkages between users, files, and websites to identify rapidly mutating threats that may only exist on a few systems. Insight reduces scan overhead by as much as 70% by scanning only files at risk and can't be evaded or coded around by self-mutating and encrypting malware.

What's New in SEP 12.1

- **Insight** - Insight separates files potentially at risk from those that are safe, for faster and more accurate malware detection.
- **Real Time SONAR 3** - Replacing Symantec's TruScan technology, this version of SONAR examines programs as they run, identifying and stopping malicious behavior even of new and previously unknown threats.
- **Browser Intrusion Prevention** - Scans for attacks directed at browser vulnerabilities.
- **Antivirus for Macintosh and Linux**

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- **Faster central console** - Optimized database to increase responsiveness.
- **Smart Scheduler** - Stays out of your way by performing non-critical security tasks when your computer is idle.
- **Enhanced client deployment** - Improved wizards and more deployment options will allow new installs and upgrades to be faster and easier than ever before.
- **Built for Virtual Environments** - Enhanced to help protect your virtual infrastructure. SEP can white list baseline images, maintain a local virtual Insight cache, randomize scans and updates, and automatically identify and manage virtual clients.
- **Faster central console** - Optimized database to increase responsiveness.

Symantec Endpoint Protection for Macintosh

Symantec Endpoint Protection for Macintosh (SEP for MAC) provides a Macintosh antivirus client that can be managed by a Windows SEPM. From within the SEPM, Macintosh clients can be sorted into groups to centrally manage antivirus and antispyware policies and exceptions as well as configuring LiveUpdate policies. Administrators can run commands on remote systems to reduce administrative overhead in smaller environments.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Messaging Gateway

Symantec Messaging Gateway (SMG) powered by *Brightmail*, delivers inbound and outbound messaging security, with effective and accurate real-time antispam and antivirus protection, advanced content filtering, data loss prevention, and email encryption. Messaging Gateway is simple to administer and catches more than 99% of spam with less than one in a million false positives. SMG leverages real-time automatic antispam and antivirus updates from the Symantec Global Intelligence Network, on-box connection throttling using both global and self-learning local IP reputation, and comprehensive reporting, allowing administrators to focus on the overall security posture of the organization, while effectively reporting status to key executives and management.

What's New in SMG 9.5

- **Unified Management** - Integration with Symantec Protection Center allows for single sign-on and data integration for better security management and visibility across security technologies.
- **Virtualization** - SMG Virtual Edition is certified for deployment on VMware environments, with ESX and ESXi targeted for production deployment.
- **Enhanced Data Loss Prevention Integration** – SMG with DLP protects confidential data across endpoint, network, and storage systems.
- **New Dispositions** - Three new dispositions for newsletters, marketing mail and suspicious URLs allows you to go beyond traditional spam dispositions.
- **Improved Antispam Scanning** - SMG leverages a number of reputation-based techniques to more efficiently and effectively deal with spam attacks.

Symantec Mail Security for Microsoft Exchange

Symantec Mail Security for Microsoft Exchange (SMS MSE) provides real-time protection for email against viruses, spam, spyware, phishing, and other attacks while enforcing content policies on Microsoft Exchange Server 2003, 2007 and 2010. It supports 64 bit Windows and Virtualized Exchange server environment with easy installation and simple administration.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Premium Anti-Spam

Powered by Brightmail technology, the Symantec Premium Antispam (SPA) add-on subscription stops 99 percent of spam while making less than 1 mistake per million messages.

Symantec Web Gateway

Symantec Web Gateway (SWG) protects organizations against multiple types of Web-borne malware, prevents data loss over Web and gives organizations the flexibility of deploying it as either a virtual appliance or on physical hardware. Powered by the Insight, Symantec's innovative reputation technology, Web Gateway relies on a global network of over 175 million of users to identify new threats before they cause disruption in organizations.

What's New in SWG 5.0

- **Insight** - Powered by Symantec Insight providing proactive protection against new, targeted, or mutating threats
- **Integration with Symantec Data Loss Prevention** - allows for a robust Web and Data Loss prevention solution from a single vendor
- **SSL decryption capabilities**
- **Multiple deployment options** - deploy Web Gateway as a physical appliance, virtual appliance, or a combination of both
- **Proxy and caching capabilities** - For customers who require proxy in network topology, require an HTTP Cache for bandwidth savings, want to decrypt SSL and/or integrate with Symantec Data Loss Prevention

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Workflow

Symantec Workflow gives administrators real power and enables their security and infrastructure solutions to integrate and work with corporate business practices. By offering a drag and drop interface, Workflow allows the Administrator to have multiple products interact with each other and provide meaningful information to administrators and managers to enable them to make informed decisions about the next stage in any process. If for instance, an endpoint detects a piece of malicious code or an attack, workflow can alert the administrator and then ask them what they would like to do – to remediate the issue. They may want to quarantine the machine, run a scan, make sure the definitions are up to date, strengthen the data leakage prevention policies in place on that machine and perhaps restrict access for the users account within Active Directory, so they no longer have access to sensitive information until the issue is resolved. By integrating and communicating with multiple Symantec and third party technologies, Workflow makes all this possible in a totally automated fashion.

Symantec System Recovery Desktop Edition

Symantec System Recovery (SSR) delivers fast and reliable system recovery to help minimize downtime and meet recovery time objectives with confidence. Quickly restore physical and virtual systems in minutes, even to bare metal, dissimilar hardware, remote locations, or virtual environments through Symantec's patented Restore Anyware technology.

Symantec System Recovery (formerly Backup Exec System Recovery) helps protect the organization proactively by capturing automated backups without disrupting productivity. Flexible recovery capabilities then allow the IT / Backup Administrator to recover what they need, when and where they need it.

What's New in SSR 2011

- **New platform and application support**
- **Recovery Disk Improvements** - SRD-enabled USB devices and firewall enhancements
- **Enhanced Customizable SRD Wizard** - Enhanced custom driver support and use ISO file as source for custom SRD
- **Management Solution Improvements** - Install to Windows Server 2008 64-bit servers and manage up to 2,500 clients from a single server

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

IT Analytics for Symantec Endpoint Protection

IT Analytics (ITA for SEP) allows customers to create their own reports and dashboards from Endpoint Protection data. By utilizing SQL Analysis services, IT Analytics enables high speed business analysis, reporting and trending of events across periods of time. In addition, key performance indicators allow customers to track how efficiently their environment is running and/or being managed.

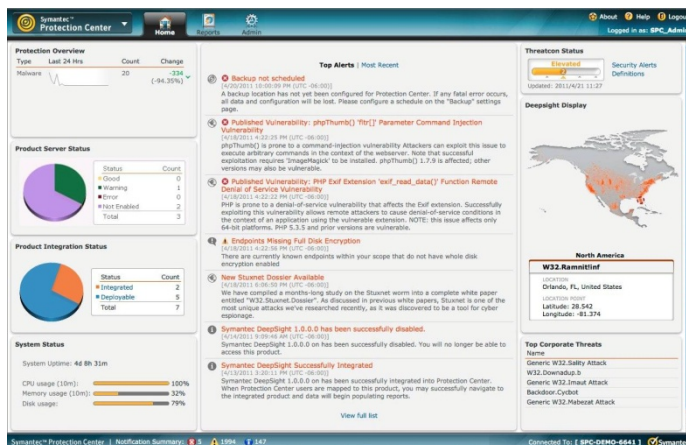
Symantec Protection Center

Symantec Protection Center is a centralized security management console that enables organizations to identify emerging threats, prioritize tasks, and accelerate time to protection based on relevant actionable intelligence. Through a combination of security intelligence and process automation, it enables users to take timely, targeted action to remediate incidents and proactively protect key systems and information assets. Unlike other solutions, Protection Center delivers context-aware security management by correlating data from enterprise security products along with early warning alerts the Symantec Global Intelligence Network, one of the world's leading commercial cyber-intelligence communities.

The initial shipping version Symantec Protection Center 2.0 will allow single sign on access to the majority of the products within the suite:

- Endpoint Protection
- Messaging Gateway
- Mail Security
- IT Analytics for Symantec Endpoint Protection

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices



Symantec Protection Center 2.0 Console

What's New in SPC 2.0

- **Product integration**- Single Sign on, data collection and action integration
- **Symantec GIN Integration** - Real time DeepSight data feeds from the Symantec Global Intelligence Network
- **Basic event correlation** - Provides collecting and normalizing data, and performing data mapping across multiple sources to create context around an event.
- **Cross Product Reporting**- Report across security solutions to track events involving malware, email and assets
- **Dashboard Notifications**- Role based prioritization list of security, infrastructure and global intelligence events
- **Prebuilt workflow templates** - Quarantine endpoint, move an asset to a different SEP policy group, update the malware definitions and run a system scan
- **Open API** - 3rd Party Integration

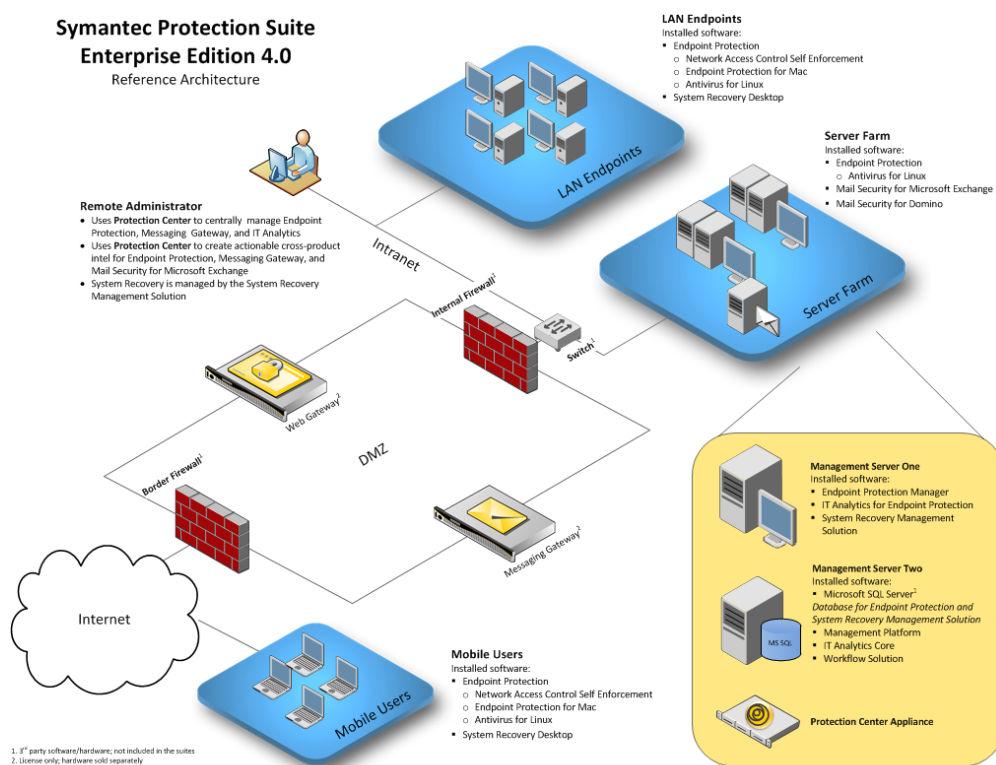
Architecture

The Symantec Protection Suite Enterprise Edition software and functionality are delivered based on the role of the security solution in the environment.

- Symantec Protection Center and IT Analytics for Symantec Endpoint Protection are included at no additional cost to improve time to protection by leveraging actionable, prioritized security information.
- Symantec Workflow can be used to automate security processes.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Symantec Mail Security is installed directly to a Microsoft Exchange Server and does not require any stand alone or additional hardware. Symantec Messaging Gateway Virtual Edition is deployed as a virtual guest on a VMWare server running vSphere 4 or ESX 3.5 (update 5) or later.
- The Symantec System Recovery Management Solution requires Microsoft SQL 2008 (or Express Edition) or later.



SPS 4.0 EE Reference Architecture

Server	Component Products
Server 1 (Management Server)	Symantec Endpoint Protection Manager (with optional embedded database)

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Server 2 (Management Server)	Symantec Management Platform System Recovery Management Server IT Analytics for SEP Workflow Server
Server 3 (Exchange/Domino/SQL Server)	Microsoft SQL Server <ul style="list-style-type: none"> • Required for use of IT Analytics with SEP • Required for SSR Management Server Microsoft Exchange/Domino SMS for Microsoft Exchange/Domino
Server 4 VMware Server	VMWare VSphere 4 or ESX 3.5 (update 4) or later Messaging Gateway Virtual Edition Web Security Virtual Edition
Security Management Server	Symantec Protection Center (Virtual or dedicated hardware)

Suggested server deployment for SPS EE

Database Considerations for the Suite

Typically, most customers wishing to use Symantec Endpoint Protection, Symantec System Recovery and IT Analytics for SEP will need to purchase and license Microsoft SQL Server. For very small deployments, SQL Express may work, but due to its limitations on table sizes it is not recommended.

