Symantec™ Protection Suite Enterprise Edition 4.0

Getting Started Guide

Dec. 2012

CONTENTS

SPS Enterprise Edition 4.0 Getting Started Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

GETTING STARTED WITH SYMANTEC™ PROTECTION SUITE

This document is not intended to replace the point-product Getting Started Guides. Please see the "Where to get more information" section for further details.

This document includes the following topics:

ABOUT SYMANTEC PROTECTION SUITE ENTERPRISE EDITION

Symantec Protection Suite Enterprise Edition (SPS EE) 4.0 is powered by Symantec Insight and protects against today's complex malware, web and spam threats with the fastest, most-effective endpoint security, combined with industry-leading messaging protection and innovative Web security.

Powerful, centralized visibility and control of your Windows®, Mac® OS X and Linux® environments are achieved with Symantec™ Protection Center v2 enabling policy enforcement, consolidated reporting, and real-time intelligence.

Symantec™ Protection Suite Enterprise Edition's unparalleled combination of award-winning technologies from the world leader in security and data protection enables you to comprehensively protect, intelligently manage, and automatically control the assets most crucial to your business—while reducing upfront and on-going costs.

About the components included in Symantec Protection Suite Enterprise Edition

Symantec Protection Suite includes multiple layers of protection from the market-leading endpoint security, messaging and web security, and data and system recovery technologies.

Symantec™ Protection Suite eliminates environment complexity by deploying integrated essential endpoint and messaging security technologies as unified solutions with coordinated management. Automatic controls help you achieve, prove, and enforce adherence to IT policy and regulatory objectives with ease. You can also simplify implementation and operations by quickly deploying with minimal disruption to your environment through easy management and optimized utilization of system resources.

Centrally manage backup and recovery tasks for multiple desktops/laptops across your entire organization to insure business continuity in the event of system outages.

Protection Suite provides instant threat protection with support from the largest Global Intelligence Network in the world and comprehensive virus protection against malicious threats that target Windows®, Linux® and Macintosh® systems.

Table 1-1 describes the protection technologies included in SPS EE 4.0 and their benefits.

Table 1-1 – Protection Suite Components

SPS Component	Description	Benefit
Protection Center v2	Symantec Protection Center v2 is a centralized security management console that allows organizations to identify emerging threats, prioritize tasks and accelerate time to protection based on relevant, actionable intelligence.	■ Cross-product reporting including prebuilt reports that cover malware, email, and assets ■ The Global