Virtualization

Symantec supports running many of the components of Symantec Protection Suite Enterprise Edition in a virtual environment. Messaging Gateway, Web Security and Symantec Protection Center can be installed to run as virtual appliances. Symantec Endpoint Protection Manager and the System Recovery Management Solution can be installed and run virtually provided the operating system is supported and there are appropriate hardware resources. Symantec Endpoint Protection Clients can be run on virtual guest machines running on a single physical host. Due to the performance impact of database servers, Symantec doesn't recommend virtualizing the SQL database servers.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Endpoint Protection

Components

Symantec Endpoint Protection combines Symantec Antivirus with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops and servers. It seamlessly integrates essential security technologies in a single agent and management console, increasing protection and helping to lower total cost of ownership. It includes Antivirus and Antispyware, Firewall, Intrusion Prevention, Device and Application Control and can be integrated into a larger Network Access Control solution.

The core components required to run a centrally managed Symantec Endpoint Protection environment include:

- Symantec Endpoint Protection Manager
- Symantec Endpoint Protection Client (on each endpoint you wish to protect, including the manager)
- Database (by default, the embedded database is automatically installed and managed). The database stores all configuration, updates, and reporting information.
- Symantec Endpoint Protection Manager Console (can be run from anywhere with network access to the Manager)
- Symantec Protection Center (integrates management of multiple solutions into a single environment)

Planning and Preparation

- Test the deployment of the Symantec Endpoint Protection Manager and Client first in a non-production environment.
- As a precaution, ensure you have a complete backup of your existing server before deployment.
- Schedule to do the actual installation to your server at an off-peak time when there will be no users or applications interacting with the server.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Ensure you have registered your company with Symantec Technical Support and have information on how to contact them to log a support case, so you're prepared should you encounter issues.
- If another vendor's antivirus or firewall is currently running, this will need to be removed in advance of installing Symantec Endpoint Protection software.
- Ensure you are installing the most current version of Symantec Endpoint Protection as it usually contains significant improvements over previous releases.
- You must have administrator rights to the target computer or to the Windows domain to install client software on Windows computers.
- For Mac computers, you can use SEP Manager only to configure client install packages. Distribution of the packages must be done through other mechanisms.

Symantec Endpoint Protection Management Server

Performance

Resource utilization is the key consideration when deciding on an appropriate management server. It is strongly recommended to take some time to review the applications and services that will be running regularly on the target server and how much memory those processes consume before installing the Symantec Endpoint Protection Manager and Client. Below are guidelines on how much memory the Symantec Endpoint Protection components will require on average:

- Symantec Endpoint Protection Manager (including Database) – Approximately 150MBs
- Symantec Endpoint Protection Client – Between 25MBs (idle) and 50MBs (running LiveUpdate or a scheduled scan)
- Symantec Endpoint Protection Manager Console (when in use) – Approximately 80MBs

Note: The Console can be run from a remote machine by using a web browser to connect to port 9090 on the management server.

In general, the database interactions will be the most performance-intensive activities on the management server. If the management server is under-resourced, moving the database off to an existing Microsoft SQL server will reduce the performance impact of the Symantec Endpoint Protection Manager.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

While every environment varies, below are some high-level guidelines on recommended hardware that will help to ensure the server machine will run smoothly with Symantec Endpoint Protection. Please see the Getting Started Guide for supported operating systems and other detailed system requirements.

Recommended Hardware

Processor	Dual-Core/ Dual CPU
Memory	4GB RAM
Disk Space	4GB for the SEPM server, 4GB for the database For Windows Small Business Server 2008 allocate 60GB for the SEPM server For Windows Essential Business Server 2008 allocate 45GB for the SEPM server Note: At least 500MB of free space is required on the system drive (usually C:\) as temp space, even if not installing to this drive

Recommended Hardware

Installation and Deployment

There are several architectural options for deploying Symantec Endpoint Protection Manager.

- **Single Server** – a single server installation is suitable for most smaller customers and utilizes the Symantec Embedded database – this is suitable for up to 5000 clients (this configuration is the most commonly used configuration in small business environments)
- **Single Server with Microsoft SQL Database** – customers that require greater scalability can use an external SQL database, which can either be dedicated or shared between multiple services. Moving the database off to a server separate from the management server can provide substantial system performance improvements.
- **Multiple Servers** – customers who require multiple management servers for failover or load balancing of client communications can design and implement a multi-server architecture – note that this architecture requires MS SQL server. This configuration is not typically required for smaller environments as continuity of protection can be maintained through redundant content updating policies to ensure clients continue to receive updated security definitions even if the management server is temporarily unavailable.

Important Note: If a Symantec Antivirus primary/parent server version 10 or 9 is already running on the management server:

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Installing the Symantec Endpoint Protection Manager will NOT automatically replace/upgrade an existing Symantec Antivirus Server. They can run in parallel as part of a phased migration.
- Installing the Symantec Endpoint Protection client later on will replace an existing Symantec Antivirus Server.
- If you have a Symantec System Center and/or Reporting Server installed on the machine, they must be removed through Add/Remove Programs before continuing (no reboot required).

Required computer restarts when installing or migrating

In some case the computer on which you install SEP software must be restarted to complete the installation process.

- All computers that run a version of MSI prior to 3.1. Client installations upgrade MSI to 3.1. If this version does not run on client computers the upgrade requires a restart.
- SEP client installations that install Network Threat Protection and Firewall.
- Symantec Sygate Enterprise Protection Migrations.

Best Practices on a Windows Small Business Server

For full details please see the Best Practices document provided at the link in the “Where to get more information” section. Note, to date the content of this document has only been validated with the English version of both Windows Small Business Server and Symantec Endpoint Protection 11.0.

It is possible to run a Symantec Endpoint Protection Manager and Symantec Endpoint Protection client on the same machine as a Microsoft Windows Small Business Server. By default, there are no technical conflicts between the two - The key consideration is resource usage on the target machine, plus as a general best practice, good planning and preparation are also strongly recommended.

- Test the deployment of the Symantec Endpoint Protection Manager and Client first in a non-production environment.
- As a precaution, ensure you have a complete backup of your existing Microsoft Windows Small Business Server environment, and ensure the backup has been tested and confirmed to work.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Schedule to do the actual installation to your production Windows Small Business Server at an off-peak time when there will be no users or applications interacting with the server.
- Ensure you have registered your company with Symantec Technical Support and have information on how to contact them to log a support case, so you're prepared for the unlikely event that you encounter issues.
- If another vendor's antivirus or firewall product is currently running on the Windows Small Business Server, this will need to be removed in advance of installing the Symantec Endpoint Protection 11.0 software.
- Important! Ensure you are installing Symantec Endpoint Protection 11.0.6 or later, which contains a number of significant improvements since the previous releases. To download the latest available version, via a web browser, go to <https://fileconnect.symantec.com> and enter a valid serial key (which you received when you purchased the software).
- Schedule weekly automatic database backups to occur.

Symantec Endpoint Protection Client on a Windows Small Business Server

- The Antivirus Email Protection features are aimed at providing additional protection to client-side email applications such as Microsoft Outlook and Lotus Notes, therefore if you won't run these directly on the Small Business Server, these features should not be selected.
- If you are currently running the ISA 2004 firewall on the Microsoft Small Business Server, you should ensure the Network Threat Protection feature is not be selected.
- Installing the Symantec Endpoint Protection client will replace an existing Symantec Antivirus primary/parent server.
- Installation of the client will be blocked if a Symantec System Center is still installed on this machine.
- Ensure the Windows Firewall is not enabled on the network connections in Windows (Start > Settings > Network Connections), since the Symantec Endpoint Protection client firewall is now protecting these systems.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Endpoint Protection Client on the Management Server

Server-based operating systems should be configured differently than workstations. Within the Symantec Endpoint Protection Manager it is recommended to create a separate client group for servers that will allow you to assign custom installation packages and policies.

- The Antivirus Email Protection features are aimed at providing additional protection to client-side email applications such as Microsoft Outlook and Lotus Notes, therefore if you won't run these client applications directly on the server, these features should not be selected.
- If you are running a Microsoft Small Business Server as your management server with the ISA 2004 firewall enabled, you should ensure that the Network Threat Protection feature is not selected.

LiveUpdate and Content Revisions

Symantec releases fully certified definition signature updates 3 times a day. Due to the nature of the threat landscape a full signature is currently around 85MB and growing. Instead of downloading and distributing an 85MB package to all of its clients the management server creates delta signatures that only push new definitions to a client. The frequency of definition updates determines the size of these deltas. A client that is always connected to the management server and is receiving regular updates may get a delta package around 200 – 250KB. Clients that haven't checked in for a time will get larger delta packages.

Determining the number of content revisions to keep depends primarily on the amount of free storage space available to the management server and how frequently the endpoints check in to the management server. Larger numbers of content revisions require more disk space. If the Symantec Endpoint Protection Manager is only keeping content for 3 days (9 revisions) and an endpoint is offline for 4 days, the endpoint will need to download a full definition set, increasing the performance network bandwidth impact.

- Run LiveUpdate 3 times a day in order to get all of the content revisions available
- Set the number of content revisions to accommodate the normal length of time clients are expected to be offline. For example, if clients can be offline for 10 days due to vacations, travel or other downtimes, set the number of content revisions to 3x10 or 30 revisions.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Client Communication Settings

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.

By default the communication settings are set to Push. During the communications the management server provides content and policy updates to the client and the client uploads logs and status to the management server.

Communication modes

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

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

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.

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:

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

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

Group Update Providers

For remote sites (such as branch offices) that are connected via WAN links to the central site where the management server resides, consider using the Group Update Provider (GUP) feature to minimize the WAN link bandwidth used on a daily basis for SEP content distribution. A GUP is a client that has been designated the only system that will go out and retrieve definitions, either from the management server or a Symantec LiveUpdate server. That client will then distribute definitions to other clients on the subnet that have been configured to identify that client as the GUP.

Administration

Keep the number of console administrators, groups, locations and policies you create to a minimum. The less complexity there is, the easier the environment will be to manage and the more responsive it will be. Create new groups only when you require a specific set of machines to have non-standard policies.

If possible, leave inheritance enabled for the application of settings and policies across your groups, locations and SEP clients, then focus on making configuration changes at the “My Company” level, so they cascade down to other groups automatically.

Notifications and Reports

In order to enable notifications that will send email to specified administrators, enter the details for your mail server via the management console (Admin tab – Servers – Server Properties).

Create notifications (Monitors tab – Notifications) when the following conditions occur:

- Virus definitions out-of-date (more than 20% of your clients running old content)
- Risk outbreak – 10 occurrences on any or distinct computers
- Authentication Failure - multiple failed console logins

Create scheduled reports that will be automatically emailed to you on a weekly basis.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Computer Status - Virus Definition Distribution summary
- Risk - Comprehensive Risk Report

Disaster Recovery

Back up your database on a weekly basis and store the backups off site where they can be recovered if needed. Backups of the embedded database can be scheduled from the management console (Admin tab – Servers – {db name}). By default the database backup directory is located in the Symantec Endpoint Protection Manager\data\backup directory under Program Files.

Backup the keystore file and server.xml file located in the Server Private Key Backup directory under the Symantec Endpoint Protection Manager directory in Program Files. See the Installation Guide for Symantec Endpoint Protection and Symantec Access Control for full details on disaster recovery.

Replication

Do not utilize management server database replication unless you have been advised to do so by a Symantec representative. In general, replication is not required.

Symantec Endpoint Protection Client Best Practices

Lock down the managed SEP clients so they cannot be tampered with by the end users or by malware. This typically involves the following:

- Password-protect the ability to uninstall and stop the SEP client.
- Lock the end users ability to modify certain settings such as whether AutoProtect (real time AV/AS scanning) can be disabled or not.
- Enable the application control policy that enforces self-protection for the SEP client.
The simplest method for distributing malware is hidden inside files shared on peer-to-peer (P2P) networks. Create and enforce a no-P2P application control policy that includes home usage of a company machine.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Review your security content distribution schedule. Antivirus signatures are released multiple times a day and IPS content roughly on a weekly basis or as needed. If possible, take advantage of these updates or at least update machines that are frequently infected.

Virtualization Support

Shared Insight Cache tool

The Shared Insight Cache tool improves scan performance in virtualized environments by not scanning files that a Symantec Endpoint Protection client has determined are clean. When the client scans a file for threats and determines it is clean, the client submits information about the file to Shared Insight Cache. When any another client subsequently attempts to scan the same file, that client can query Shared Insight Cache to determine if the file is clean. If the file is clean, the client does not scan that particular file. If the file is not clean, the client scans the file for viruses and submits those results to Shared Insight Cache. Shared Insight Cache is a Web service that runs independently of the client. However, you must configure Symantec Endpoint Protection to specify the location of Shared Insight Cache so that your clients can communicate with it. Shared Insight Cache communicates with the clients through HTTP or HTTPS. The client's HTTP connection is maintained until the scan is finished.

Note: Shared Insight Cache is only available for the clients that perform scheduled scans and manual scans.

Virtual Image Exception tool

To increase performance and security in your virtual desktop infrastructure (VDI) environment, you can leverage base images to build virtual machines. The Symantec Virtual Image Exception tool lets your clients bypass scanning base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in your VDI environment.

NOTE: SYMANTEC ENDPOINT PROTECTION SUPPORTS THE VIRTUAL IMAGE EXCEPTION TOOL FOR MANAGED CLIENTS AND UNMANAGED CLIENTS.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Where to get more information

Resource	Location
SEP Knowledgebase	http://www.symantec.com/business/support/overview.jsp?pid=54619
Documentation	http://www.symantec.com/business/support/documentation.jsp?language=english&view=manuals&pid=54619
SEP Community	http://www.symantec.com/connect/security/forums/endpoint-protection-antivirus

Symantec Network Access Control Self-Enforcement

Components

Symantec Network Access Control Self-Enforcement provides additional capabilities that complement the Symantec Endpoint Protection solution and includes the following components:

- Symantec Network Access Control Manager
- Symantec Endpoint Protection Client
- Symantec Network Access Control Client (included in the SEP Client, no additional deployment necessary)
- Database (by default, the embedded database is automatically installed and managed)
- Symantec Enforcer (optional hardware appliance)
- Symantec Endpoint Protection Manager Console with Network Access Control Self-Enforcement (can be run from anywhere with network access to the Manager)
- Symantec Protection Center (web-based console integrates management of multiple solutions into a single environment)

Planning and Preparation

The Symantec Network Access Control Self-Enforcement management console installs into the Symantec Endpoint Protection management console so the SEPM should be deployed first. No additional system requirements or software dependencies are necessary for the implementation of SNAC Self-Enforcement. SNAC Self-Enforcement on the endpoint is managed by the SEP client.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Performance

Performance impact and system requirements are identical to those listed in the SEP Best Practices section.

Installation

- Install the Symantec Endpoint Protection Manager first
- Download and extract the “Symantec Network Access Control” DVD zip file to a temporary location on the local hard drive and run setup.exe. Choose “Install Symantec Network Access Control” and then click “Install Symantec Endpoint Protection Manager.
- Once the SNAC Manager has been installed you will see a new section under the “Policies” tab called “Host Integrity”. This is where SNAC Self-Enforcement policies will be created and assigned.

Use Host Integrity policies to make sure that the client computers that access your network meet your organization’s security policies. Use Host Integrity policies to ensure that client computers:

- Are running antivirus and antispyware applications. If they do not, allow them to remediate by downloading and installing the required applications.
- Have the latest virus definitions. If they do not, automatically download virus definition updates.
- Have the latest patches and service packs. If they do not, allow them to remediate by downloading and installing the required patch or service pack.
- Have backup software installed. If they do not, allow them to remediate by downloading and installing the required backup application.
- Have the software that lets you perform remote installations. If they do not, allow them to remediate by downloading and installing the required remote installation software.

Where to get more information

Resource	Location
Implementation Guide for SNAC	ftp://ftp.symantec.com/public/english_us_canada/products/symantec_network_access_control/12.1/manuals/rtm/Implementation_Guide_SEP12.1.pdf
Getting Started Guide	ftp://ftp.symantec.com/public/english_us_canada/products/symantec_network_access_control/12.1/manuals/rtm/Getting_Started_SNAC12.1.pdf
SNAC Community	http://www.symantec.com/connect/security/forums/network-access-control

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Messaging Gateway

Symantec Messaging Gateway Virtual Edition uses VMware products to create a simulated computer environment (a virtual machine) for its guest software. The guest software is a complete operating system that contains the Symantec Messaging Gateway Virtual Edition software. It runs in a similar manner to the application as installed on a stand-alone hardware platform.

Components

SBG Virtual appliances can be configured for two roles. During the initial command line setup, the installation wizard prompts the Administrator to choose the role that each appliance performs. Symantec recommends deciding which function or set of functions to assign to the appliance before installation.

Control Center

The Control Center is used to configure and manage Symantec Messaging Gateway from a Web-based interface. The Control Center provides information on the status of all of the Symantec Messaging Gateway hosts in the environment, including logs and reports. At least one Control Center must be configured for a deployment. One Control Center can control one or more Scanners. A scanner can be controlled by only one Control Center.

Scanner

Scanners can perform all of the following tasks:

- Filter email for viruses, spam, and noncompliant messages
- Check email against Good Senders lists and Bad Senders list
- Filter IM messages for Spim (Instant Messaging Spam) and scan IM file transfers for viruses

Control Center and Scanner

In this configuration the appliance performs both functions. This configuration is suitable for most small installations.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Planning and Preparation

With Symantec Messaging Gateway Virtual Edition, you can deploy the Symantec Messaging Gateway as a virtual appliance on your existing VMware infrastructure, provided that the resources that are allocated to Symantec Messaging Gateway Virtual Edition meet the minimum requirements. Symantec supports mixed environments, with physical and virtual appliances deployed in the same environment.

Supported Production Deployments for SMG Virtual Edition

- VMware® ESX 3.5 update 5, ESX 4.0, ESXi 4.1
- VMware® vSphere 4.1
- VMware® ESXi 3.5 update 5, ESXi 4.0, ESXi 4.1

Other versions of ESX Server and ESXi as well as other VMware products, such as VMware® Workstation and VMware® Player, and virtualization platforms from other vendors, such as Citrix® and Microsoft®, are not currently supported.

This document assumes that the user has an existing VMware ESX deployment, is familiar with administering virtual machines such as the Virtual Infrastructure Client, and has the resources to meet the prerequisites that are outlined in this document. You must have already installed and configured the ESX Server before installing Symantec Messaging Gateway Virtual Edition. For ESX Server requirements, refer to your VMware documentation.

Recommended Hardware Allocation

Processor	4 Virtual Processors- Symantec recommends allocating at least 4 virtual processors or more based on workload demands and hardware configuration.
Memory	4GB RAM - A minimum of 2 GB is necessary to run Symantec Messaging Gateway and the virtual machine.
Disk Space	90 GB - For best results, Symantec recommends reserving at least 90 GB of disk space for most deployments.
NICs	Symantec recommends two NICs for performance reasons.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Spam Control and Mail Considerations

Reside on the Edge

Messaging Gateway can be fully utilized when it is positioned on the “Edge” of the inbound mail flow with no Message Transfer Agent or Mail host preceding it. In this way email from internet will be delivered directly to the Messaging Gateway Scanner. This will allow Messaging Gateway Adaptive Reputation to see the original source IP address for inbound connections and reject incoming based on IP reputation.

Inbound and Outbound

Messaging Gateway should be used to scan both inbound and outbound messages. Scanning inbound messages provides protection from unwanted spam, viruses and unwanted content. Scanning outbound messages provides data loss prevention of intellectual property and confidential data. Outbound scanning also provides spam blocking that might cause the company domain to become added to blacklists or otherwise blocked and it enforces encryption of sensitive messages

Scanning both directions provides full message tracking in audit logs and complete reporting of messaging patterns. Bi-directional scanning can also block incoming backscatter spam attacks (Non Delivery Report, based spam).

Use Multiple IP addresses

In Messaging Gateway version 9.0 the need for multiple IP addresses was eliminated, allowing the use of a single IP and port for both inbound and outbound mail flow. However, this requires more CPU cycles per connection. It is still best practice to use a unique IP address or port for both inbound and outbound.

In environments with multiple email domains, it is possible to assign an IP address per domain. This allows domains to continue to send email if a second domain's IP becomes blocked.

Keep the software up to date

By keeping the Symantec antispam software updated the Administrator makes sure they can take advantage of the latest technology in antispam software.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Configure Regular Backups

Symantec Messaging Gateway provides three levels of backup included in its interface.

- Full Backup - Backs up the complete database, as well as Suspect Virus Quarantine messages and compliance messages that are stored on disk.
- Backup only Configuration and Incidents - Backs up all configuration data in the database, as well as compliance data and compliance messages that are stored on disk.
- Backup only Configuration, Incidents, Logs and Reports - Backs up all configuration, incident, report, and log data in the database; as well as compliance messages that are stored on disk.

Backup from the appliance is performed at the Control Center for the entire deployment.

Selecting the appropriate level of back should be determined based on service level agreement.

Backups can be run manually or scheduled. A common proactive strategy is to schedule nightly configuration backups and weekly full backups.

When deploying virtual appliances, Symantec Messaging Gateway supports all methods provided by VMware ESX for backup and restore, including cloning and snap shots. Please refer to your VMware documentation for more information.

Configuration

Use DDS address resolution to populate Policy Groups

Messaging can use LDAP to retrieve Distribution lists and security groups from the directory.

Creating policy groups that reference the directory groups will reduce administration time managing policies for specific use cases.

Maximize network Interface

Set interfaces to the highest speed possible. For example, full duplex and non-auto-negotiate. On certain network environments, the auto-negotiation process does not set the best speed/duplex option on the link between the appliance's NIC and the switch. Symantec suggests the administrator manually selects the best possible speed/duplex combination for each Ethernet interface.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Update Alert and Notification “from Address”

The default email address for Messaging Gateway to send outbound messages is from IT@yourcompany.com and alertadmin@yourcompany.com. These should be changed to reflect the internal mail address scheme. These addresses can be found in the following locations:

- Content, Notifications
- Administration, Alerts
- Administration, Reports

Protocols Configuration

Implement Recipient Validation for ALL domains possible.

Most of the spam is sent blindly without attention to the recipient name in some sort of brute force attack that also enables the spammer to discover who the existent/valid recipients are using a technique called Directory Harvest Attack (DHA). Recipient validation allows the Administrator to accept only those messages that have a valid recipient and reject messages to invalid recipients if Reject Invalid Recipients is enabled. This greatly reduces the volume of spam to be processed.

Reputation Configuration

Use the Symantec Global Bad Senders to detect spam sources

Make use of Symantec Global Bad Senders data to stop a majority of spam at connection time.

Use action “reject” instead of “delete” or “defer” when possible

The idea behind this is: the more rejected, the less processed. Knowing that the vast majority of the inbound SMTP traffic received these days is spam (75-90%) greatly helps to use the resources available to process valid messages.

Enable Directory Harvest Attack (DHA) with action “reject” (requires Recipient Validation).

Spammers employ directory harvest attacks to find valid email addresses at the target site. A directory harvest attack works by sending a large quantity of possible email addresses to a site. An unprotected mail server will simply reject messages sent to invalid addresses, so spammers can tell which email addresses are valid by checking the rejected messages against the original list.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Enable Connection Classification

To use this feature the appliance must be deployed at the gateway (receiving SMTP connection from the original IP address). When enabled, it will restrict the quality of service to connections from sources that are known to send spam.

Spam Policies

Set Spam verdict to Delete message

With an accuracy of less than 1 in a million false positives makes Symantec Messaging Gateway is the gold standard of antispam solutions. Spam could represent more than 90% of the total volume of messages received. According to several studies, the time lost manually reviewing and deleting spam costs the most in lost productivity, therefore Symantec strongly suggests to set the antispam policies to delete spam automatically.

Set Suspect Spam verdict to Hold in Quarantine

Similar to spam verdict, suspect spam is represented by the messages that are on the edge of receiving full spam verdict. Adjusting Scan Setting Threshold will affect the ratio of spam to false positive messages determined to be suspect spam. Lowering the Threshold will result in more messages receiving a suspect spam verdict. Messaging spam rules are weighted to the default threshold setting of 72. It is usually recommended to quarantine suspect spam until an ideal threshold level is reached. Once optimal threshold is reached, change action to “delete message”.

Use Action “Bypass content filtering policy” in spam and suspect spam verdicts

When using Content policies that block based content policy, inappropriate language for example, it is possible for the messages usually deleted as spam, to now be quarantined or tagged. This distorts tracking legitimate messages with content violations with spam messages. It is recommended to leverage the action “Bypass content filtering policy” and select appropriate content policies.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Enable Bounce Attack Prevention (BAP)

Bounce Attack Prevention protects the systems from bounce attacks. BAP will identify fake Non Delivery Reports (NDRs) and prevent backscatter attacks from entering the network with configurable actions, including rejecting or deleting these messages, while still allowing legitimate bounce message notifications to be delivered normally. Bounce Attack Prevention requires both inbound and outbound message scanning.

Enable probe participation

Symantec Messaging Gateway provides the option to convert invalid recipient email addresses into probe accounts which can be used in the Symantec Probe Network. Probe accounts help Symantec track spam and learn from it. The intelligence that Symantec gains from probe accounts enables continuous improvement of the rules that govern spam filters. Better filters means fewer spam intrusions on the network.

Configure Spam Quarantine Expunger

Messages held in spam quarantine will be purged after a configurable amount of time. Set the expunger to match the corporate policy. Holding messages for greater periods of time will increase the amount of hard disk space required.

Enable sender authentication

The Administrator can enable SPF and SenderID sender authentication on a per domain basis and DomainKeys Identified Mail (DKIM) validation on a system-wide basis. Sender authentication features included on the Symantec Messaging Gateway appliance such as SPF also depend on how the sender domain SPF records have been created. For these, only enable sender authentication for domains the Administrator knows are properly configured and frequently spoofed. For DKIM, the Administrator can create a content filtering policy to apply actions based on the results of DKIM validation.

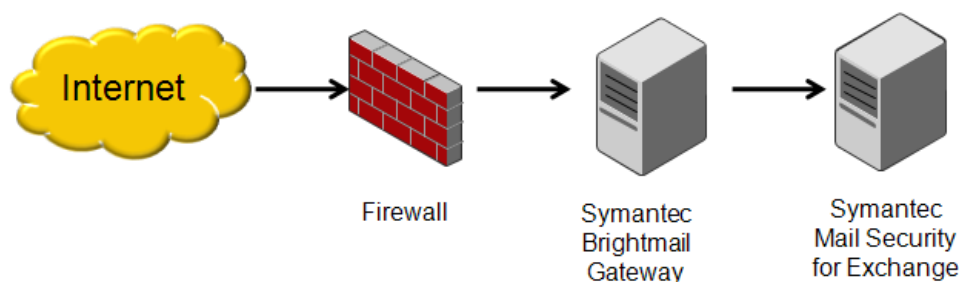
Use default virus policies

It is important to review the virus policies in Symantec Messaging Gateway. Using the default configured virus policies will provide the best overall AV experience.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Using Both Messaging Gateway and SMS for Exchange

To provide a more secure policy, it is important to provide multiple layers of protection to your environment, as shown logically in the illustration below:



Why does Symantec recommend the use of multiple servers?

- Each software package will have full control of the appropriate ports and processing power needed to properly function.
- It provides redundant service; each software package can "back up" the functions of the other if their primary servers need to be taken out of service.
- Troubleshooting mail delivery problems is easier when each step in the delivery process can be segmented into discrete parts.
- Internal email may not necessarily be passed through the Messaging Gateway. SMS for Exchange makes sure mail between internal users gets scanned.
- Historical data in the information stores may be unscanned by newer definitions. SMS can ensure the data store is scanned regularly.

When using Symantec Messaging Gateway as an interim step between the Internet and the Symantec Mail Security server, the DNSBL functions of Symantec Mail Security will not function, as the client IP address that the Symantec Mail Security server will receive is the IP address of the Symantec AntiVirus for SMTP Gateways server. The DNSBL features in Symantec AntiVirus for SMTP Gateways will continue to work as expected, provided the server receives the actual IP address of the external client and not the IP address of the Firewall or Router when an email is delivered to the server.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Where to get more information

Resource	Location
Installation Guide for SBG	http://www.symantec.com/business/support/index?page=content&id=DOC3742&key=53991&actp=LIST
SBG Admin Guide	http://www.symantec.com/business/support/index?page=content&id=DOC3741&key=53991&actp=LIST
SBG Community	http://www.symantec.com/connect/security/forums/Messaging-gateway

Symantec Mail Security for Exchange

Symantec Mail Security for Microsoft Exchange (SMS FOR MSE) provides protection of messages as they pass through the email host or are stored in the messaging host's database. This includes:

- Virus scanning repair and removal.
- Content based scanning.
- Spam Filtering (optional Symantec Premium Antispam add-on)

Components

Symantec Mail Security for Microsoft Exchange is a complete solution that installs on the Microsoft Exchange Server and consists of two components:

- Symantec Mail Security for Microsoft Exchange Server
- Symantec Mail Security for Microsoft Exchange Console

When installed each Microsoft Exchange server will host both. The console in each install of SMS for MSE can manage the local install as well as installs on other Microsoft Exchange hosts. Additionally SMS for MSE console can be installed on additional workstations for remote administration.

Symantec Mail Security for Microsoft Exchange does not protect the core Windows operating system. To protect the Windows host, Symantec recommends using Symantec Endpoint Protection or Symantec Critical System Protection.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Planning and Preparation

One of the most important considerations when planning a Symantec Mail Security for Microsoft Exchange deployment is to understand the Microsoft Exchange server environment. Microsoft Exchange deployments fall under two scenarios:











A single Exchange server deployment, typical for small to medium size organizations:

- For Microsoft Exchange 2003: Front-end/Back-end architecture combined on a single server.
- For Microsoft Exchange 2007/2010: All roles are deployed on a single server acting as the Hub, Mail, and Client Access server. No Edge Server deployment.

Multiple Microsoft Exchange server deployments, typical for larger enterprise environments:

- For Microsoft Exchange 2003: Multiple Exchange front-end servers relaying to multiple Exchange back-end servers.
- For Microsoft Exchange 2007/2010: Exchange server deployed within the DMZ as the edge transport and additional servers deployed within the secured network as the Hub and/or mail server. In Microsoft Exchange 2007/2010, SMS FOR MSE installs on the Edge, Mailbox and Hub roles only.

SMS FOR MSE Supported Versions

Platforms	SMS FOR MSE 6.0	SMS FOR MSE 6.5
Windows 2000 Exchange 2000		
Windows 2003 Exchange 2003		
Windows 2003 Exchange 2007		
Windows 2008 Exchange 2007		
Windows 2008 Exchange 2010		

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Before installation can be completed the Administrator must ensure that they have the following pre-installation steps completed.

Pre-Installation

Obtain a network diagram to ensure the Administrator has a full understanding of the messaging architecture. Be sure to collect the following data:

- How messages are received by the Exchange servers and any other server communications.
- Active directory details.
- Will the same AD domain be used throughout the organization?
- Will Exchange servers in a child domain or different domain also need to be administered from the same SMS FOR MSE console?
- What user has been chosen as the SMS FOR MSE Admin?
- Has there been a previous install that added the SMS FOR MSE user groups to the AD schema? Are they still valid? Do they have any members, any permissions applied?

Validate the system requirements.

Refer to the Symantec Mail Security for Microsoft Exchange Implementation guide; section System Requirements to confirm that the current system meets the minimal system requirements. Typically common install errors are a lack of the following:

- For Microsoft Exchange 2003 and 2007, identify the .NET framework version and ensure it is at least version 2.0.
- For installs on Microsoft Exchange 2007 Mailbox role only, ensure that Microsoft Exchange Server MAPI client and Collaboration Data Objects 1.2.1 is installed.
- For Microsoft Exchange 2010, identify the .NET framework version and ensure it is at version 3.5.
- For Microsoft Exchange 2010 installs ensure that Microsoft Windows Powershell 2.0 is installed.
- Before the Administrator installs SMS FOR MSE on Exchange 2010 mailbox role, the Administrator must specify a domain user account. This is required during a manual/scheduled scan, SMS FOR MSE needs to communicate with the Exchange CAS role.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- For Microsoft Windows 2008 Server, the Administrator will need to install IIS 6 Management Compatibility and ensure IIS 6 Scripting Tools is also installed. Use the Server Manager under Administrative Tools to install the Web Server (IIS).

Refer to the following KB article for more information on System Requirements:

<http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2010021514591054>

Running 3rd party antivirus on the Exchange Server. If the Administrator are running a 3rd party antivirus solution to protect the system's operating system, make sure the Administrator set up an exception so that the antivirus software does not scan the SMSME directory. If currently using Symantec Endpoint Protection or Symantec Antivirus refer to the following KB articles for more details:

- [Exclusions needed for antivirus scanning when using Symantec Mail Security for Microsoft Exchange on an Exchange Server 2010](#)
- [About SEP automatic exclusion of files and folders for Microsoft Exchange server and Symantec products](#)

Symantec Mail Security for Microsoft Exchange Port requirements

SMS FOR MSE Firewall Port requirements

Component	Port	Process	Purpose
Rapid Release Definitions	21	ftp.exe	Frequent AV updates
LiveUpdate	80	LuComserver.exe	Frequent AV updates
Conduit	443	Conduit.exe	Continuous Premium Antispam updates
DEXL Service	8081	Process ID: 0 or 4 (System)	Console Communications
CmafReportSrv	58081	CmafReportSrv.exe	Reporting Database

- If the optional Rapid Release feature is not used, SMS for MSE will not initiate activity on port 21.
- If Symantec Premium Antispam is not licensed and enabled, SMS for MSE will not initiate activity on port 443.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- If Symantec Premium Antispam is enabled, be sure to open port 443 on the firewall for bi-directional traffic to aztec.Messaging.com. Note, Symantec Premium Anti-Spam is not needed if using Symantec Messaging Gateway in environment.
- The port used for communications with SMS for MSE's Console can be configured during installation or at any time after. Please note that activity will only be seen on these ports when using the console to administer a remote server.

Installation

- Ensure the Administrator has a valid license file available.
- Install during off-peak hours. The installation will be conducted on the Administrator production Microsoft Exchange server. You can install SMS for Exchange without affecting the existing Exchange services . However the following must be done to enable SMS for Exchange filtering:
 - For Microsoft Exchange 2003 the Administrator must restart the Microsoft IIS service.
 - For Microsoft Exchange 2007/2010 the Administrator must restart the Exchange Transport service.
- When selecting from a typical or custom installation consider the following prior to selecting the course of action:
 - Use the complete installation option when installing on the Exchange Server.
 - Use the custom installation option when installing on a non-Exchange Server used for management purposes only.
- During the installation a service port will be identified so that the Management console will be able to communicate with the SMS FOR MSE. The default is port 8081. This is a common port and the Administrator may need to manually change the port during the installation process. If the Administrator installs the management console on a separate server or desktop and have a firewall separating the two systems, ensure they can communicate across the defined port.
- The license files should be accessible during this step of the installation. The license file will enable antivirus protection, Symantec premium antispam, and the use of SMS FOR MSE. During the license file registration process the system will attempt to download the most current antivirus rules. Verify that the Administrator has outbound access through the firewall on port 80 before allowing this communication.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Performance

As a general rule the SMS for Exchange product consumes a minimum of 5-10% of additional system utilization. Ensure that the defined system has enough available resources to handle the added load. Message delivery latency may occur if Microsoft Exchange server is running at hardware capacity.

Administration

Mail Security for Exchange and Symantec Endpoint Protection

SMS FOR MSE 6.x folders are not automatically excluded by the SEP automatic exclusion system. If you are installing SMS FOR MSE 6.x, one directory needs to be excluded manually. Assuming a default installation path for Mail Security: C:\Program Files\Symantec\SMS FOR MSE\6.0\Server\

The actual path to the above directory can vary, depending on custom installations, and will need to be set up accordingly.

The following document can be used to create centralized exceptions of the 'folder' type for the Server folder: [Making exceptions using centralized exception policies in Symantec Endpoint Protection Manager](#).

LiveUpdate

When running Symantec Endpoint Protection (SEP) or Symantec Antivirus(SAV) with SMS FOR MSE, on Windows server 2003 both products will share antivirus definitions. Symantec recommends that the Administrator disables the LiveUpdate Server within SMS for MSE. Do not disable for 64-bit operating systems.

Mail Security for Exchange on Microsoft Exchange 2007

Exchange 2007 can be installed with several different roles. As each role should have different exclusions, exclusions should be based on the roles you have installed. Symantec Endpoint Protection's Exchange 2007 automatic exclusions detect the mailbox role and set the required base exclusions. In a clustered environment, you must make additional exclusions manually.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec recommends that you exclude the quorum disk, the %Winnt%\Cluster folder, and the file share witness which is located on another server in the environment, typically on the Hub Transport server.

For more information on how to make these exclusions manually, please see [How to add a Security Risk Exception in the Endpoint Protection Manager](#).

For a list of recommended exclusions for Exchange 2007, read the Microsoft TechNet article [File-Level Antivirus Scanning on Exchange 2007](#).

Setting Exclusions for Microsoft Exchange 2010

Currently Symantec Endpoint Protection (SEP) and Symantec Antivirus (SAV) do not have automatic exclusions for Symantec Mail Security for Exchange, nor Exchange 2010. These exclusions need to be set manually in order to prevent the local antivirus solution from scanning directories that may conflict with mail flow or cause issues to the integrity of the information store.

1. [This](#) Microsoft article describes the folders that you must exclude from any local antivirus software (Symantec or otherwise) to ensure proper functionality of Exchange Server 2010. <http://technet.microsoft.com/en-us/library/bb332342.aspx>. Depending on the role of the Exchange server, you may need to set different exclusions according to the Microsoft article listed above.
2. After you set exclusions for Exchange 2010, exclude the following folder for Mail Security: <Install drive>\Program Files (x86)\Symantec\SMS FOR MSE\6.5\Server
3. The presence of email scanning tools for SEP and other antivirus software may conflict with mail flow on the server. The best practice is to install the antivirus client without the email scanning tools by performing a custom installation. These email scanning tools do not honour exclusions and have built-in SMTP activities that may interfere with normal and efficient email production.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

For details, read [How to improve email performance by removing the email scanning tools of the Symantec Endpoint Protection or Antivirus product.](#)

Mail Security for Exchange on a Microsoft Small Business Server

SMS for MSE is supported on both SBS 2003 and SBS 2008. Use the latest available release of SMS for MSE for best results.

Make sure that the correct numbers of threads are calculated.

To control (tune) scanning speed and performance, Symantec Mail Security allows administrators to set the number of VSAPI scanning threads and the number of scan processes. It is recommended to initially configure the number of VSAPI scanning threads and the number of scan processes as per the instructions in [this article](#), monitor performance and make adjustments (override the defaults) if necessary.

Ensure that the correct exclusions are in place on the Server's Antivirus Program

Administrators should add centralized exclusions to ensure that there is no chance of the AV product which protects the server's file structure scanning materials that are in use by SMS for MSE. The latest releases of Symantec Endpoint Protection (SEP) and Symantec Antivirus (SAV) should automatically detect MS Exchange and SMSMSE and set the correct exclusions. It is wise to create redundant exclusions to guarantee that there will be no interference. See [Configuring exclusions when Symantec Mail Security for Microsoft Exchange and either Symantec Endpoint Protection or Symantec AntiVirus Corporate Edition are installed together](#)

If Symantec Endpoint Protection or Symantec Antivirus is installed, Ensure SMS for MSE's LiveUpdate is Configured Correctly

For 32-bit Small Business Servers, SMS for MSE's LiveUpdate should be disabled. SEP or SAV will automatically share definitions with SMS for MSE. For 64-bit Small Business Servers, ensure that SMS for MSE's LiveUpdate is enabled. For details, please see [About Enabling LiveUpdate When Symantec Mail Security for Microsoft Exchange 6.0.9 and Symantec Endpoint Protection 11.x Are Installed on a 64-bit Exchange 2007 Server](#)

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Ensure that the SBS has ample resources

The Small Business Server combines many important server roles on one computer (Active Directory Domain Controller, Exchange Server, MS SQL Server, SharePoint server, IIS, WSUS, and so on). Shortages of memory, processing power, and disk space can be common if the server is not configured and maintained well. A lack of resources has the potential to affect SMS for MSE.

Use Microsoft's SBS Best Practices Analyzer to ensure the server is in good health

Underlying issues such as low resources, old driver versions, and network trouble will have an effect on SMSMSE and MS Exchange. Microsoft has made a tool freely available which can analyze a Small Business Server and highlight any such issues. Symantec Technical Support recommends that these tools be run periodically and that server administrators act upon any errors, warnings, or recommendations.

[Microsoft Windows Small Business Server 2003 Best Practices Analyzer](#)

[Windows Small Business Server 2008 Best Practices Analyzer](#)

Where to get more information

Resource	Location
SMS for MSE Getting Started Guide	http://www.symantec.com/business/support/index?page=content&id=DOC3901&key=51980&actp=LIST
Product Manuals	http://www.symantec.com/business/support/index?page=content&id=DOC2206&key=51980&actp=LIST
SMS for MSE Community	http://www.symantec.com/connect/security/forums/domino

Symantec Mail Security for Lotus Domino

Symantec Mail Security for Domino is a complete, customizable, and scalable solution that scans Lotus Notes database document writes and email messages that pass through the Lotus Domino server. Mail Security is also compatible with IBM Lotus Sametime 7.x and QuickPlace 6.5 and 7. Mail Security protects the Lotus Domino server from the following:

- Threats (such as viruses and worms)
- Security risks (such as adware and spyware)

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Unwanted content
- Unsolicited email messages (spam)

Symantec Mail Security for Domino also lets the Administrator manage one or multiple Domino servers. The Lotus Domino environment is only one avenue in which threats can penetrate the site. For complete protection, ensure that every computer and workstation at the site is protected by a desktop antivirus solution.

Planning and Preparation

Before the Administrator installs Symantec Mail Security 8.0.5 for Domino, ensure that the environment meets the system requirements. The administrator who installs the product must have full read and write access to the registry and file system.

The Mail Security installation program reads the Windows registry to locate the Lotus Domino server and default data directories. In addition to Mail Security registry keys, Mail Security installs files to the following directories (new directories are created as needed).

If there are multiple Lotus Domino partitions on the same server, the installation program detects each one, and lets the Administrator specify the partitions on which to install Mail Security. If the Administrator installs Mail Security to a partitioned server on a Windows cluster computer, the installation program might ask which of the Mail Security databases the Administrator wants to keep even if Mail Security was never installed on the computer. Installation proceeds regardless of which option the Administrator selects.

Mail Security does not support protecting multiple versions of Domino that are running on the same computer. Only the most recently installed version of Domino is protected. To ensure the most secure configuration, the Mail Security extension manager dynamic link library file (nnem.dll) should load *before* any third-party Domino extension manager. You should ensure that the nnem.dll is the first entry for the EXTMGR_ADDINS parameter in the *notes.ini* file.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Some third-party software are Domino add-in tasks and run as a service on the Windows operating system. These services might prevent the Mail Security extension manager dynamic link library file from loading if they start before the Domino server starts. Therefore, these processes should only start after the Domino server starts.

Deployment Best Practices

An Administrator can install or upgrade Mail Security using the installation wizard that is on the product DVD. Mail Security uses the Windows Installer service. Ensure that the service is enabled before beginning installation.

To prepare for installation

If Symantec Premium Antispam is installed, ensure that it is disabled. For more information on enabling and disabling Symantec Premium Antispam, refer to *Symantec Mail Security 8.0.5 for Domino Implementation Guide*. When deployed with Symantec Messaging Gateway, Symantec Premium Antispam is not necessary.

Shut down the Lotus Domino server. The Lotus Notes client must also be shut down if it is on the same computer.

Accessing Mail Security

Mail Security is fully integrated with the Lotus Notes environment and can be accessed like any other database. When the Administrator opens any Mail Security database, a navigation pane appears on the left. Access any of the Mail Security databases from the navigation pane. Each Mail Security database contains options that are specific to that database. For example, the Log database contains options for server messages, product information, and incidents. The navigation pane only contains the options for the databases that are available and for which the Administrator has at least Reader access. For example, the navigation pane does not display the options for the Definitions database if it has not been created. If the Administrator creates a Definitions database, they must close all of the Mail Security databases and documents. When they open any of the Mail Security databases, the Virus Definitions option appears on the navigation pane. For information about creating a Definitions database and on troubleshooting user interface errors and issues, refer to *Symantec Mail Security 8.0.5 for Domino Implementation Guide*.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Configuration Best Practices

Sign the Mail Security databases

Before the Administrator opens the databases for the first time, sign the databases with a trusted Notes ID file, using the Domino Administrator client. Signing the databases is necessary to ensure the proper operation of all of the Mail Security features in the Domino environment. To properly sign the Mail Security databases, ensure that the following settings are configured in the Domino Administrator client:

- Sign all design documents (do not update existing signatures only).
- Sign all data documents using an administrator ID.

Configure the ID as follows:

- The ID should sign all data documents, not just those with existing signatures.
- The ID should be a trusted administrator's ID or server ID.
- The ID should have the right to run unrestricted Methods and Operations, which is necessary to run all of the database agents.
- The ID used to sign the databases should appear on the workstation's Execution Control List (ECL).

Ensure that the trusted Notes ID in the Execution Control List is listed with the following rights in the Notes client:

- Access to current database
- Access to environment variables
- Access to external code
- Access to external programs
- Ability to read other databases
- Ability to modify other databases
- Ability to export data

For more information on signing databases, see the Domino Administrator and Lotus Notes documentation.

Granting rights to run unrestricted agents

Mail Security contains agents to help the Administrator manage database size and run scheduled queries. They must grant rights to the user who signs the IDs. The agents are as follows:

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Log purge agent - purges events from the Log database. By default, threat incidents are purged after 365 days. Server messages and other incidents are purged every 30 days.
- Quarantine/Backup purge agent - purges items from the Quarantine database. By default, all items in the Quarantine are purged after 30 days.
- Scheduled reports agent - runs scheduled queries in the Log database. By default, the agent runs scheduled queries once a day and posts the queries in the Completed Reports view.

For users to enable, disable, or modify an agent, the administrator must grant rights to run unrestricted agents in the Server Document of the server that is running Mail Security. **Note:** Agents are disabled by default. An Administrator must enable the agents that they want to use.

Restrict access to Mail Security databases

To maintain security in the Lotus Domino environment, restrict access to the Mail Security databases to administrators by setting the Access Control List (ACL) for following databases:

- Settings (sav.nsf)
- Log (savlog.nsf)
- Quarantine (savquar.nsf)
- Definitions (savdefs.nsf), if used

The Quarantine database requires that the Administrator also assign roles to Quarantine database users. These roles restrict access to various Quarantine views and control who can release documents from the Quarantine. When the Administrator sets access control for the Quarantine database, they must assign roles to those groups and users who use the Quarantine.

Disable Symantec Premium Antispam

With the inclusion of Symantec Messaging Gateway as part of the Symantec Protection Suite Enterprise Edition for Gateway, Symantec Premium Antispam add-on to Symantec Mail Security should not be used. Symantec Messaging Gateway uses the latest technologies to block messages before they touch the Domino environment. Using Messaging to block spam is faster more accurate and does not use Domino Server resources.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Recommended Maintenance

Scan the Domino server for risks and violations

You can configure Mail Security to scan the Domino server on a regular schedule, or the Administrator can start a scan on demand. The auto-protect feature detects risks, spam, and content filtering rule violations in real-time as email messages are routed through the Lotus Domino server or as documents are written to the server. Mail Security scans document writes and email messages in all databases on Lotus Domino servers which have not been excluded. It includes files in compressed and encoded formats, such as Zip. It also decomposes and scans file attachments for threats and security risks

Where to get more information

Resource	Location
Product Manuals	http://www.symantec.com/business/support/index?page=content&key=51977&channel=DOCUMENTATION&locale=en_us
Knowledgebase	http://www.symantec.com/business/support/overview.jsp?pid=51977&view=kb
SMS Domino Community	http://www.symantec.com/connect/security/forums/domino

Symantec Web Gateway

Symantec Web Gateway protects organizations against multiple types of Web-borne malware, prevents data loss over Web and gives organizations the flexibility of deploying it as either a virtual appliance or on physical hardware. Powered by the Insight, Symantec's innovative reputation technology, Web Gateway relies on a global network of over 175 million of users to identify new threats before they cause disruption in organizations.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Components

Symantec Web Gateway software is delivered in an appliance form factor including hardened Linux operating system, virtual support for ESX and ESXi and Web Gateway software. Symantec offers two appliance form factors, which may be purchased separately. Symantec Protection Suites licenses include the user licensing for Web Gateway. Physical appliances are an additional cost. These appliance form factors can be used in any combination to meet network traffic requirements.

The Symantec Web Gateway appliance can be configured to manage one or more other gateway appliances. This configuration is called a Central Intelligence Unit (CIU). On the Central Intelligence Unit, most Web GUI pages let allow changes or report views for all managed appliances or individual managed appliances. Symantec Web Gateway appliances can be configured to be either a web gateway or a Central Intelligent Unit, not both. A CIU **cannot** be used as a gateway appliance to monitor/control web traffic. A gateway appliance can only manage itself.

Deployment Best Practices

Placement of Web Gateway on the network.

Symantec Web Gateway offers multiple ways to deploy to meet company needs. There are generally two connection modes to deploy the web gateway. An *Active Tap* deployment receives traffic from a configured port on Network Switch. An *Inline* deployment is where the Web Gateway sits between the corporate users and the outside internet.

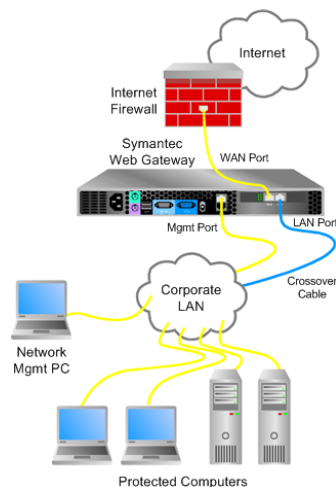
Connection Mode Comparison

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

	Inline Mode	Active Tap Mode
HTTP	Hijacks End-User -> redirect to Blocking page TCP reset -> Server side	TCP reset -> End-User and Server sides
TCP	TCP reset -> End-User and Server sides	TCP reset -> End-User and Server sides
Non TCP	Drops traffic to block	Monitoring only – no Blocking
HTTP Download by Human	Hijacks End-User -> redirect to Download progress page Hijacks Server side -> redirect to internal server	Monitoring only – no Blocking
Machine Download and Non-HTTP (FTP, IM...)	Streamed Download Blocking by corrupting the file	Monitoring only – no Blocking

Placement on the Network will determine the scope of protected systems. The closer the web gateway is positioned to the Internet, the greater the security coverage. To provide the greatest protection and coverage it is common to deploy the Symantec Web Gateway appliance just inside the firewall running in Inline Mode.

Basic Deployment



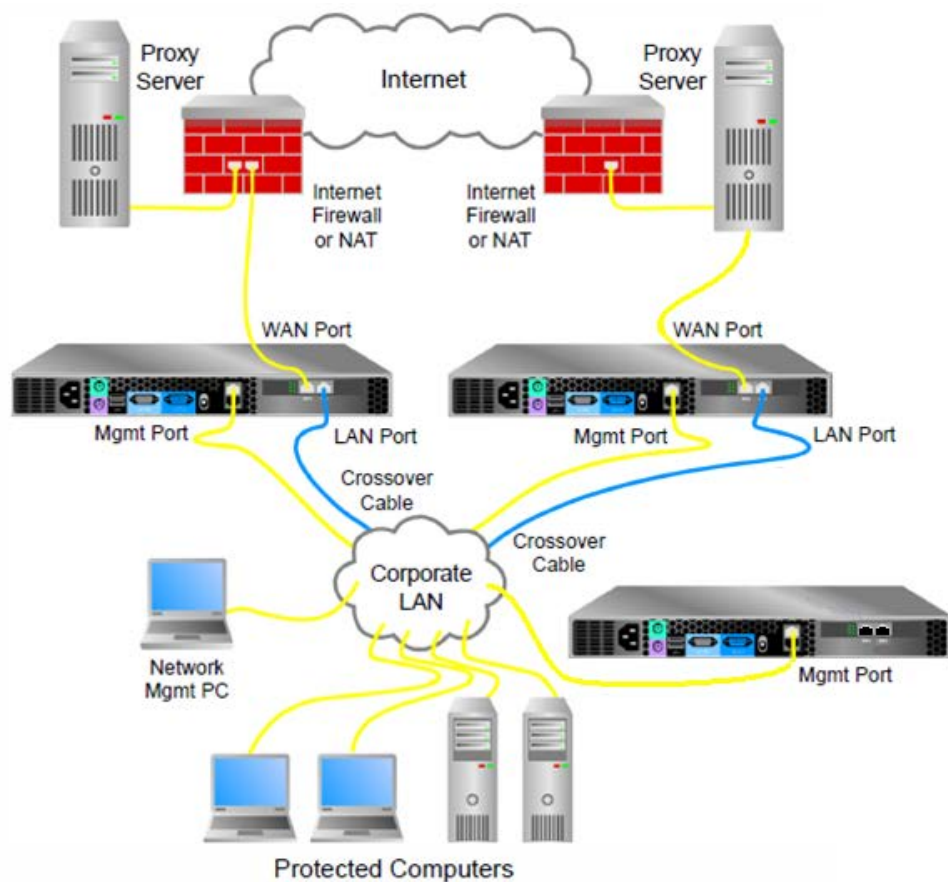
- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Basic Deployment Architecture

The diagram below illustrates connecting two Symantec Web Gateway appliances to two firewalls as part of a high availability environment. The firewalls can be configured in active-active failover or active-standby failover. The Symantec Web Gateway appliances should be configured identically except for the network settings. When used with a web proxy it is important to place Symantec Web Gateway between the corporate LAN and the Proxy Servers. In diagram 6 the left firewall web proxy deployment shows the Web Proxy being connected to a port on firewall. This is typical configuration when Proxy uses a single port. The right firewall web proxy deployment is using a two port or pass through Web Proxy, the WAN port of Web Gateway should be connected to the LAN side of Web Proxy. The WAN side of web proxy would then connect to firewall. In both deployments Proxy configuration will remain the same.

Optionally we can add a Central Intelligence Unit to the deployment. The CIU allows for central *management* of the gateway appliances. Providing a single interface to view consolidated reports, apply global policies as well as manage individual gateways.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices



Advanced Web Gateway Deployment

Web Gateway – Firewall Port Requirements

Symantec Web Gateway deployment requires the following firewall changes for deployment:

Symantec Web Gateway Firewall Ports

Port	Protocol	From	To	Description
53	UDP	Symantec Web Gateway	User-defined DNS servers	External DNS lookups, if configured
80	TCP	Symantec Web Gateway	Internet	LiveUpdate Antivirus definitions updates ¹

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Port	Protocol	From	To	Description
123	UDP	Symantec Web Gateway	pool.ntp.org (by default)	Network Time Protocol
161	UDP	Symantec Web Gateway	SNMP servers	SNMP, if configured
389	TCP	Symantec Web Gateway	Active Directory	User information from Active Directory, if configured
443	HTTPS	Symantec Web Gateway	Internet	Rule updates, software updates license registration and Remote Assist ²
443	Proprietary	Central Intelligence Unit	Symantec Web Gateway	Status polling
443	Proprietary	Symantec Web Gateway	Central Intelligence Unit	Configuration updates
514	UDP	Symantec Web Gateway	Remote syslog	Malware alerts or system alerts to remote syslog, if configured

Note:

- Antivirus definitions updates will use the following by default:
- liveupdate.symantecliveupdate.com - Default automatic antivirus updates (Port 80/TCP)
- liveupdate.symantec.com - Default automatic antivirus updates (Port 80/TCP)

Messaging Gateway uses the following hostnames for updates/licensing/rules:

- threatcenter.symantec.com- Used to retrieve new build versions (Port 443/TCP)
- license.cobion.com- Used to register the appliance (Port 443/TCP)
- filterdb.iss.net- Used to retrieve URL classification data (Port 443/TCP)

It is imperative to not use specific IP addresses for the above hostnames when creating firewall rules.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Web Gateway Virtual Edition

Symantec Web Gateway Virtual Edition runs as a virtual machine on VMware so that you can run Symantec Web Gateway on the hardware and operating system of your choice.

Virtual Edition Considerations

All network configurations are supported.

- Inline (supported but not recommended)
- Proxy
- Inline + proxy
- Port span/tap
- Central Intelligence Unit

Symantec Web Gateway Virtual Edition does not have a bypass mode like the Symantec Web Gateway appliances. For Symantec Web Gateway Virtual Edition, in an inline network configuration, network traffic is halted when the service is disabled or the physical host computer is turned off.

You must connect the computers that you want to access the Web GUI to the Ethernet port that is assigned to the Management network.

Symantec does not support restoring from a VMware snapshot.

Deploying the Web Gateway Virtual Edition

Deploy the OVF template that you download from FileConnect on a VMware ESX/ESXi Server. If you use ESX version 4.1, when you download the template, you may be asked to choose thin disk provisioning or thick disk provisioning. Symantec Web Gateway recommends that you use thick disk provisioning.

An OVF template is a virtual machine that includes the software that you plan to run on the computer. You can deploy the OVF template with a vSphere client on a different computer than the computer that hosts your ESX/ESXi Server.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Web Gateway only supports the deployment of an unaltered OVF template file.

Symantec Web Gateway does not support the creation of an OVF template from the Symantec Web Gateway template.

The OVF deployment usually takes about 10 minutes. When it completes, the new computer appears in your inventory. You may want to configure your guest computer to restart when the host computer restarts.

Central Intelligence Unit

Any Symantec Web Gateway appliance can be configured to manage one or more other Symantec Web Gateway appliances. On the Central Intelligence Unit, most Web GUI pages allow changes or report views for all managed appliances or individual managed appliances. Appliances that process web traffic and are not configured as a Central Intelligence Unit are referred to as a gateway appliance. Symantec Web Gateway appliances can be configured to be either a web gateway or a Central Intelligent Unit, not both. You can continue to log on to the Web GUI of managed gateway appliances after adding to a Central Intelligence Unit. Once an appliance is configured as a Central Intelligence Unit, that appliance cannot function as a Symantec Web Gateway.

- Centralized management - Make the same change to multiple appliances at the same time or make unique changes to individual appliances from the Central Intelligence Unit
- Centralized reporting - View consolidated reports from all managed appliances

Configuration Best Practices

Configuring Web Gateway to Fail closed

The Symantec Web gateway appliance includes a special network card that is used for inline mode. In the event of a power failure, the web gateway appliance's LAN and WAN ports will act as a cross over cable. As noted in the basic deployment diagram a crossover cable is usually used between corporate LAN and appliance LAN port. This has the effect of making cable to LAN and a WAN port act as a standard cable, and allows traffic to continue even when appliance is powered down or in bypass mode, which is known as failing open. In order to fail closed, use a standard cable between Corporate LAN and the LAN port on the appliance. This will have effect of acting as a crossover cable. You will also need to disable the ability to auto switch between standard and crossover on ports for both Corporate LAN switch and Firewall.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

SYMANTEC WEB GATEWAY VIRTUAL EDITION DOES NOT HAVE A BYPASS MODE LIKE THE SYMANTEC WEB GATEWAY APPLIANCES. FOR SYMANTEC WEB GATEWAY VIRTUAL EDITION, IN AN INLINE NETWORK CONFIGURATION, NETWORK TRAFFIC IS HALTED WHEN THE SERVICE IS DISABLED OR THE PHYSICAL HOST COMPUTER IS TURNED OFF.

Enable Web Gateway Modules

Some features of Symantec Web Gateway must be enabled to function. Alternatively, some features can be disabled to improve the efficiency of Symantec Web Gateway.

Enable Application Control	Allow, monitor, or block the programs that access the Internet. Configure application control policies on the Edit Policy page. This feature is included in the base license.
Enable Content Filter	Allow, monitor, or block access to internet sites based on URL filtering using pre-defined categories. Content Filtering requires a separate license not included with Symantec Protection Suite Enterprise Edition for Gateway. Configure URL filtering policies on the Edit Policy page. The following setting is available for this module: <i>Consolidation</i> Do not group individual URL visits under the parent domain for this time period.
Bypass Whitelist for Content Filter	If <i>Bypass Whitelist for Content Filter</i> is checked, the internal whitelist is disabled. If it is checked, the Web pages in the internal whitelist that normally would be ignored are subject to monitoring and blocking. This feature is included in the base license. The internal whitelist contains the domain names for definition and software updates of antivirus and software vendors. Due to security concerns, Symantec cannot publish the contents of the

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

internal whitelist. If *Bypass Whitelist for Content Filter* is unchecked, URLs in the internal whitelist are not blocked or monitored for URL filtering or scanned for malware. Any subdomains of the domains in the internal whitelist are excluded from URL filtering and malware scanning also. Check the box if the Administrator do not want to omit these domains from URL filtering and malware scanning.

Record browse time

Records the approximate amount of time that each user spends using a Web browser to view Web sites. This feature is included in the base license. The following settings are available for this module:

Threshold Web browsing activity under this value is not recorded. The default is 5 minutes.

Sensitivity If no Web browsing activity is *detected* after this time has elapsed, stop tabulating the browse time. The browse time may be ignored or recorded, depending on the *Threshold* value. The default is 3 minutes.

About Active Directory integration

Symantec Web Gateway can be configured to integrate with Active Directory. Active Directory is a Microsoft product that stores user account information and provides authentication on Microsoft Windows networks. Integration with Active Directory provides the following benefits:

Users are displayed in reports

User names are displayed in reports.

User-based policies

You can create policies based on Active Directory user names and group categories.

Note: Active Directory integration only works with Active Directory running on Windows

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Server 2003 and 2008. Symantec Web Gateway does not support any other type of LDAP directory service. Symantec Web Gateway does not support global catalogs if the Administrator configure domain controller integration. Symantec Web Gateway does not integrate with Active Directory running on a virtual machine such as VMware or Citrix.

- You can configure Active Directory integration using a domain controller interface, using NTLM, or both. The following table compares the two methods of Active Directory integration. Comparing Active Directory integration with a domain controller and NTLM

Because of the overall effectiveness and user experience, best practice for deployments is to use a Domain Controller Interface for Active Directory authentication. For additional information on using NTLM for Authentication, please refer to the Symantec Web Gateway Version 4.5 Implementation Guide

Best Practice before blocking URLs

When it is determined that a Web site should be blocked based on URL category, It is best practice to first set URL category to monitor. After a period of time, check the reports to see what Web sites have been monitored. This provides an opportunity to verify that the web sites affected by this policy match only the types of Web sites intended. Also, test that the desired action occurs by accessing the Symantec Web Gateway test page from a computer in each policy work group.

Configuring the policy precedence order

Policies are evaluated in the order that they appear on the **Policies > Configuration** page.

Symantec Web Gateway evaluates the policy at the top of the page first. If more than one policy applies to the same computer, only the rules in the first matching policy determine what action to take. Symantec Web Gateway ignores the policies after the matching policy.

Assume that a policy for malware that applies to subnet 192.168.0.0 and a separate policy for malware that applies to VLAN ID 2. If a computer on VLAN 2 using IP address 192.168.0.5 encounters malware, only the first matching policy determines the action to take. This can also be applied when configuring a user, department or Organizational Unit.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Adjusting the precedence is usually only necessary when mixing policies work groups of different network types. If policies consistently use subnet, IP range, or VLAN ID to define all of the work groups, then new policies are inserted in the correct order. If using work groups of different network types in the policies, ensure that the policies are ordered appropriately. Test that the desired action occurs by accessing the Symantec Web Gateway test page from a computer in each policy work group.

[See "Testing Symantec Web Gateway for successful blocking or monitoring"](#)

You can also change the order of Spyware Category, Spyware Severity, and Detection Type within a policy.

Best Practice for General policy work groups precedence

When determining the initial layout of the policies here is a good starting point. Start with the most restrictive user work group. Expand based on LDAP users work group size. Then move to IP based work groups and expand to larger IP ranges. The final policy should be the catch-all for all computers.

- Single user
- Small group of users
- Large group of users
- Individual IP
- Small IP range
- All Computers

Policy Configuration

Administrators have the flexibility to create different web filtering policies for different groups within the organization. When creating different group policies, a key step is to identify the users or machines to whom the policy applies. Administrators have the ability to create group policies based on:

- Subnet
- IP Range
- VLAN ID
- Numerous LDAP attributes, if integrated with Windows LDAP directory

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

For example if integrated with Active Directory, users who belong to an IT Organizational Unit may be given access to a broader set of urls, and applications than users belonging to say an Accounting Organizational Unit may be allowed.

Templates can also be created to help serve as a starting point or baseline when creating new group policies.

Mixed User IP policy work groups

There are cases where it may be necessary to combine machine based work groups with user based work groups. An example is an employee who has liberal access to internet from any workstation he logs into. However if this same employee logs into a server or thin client, their Internet access needs to be restricted. While others who access servers or thin clients can access other internet sites on those same servers.

Download behavior in user Web browsers

You can configure Symantec Web Gateway policies to scan file downloads from the Internet for malware such as spyware and viruses. The *File and Active Content Detection* setting for policies determines the Web browser download behavior. The *Block* and *Use Default* actions are not available for the port span/tap network configuration.

For both the *Block* and *Monitor* actions, if the download takes longer than a few seconds, Symantec Web Gateway displays a message in the user Web browser. The message indicates that Symantec Web Gateway is scanning the download. The contents of this patience page cannot be changed. However, the Administrator can change the language that is used on this page and the image that is displayed on the page.

Recommended Maintenance

Check Blocking Feedback

Review the Blocking Feedback screen to view a list of items that users on the network have marked as being blocked in error.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

When the Web Gateway is in blocking mode and a user requests to view a site or download a file known to contain spyware, they are given a blocking page. They will also view a blocking page if they visit a URL blocked by the content filter category. By default, this page includes a link the user can use to indicate that they feel that the site or file was blocked in error. These reports are tabulated and presented here. Policymakers may review this report to make determinations about which sites or files, if any, should be unblocked.

Check System Status

The *System Status* screen gives a broad overview of the Symantec Web Gateway. Included is information about the device's *License*, *Appliance Status*, *System Information*, and *Recent System Changes*.

Check Updates

Use the Updates screen to check for database and software updates for the Web Gateway device, install the updates, view the version numbers of the releases currently installed, and revert to the previous versions.

Periodically the Web Gateway will check with the Symantec Threat Center to see if new updates are available. There is also an option to manually check for updates.

Managing Unresolved Users

Even with Active directory integration it is possible for computers to not be authenticated to an active directory user account. The three most common reasons include:

Rogue DC logon	The DC that the user logged into was not configured with DC Interface
Non Windows client	A Macintosh Linux Wi-Fi phone are examples of clients that by default do not log into an Active Directory domain. Unless they access email or other service requiring authentication
No domain logon	A system that is not part of the Active Directory domain, such as an employee's

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

personal laptop

Review the following considerations to manage unresolved users on computers.

Create IP based policies based on IP Range or IP subnet.	It is good practice to back up user based policies with IP based policies. In the event of a failed user log in, it might be possible to determine the correct policy based on the IP range assigned to the computer. Frequently these policies are far more restrictive than the user based policy.
Enable both Domain Controller Interface and NTLM Authentication to prompt users	Use this option only when User identification is essential to business practices. By enabling NTLM authentication all users that Symantecre not determined via Domain Controller Interface will be prompted for logon when accessing the internet. This also requires more processing by the gateway appliance and may impact performance.

Testing Symantec Web Gateway for successful blocking or monitoring

Symantec has a Web site to test how Symantec Web Gateway blocks or monitors network data.

Start a Web browser on a computer in the LAN that is connected to Symantec Web Gateway. If Symantec Web Gateway is in blocking mode and the Administrator have enabled policy management, the computer must be included in a policy that blocks spyware access.

On the Internet, go to the following URL: www.symantec.com The Symantec Web site should display normally without any block messages.

On the Internet, go to the following URL: testwebgateway.com/test/bltest.htm

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Blocking mode or monitoring mode should be indicated as follows:

Blocking mode	If the Administrator have configured Symantec Web Gateway in blocking mode, a block page appears in the Web browser. If the block page does not appear, Symantec Web Gateway is not correctly configured to block access to spyware.
Monitoring mode	<p>If the Administrator have configured Symantec Web Gateway in monitoring mode, the test page appears in the Web browser. To check for successful monitoring, find the computer in the Web GUI. The report should show that the computer accessed a malware page.</p> <p>If the Web GUI does not indicate that the computer accessed a malware page, Symantec Web Gateway is not correctly configured to monitor access to spyware.</p>

About reports

You can display reports on a wide range of statistics such as the following information:

- Most accessed Web sites
- Most active users
- Spyware-infected computers
- Most common malware
- Network attacks
- Infection sources

You can click linked statistics on the reports to get more information about that user, computer, Web site, category, etc.

If the Administrator has configured Active Directory integration, Symantec Web Gateway displays some report statistics by Active Directory user name. If the Administrator have not configured Active Directory integration, Symantec Web Gateway displays those report statistics by host name instead.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Where to get more information

Resource	Location
Product Manuals	http://www.symantec.com/business/support/index?page=content&key=58161&channel=DOCUMENTATION&locale=en_us
Knowledgebase	http://www.symantec.com/business/support/index?page=landing&key=58161&locale=en_us
SMS Domino Community	http://www.symantec.com/connect/security/forums/web-gateway

Symantec Workflow

Components

Workflow Solution

Workflow is a standalone solution that does not require the Symantec Management Platform to function. It will integrate with an existing Management Platform.

Workflow Designer

Workflow Designer is the tool used to design workflow process. It contains components that can be arranged into custom workflow projects and publish to the Workflow server. Workflow Designer is the user interface for creating workflow projects in Symantec Workflow 7.0.

Workflow Server

Workflow Server runs and manages published workflow projects. It should be installed on any computer to publish workflow projects. It is installed automatically when installing any Workflow component.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Process Manager

Process manager is a Web portal used to manage published processes that include human interaction. Installation of Process Manager is not required. However if utilizing interactive web forms, for example, Process manager is needed. In environments with more intensive workflow projects that require human interaction, a 64-bit system with 8 gig RAM is recommended for the Process Manager server.

Symantec Management Platform Requirements

The Symantec Management Platform, formerly known as Altiris Notification Server, requires an installation of Microsoft SQL server. The MS SQL server can be located on the same system as the Symantec Management Platform or on a separate system.

Workflow System Requirements

Hardware	Minimum requirements for evaluation	Recommended for Small Business	Recommended for Large Enterprise
CPU	Pentium 4	Dual processor dual core Xeon	Dual process quad core Xeon
CPU Speed	1.8GHz	2.53GHz	2.53GHz
RAM	1GB	4GB, DDR2	8GB, DDR2
Cache	No specific requirement	3MB L2	6MB L2
Network	No specific requirement	Gigabit	Gigabit
Hard Disk	5GB of free disk space	10,000 RPM SCSI or better. 10GB of free disk space	10,000 RPM SCSI for RAID 1, 4 or 10. Additional space dependent on implementation of site services, Software Library and other considerations.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Workflow Component Requirements

Workflow includes a number of pieces that can be installed on the same or different computers. If the installing all of them on one computer, that computer must meet all the prerequisites listed in the table below. If installing only one piece listed below, the host computer must meet the prerequisites for that piece.

Workflow Prerequisites

Software	Prerequisites
Workflow Solution	Symantec Management Platform 7.1 Microsoft .NET Framework 3.5 Symantec Management Platform Webservice 7.1
Workflow Server	Microsoft IIS 5.x or 6.x
Workflow Designer	Microsoft .NET Framework 3.5 Workflow Server – gets installed automatically during Workflow Designer installation Optional: Microsoft IIS 5.x or 6.x – An internal Web server is delivered with Workflow Designer that can be used with the debugger
Process Manager	Microsoft .NET Framework 3.5 Microsoft IIS 5.x or 6.x Microsoft SQL Server 2005 or SQL Express Workflow Server – Gets installed automatically during Workflow Designer installation.

Deployment Best Practices

Before beginning the Symantec Workflow 7.1 installation, it is recommended to install the Microsoft SQL server.

Symantec Workflow 7.1 Installation Steps Overview

- Prepare the Workflow Server
- Install the Symantec Installation Manager
- Install Symantec Workflow Solution
- Install Workflow Server/Designer/Process Manager

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Where to get more information

Resource	Location
Symantec Workflow 7.1 Installation Guide	https://kb.altiris.com/article.asp?article=49544&p=1
Workflow Users Guide	http://www.altiris.com/upload/workflow7ug_002.pdf
Workflow SWAT	http://www.workflowswat.com
Symantec Workflow Community	http://www.symantec.com/connect/endpoint-management-virtualization/forums/workflow-solution

Symantec System Recovery

Components

Centralized Management

The Symantec System Recovery Management Solution is based on the Symantec Management Platform, formerly known as the Altiris Notification Server. Three client-installed components are needed in order for a client to be managed from a Symantec System Recovery Management Solution server

- Symantec System Recovery Client
- Altiris Agent (also referred to as the Symantec Management Agent or SMA)
- Symantec System Recovery plug-in (enables agent-to-server communication)

Once the Symantec System Recovery 2011 Management Solution server has been installed, deploying the required agent packages to the clients that will be protected by Symantec System Recovery 2011 and managed centrally is a four step process:

1. Using the Altiris infrastructure to discover servers and desktops/laptops on the network

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

2. Deploying the Altiris agent, also known as the Symantec Management Agent (SMA) to the desired target systems
3. Deploying the Symantec System Recovery plug-in to the systems
4. Deploy the Symantec System Recovery agent itself to the systems (either in 'full' or 'headless' mode; headless = no local UI)

Once all necessary agents have been deployed, the administrator can configure and deploy backup policies, client configuration policies, license policies, etc.

It's important to understand that only status and configuration data is exchanged between the Symantec System Recovery Management Solution server and managed clients. Backup data (recovery points) is moved directly from protected clients to storage, and does not travel to or through the Symantec System Recovery Management Solution server. The only exception to this would be if the server was also hosting local storage to which backups were being sent via a network share (e.g. the server was hosting the management server as well as the backup storage).

A single Symantec System Recovery Management Solution server can manage up to 5,000 clients. The Symantec System Recovery Management Solution enables administrators to discover clients on the network, decide which clients he wishes to protect and manage from the Symantec System Recovery Management Solution console, and distribute agent packages to these systems remotely. Agent package distribution is done via policy, allowing the administrator to "set it and forget it" if desired, resulting in automatic agent and policy deployment to new systems that enter the network and match the attributes of those policies.

The Symantec System Recovery Management Solution supports the discovery and remote management of both the Windows version of Symantec System Recovery as well as the Linux version from the same Symantec System Recovery Management Solution server, allowing for the management of mixed Windows/Linux environments without the need to set up a separate Linux-specific management infrastructure.

The Symantec System Recovery Management Solution requires a SQL backend. If a full SQL server is available on the network, during installation you can point Symantec System Recovery Management Solution to the full SQL server instance to use it for metadata storage. If a full SQL

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

server is not available or if the administrator does not desire to use existing SQL resources for the Symantec System Recovery Management Solution, the installation process will install SQL Express.

Please note that using SQL Express as the SSR-MS backend limits scalability to 500 clients per server. For best performance in large environments, it is recommended that an “off box” (hosted on a different server) instance of SQL be paired with the SSR-MS server. SSR-MS uses SQL heavily, and having dedicated compute and disk I/O resources available to the SQL backend has a significant and positive performance impact.

Other features of the Symantec System Recovery Management Solution include: Backup destination storage monitoring, off-site copy and dedicated offsite copy, dedicated P2V, express recovery tasks, remote recovery, centralized and exportable reports, agent package customization, and more.

Another key value-add of the Altiris framework upon which the Symantec System Recovery Management Solution is built is the ability to host and run additional Altiris solutions using the same framework and infrastructure. This includes the Altiris Client Management Suite, Server Management Suite, and more.

Symantec System Recovery Windows Client

The Symantec System Recovery Windows Client is a fully standalone product that can protect individual servers or desktops/laptops.

The Symantec System Recovery Windows client contains a core agent that is the underlying ‘engine’ of the Symantec System Recovery product and performs most backup and recovery functions of Windows servers and endpoints. The core agent can be installed and managed in any of the following ways:

- Installed and managed locally using the local user interface
- Remotely push-installed to other systems on a one-at-a-time basis using the local user interface

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Push installed and managed remotely on a one-to-many basis using the Symantec System Recovery 2011 Management Solution (when using management solution to deploy SSR it can be deployed in agent-only mode or in full mode which includes the local user interface)

The full Symantec System Recovery Windows client, or just the core agent, can be installed on 32-bit and 64-bit versions of Windows Server 2003, Windows Server 2008, Windows 7, Windows XP, and Windows Vista. For the latest supported platforms and applications, please refer to the Symantec System Recovery Software Compatibility List is available at the Symantec Business Support website.

When managing the core agent using the Windows local user interfaces the following features and capabilities are available:

- Scheduled Volume-level Backups (Recovery Points)
- One Time Volume-level Backups (Recovery Points)
- Scheduled File/Folder Backups
- Event-driven Backups
- Calendar Status View
- System Tray Icon (Green/Yellow/Red Status)
- Volume Status Reporting
- Performance Throttling
- Compression and Encryption
- Backup Storage Management
- Scheduled Physical-to-Virtual Conversions
- One-time Physical-to-Virtual Conversions
- Launching the Recovery Point Browser application
- Launching the Granular Restore Option application
- Hard Drive Copy

Recovery Point Browser

A key supporting application included with the Symantec System Recovery product is the Recovery Point Browser application. Recovery Point Browser allows recovery points to be easily opened to the local user enabling the following capabilities:

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- Exploring the file/folder contents of a recovery point
- Recovering selected files and/or folders from a recovery point
- Copying or cloning a recovery point, and in doing so (if desired) adjusting compression and encryption settings
- Copying or cloning a recovery point, and in doing so splitting a recovery point into segments or combining a segmented recovery point or incremental recovery point chain into a single recovery point file
- Performing consistency and validation checks against a recovery point

Granular Restore Option

The Granular Restore Option was designed to allow users to recover files, folders, Exchange emails and Microsoft SharePoint server objects from a recovery point without having to restore the entire volume or system. The Granular Restore Option leverages a very easy to use, simply presented interface allowing users to easily browse or search the contents of a recovery point and with a simple right-click of their mouse, recover files/folders, Exchange data, or SharePoint data. The Granular Restore Option is compatible with Exchange 2003, 2007 and 2010, SharePoint 2003, 2007, and 2010 as well as SharePoint Services 3.0 (2007). In order to restore granular Exchange data, the Outlook 2003 or Outlook 2007 client must be installed to the system on which the Granular Restore Option is being used. For the latest supported platforms and applications, please refer to the Symantec System Recovery Software Compatibility List is available at the Symantec Business Support website.

Security Configuration Tool

The Security Configuration Tool is a simple utility also installed with Symantec System Recovery that enables the local administrator to determine what users have access to the Symantec System Recovery product, and for those that are granted access, what level of permissions they have (full control or status only).

LiveUpdate

In addition, LiveUpdate is also included with the Windows client, allowing standalone instances of Symantec System Recovery to receive and install product updates directly from the internet.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Symantec Recovery Disk

The Symantec Recovery Disk is the recovery environment that can be use to boot a system into recovery mode in order to perform a full bare metal recovery or dissimilar hardware recovery. The Symantec Recovery Disk for SSR 2011 can be used to recover backups (recovery points) created by SSR 2011 as well as any previous version of the product, such as Backup Exec System Recovery 2010, 8.5, 8.0, 7.0, etc. Performing a recovery with the Symantec Recovery Disk was designed to be both very easy for those new to the process and very powerful and flexible for experienced users. The basic process for performing a bare metal or dissimilar hardware restore is as follows:

1. Boot the system to be recovered with the Symantec Recovery Disk
2. Locate the recovery point to be restored (could be on a local USB drive, a network share, etc)
3. Select the local disk to where the recovery point will be restored
4. Start the recovery

When a server or desktop/laptop has been booted into recovery mode, the user can also perform “cold backups” if desired, which can be very useful for protecting hardened or locked-down systems on which software, such as a backup agent, cannot be installed.

The Symantec Recovery Disk is based on the powerful WinPE operating system from Microsoft, and enables full hardware support when a system is booted into recovery mode (including mass storage controller/RAID support, full networking support, locally attached USB device support, etc). In addition to bare metal recovery, dissimilar hardware recovery, and cold backup capabilities, the Symantec Recovery Disk also includes a host of configuration and troubleshooting tools, allowing the user to adjust network settings, map a network drive, check the local file system for errors, adjust partition table settings, gather restore logs, and more.

The Symantec System Recovery Disk is multilingual and supports all the languages supported by the Symantec System Recovery 2011 product. When booting a system into the recovery environment the user is able to select their desired language.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

The default recovery disk comes on CD media (or an ISO file for electronic versions). The default System Recovery Disk is ready to be used for recoveries right out of the box, and includes a large driver database that supports most server and desktop/laptop hardware available. The default driver database is updated with each release of Symantec System Recovery.

For cases where a customer is using older or very new hardware, in which cases the default driver database may not include all the necessary drivers to perform a successful bare metal or dissimilar hardware recovery operation to the hardware in the environment, Symantec System Recovery includes tools that will help the user identify needed drivers not included in the default driver database, add those and other desired drivers into the driver database, and create a new custom Symantec Recovery Disk that includes these changes. The first is a utility called Driver Validation and the second is called the Customizable Recovery Disk Wizard.

A key new feature in Symantec System Recovery 2011 is the ability to create a customized Symantec Recovery Disk on bootable USB media. This is a non-destructive process, meaning that if the USB drive or key contains data already, this data is preserved. Using a USB device as your Symantec Recovery Disk media/device affords the user a number of advantages, such as:

- Performance: USB devices generally boot and run substantially faster than CD media, speeding up the recovery process
- Customization: USB devices are “writeable” allowing for additional utilities or tools to be stored on them
- Backup Storage + Recovery Media: Use a USB device as both your backup storage device as well as your recovery media; should you ever need to perform a recovery, there is no longer a need to hunt down your recover CD before you can begin – the device that contains your backups can also be used to restore them!

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

LightsOut Restore is another feature based upon the Symantec Recovery Disk. When installed, the LightsOut Restore feature copies the Symantec Recovery Disk to folder on the systems local hard disk and adds or updates the Windows boot manager. Essentially, the result is the Symantec Recovery Disk installed directly to the computer. When LightsOut Restore has been installed, each time the system boots the user is able to choose to either boot into Windows normally (default option; will timeout to this option) or boot into the embedded Symantec Recovery Environment. LightsOut Restore can also be remotely deployed using the Symantec System Recovery Management Solution, and enables the Symantec System Recovery Management Solution to perform remote, automated recoveries of managed systems.

SRD-enabled USB Drives

Using an SRD-enabled USB device as your recovery media instead of the default recovery CD offers the following advantages:

- Performance: USB devices generally boot and run substantially faster than CD media, speeding up the recovery process
- Customization: USB devices are “writeable” allowing for additional utilities or tools to be stored on them
- Backup Storage + Recovery Media: Use a USB device as both your backup storage device as well as your recovery media; should you ever need to perform a recovery, there is no longer a need to hunt down your recover CD before you can begin – the device that contains your backups can also be used to restore them!

Performance

Client computer performance during backup

System Recovery requires significant system resources to run a backup. If remote users are working at their computers when a backup starts, they might notice that the performance of their computer slows down. If slowing occurs, you can reduce the speed of the backup to improve client computer performance.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Indexing

Indexing is a resource-intensive operation that you should consider when planning for deployment. The indexing load will be at its peak while indexing base recovery point images, such as the first time a storage location is indexed, with a relatively smaller load when subsequent incremental recovery points are indexed. It is not feasible to provide precise guidance for the number of client machines that can be indexed by a single server, since the actual impact of indexing on a machine will vary based on the hardware configuration, the amount of data being indexed, and whether the data resides on local storage or a network share. However, until you can examine the actual performance in your specific installation, you should plan for indexing to take minutes for each base image and seconds for each incremental image.

Recovery point destination server

At the time you create the recovery point destination, it is recommended that you specify a location (a network share) other than the server where the Indexing Server is installed to reduce performance impact.

Compression

When you define a schedule for a backup job, you can choose the compression level for the recovery points. When a recovery point of a drive is created, compression results may vary, depending on the types of files on the drive.

The following compression options are available:

- None - This is the best choice if storage space is not an issue. However, if the recovery point is saved to a busy network drive, the use of high compression may be faster than no compression because less data needs to be written across the network.
- Standard (recommended) - (Default) Uses low compression for a 40% average data compression ratio on recovery points.
- Medium - Uses medium compression for a 45% average data compression ratio on recovery point files.
- High - Uses high compression for a 50% average data compression ratio on recovery point files. High compression is usually the slowest method.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

When a high compression recovery point is created, CPU usage may be higher than normal. Other processes on the computer may also be slower. To compensate, you can adjust the operation speed of the backup process. Speed adjustments may improve the performance of other resource intensive applications that you are running at the same time.

Best Practices before a backup

Schedule backups for a time when you know computers are turned on

Computers must be turned on and Windows must be running at the time a backup occurs. If the computer remains off after being polled six times, the computer is put into a "Needs attention" state. However, if System Recovery (with a user interface) is installed on the client computer, System Recovery asks the user if they want to run the missed backup (after the computer is turned on and they log on to Windows). In the meantime, the backup status of the client computer in the System Recovery Manager console is "Needs Attention".

Where possible, separate the operating system from the business data

This practice helps speed the creation of recovery points and reduces the amount of information that needs to be restored.

Use a network destination or a secondary hard disk on the client computer as the recovery point storage location

You should store recovery points to a network share or to a hard disk on the client computer other than the primary hard disk C. This practice helps ensure that you can recover the system in the event that the client's primary hard disk fails.

Use defined recovery point destinations

By defining recovery point destinations that are separated from backups and computers, you can easily see how many computers are backed up to a given location and optimize network load balancing during a backup.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Best Practices during a backup

Improve client computer performance during a backup.

System Recovery requires significant system resources to run a backup. If remote users are working at their computers when a backup starts, they might notice that the performance of their computer slows down. If slowing occurs, you can reduce the speed of the backup to improve client computer performance.

Best Practices after a backup

Maintain duplicate recovery points for safety.

Store recovery points on the network and create CDs, DVDs, or tapes of recovery points for storage off-site in a safe, secure place. Use Symantec Backup Exec for Windows Servers (not included in the Symantec Protection Suite Enterprise Edition) to back up recovery point locations on the network.

Verify that recovery points or recovery point sets are stable and usable.

- Where possible, document and test your entire recovery process by doing a restore of recovery points (using the System Recovery console) and single files (using the Recovery Point Browser in System Recovery Retrieve) on the original client computer where the recovery points were created. Doing so can uncover potential hardware or software problems.
- Enable the Verify recovery point after creation feature when you create a backup job.
- Use the Convert to Virtual feature to test and evaluate restored recovery points.

Manage storage space by deleting old backup data.

Delete incremental recovery points to reduce the number of files you have to maintain. This strategy also uses hard disk space more efficiently.

Review information in the Error Jobs dialog box and on the Home page.

Periodically review the contents and events in the Error Jobs dialog box and on the Home page to ensure stability in the computer system. You should also review log files periodically.

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

Review the contents of recovery points.

Ensure that you back up essential data by periodically reviewing the contents of recovery points files with Retrieve or the Recovery Point Browser in System Recovery.

Where to get more information

Resource	Location
Product Manuals	http://www.symantec.com/business/support/index?page=content&key=53847&channel=DOCUMENTATION&locale=en_us
BESR Community	http://www.symantec.com/connect/backup-and-archiving/forums/backup-exec-system-recovery

IT Analytics for Symantec Endpoint Protection

IT Analytics software enables users to maximize the value of the data that resides within the Symantec Management Platform by incorporating multidimensional analysis and robust graphical reporting features. This allows users to explore the Symantec Configuration Management Database without advanced knowledge of databases or third-party reporting tools, empowering them to ask and answer their own questions quickly, easily, and effectively.

System Requirements

Symantec Management Platform

- Notification Server 7.1
- Windows 2008 Server
- SQL Server 2008
- Internet Explorer 7
- .NET Framework 3.5
- Microsoft® Message Queuing Service

Additional Software Requirements

- Microsoft® SQL 2008 Database Engine (for Symantec CMDB databases)
- Microsoft® SQL Server 2008 Analysis Services (for IT Analytics Cube database)
- Microsoft® SQL Server 2008 Reporting Services (for IT Analytics Reports)

- Symantec Protection Suite 4.0 Enterprise Edition Best Practices

- ADOMD.NET installed on Notification Server

Reporting

Cube Reporting

Cube reporting is the most powerful capability in IT Analytics. All of the reports in the Pivot Table branch of the tool tree allows the user to build a report of graph from scratch by dragging and dropping the selection criteria from the Field list on to the Alerts cube. It's a easy to use mechanism to quickly mine Altiris history to discover and exploit information that might otherwise be missed.

Key performance indicators

Key performance indicators allow the management team to set specific performance criteria based upon any of the cube values and monitor progress on a daily basis.

Agent Population Dashboard

This dashboard provides the administrator a graphical breakdown of all the Symantec agents installed in the enterprise. It is used to view the breadth of agent coverage that exists and the types of agents that are reporting back to the management servers.

Event Monitoring

The event console is used to capture specific kinds of operational events and consolidate them into a single tool for better monitoring and management of the infrastructure. This new IT Analytics reports builds upon the Event Console in order to provide a high level graphical view of what's happening in the environment and what are the trends associated with those events.

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 Mountain View, 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
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec and the Symantec logo 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.

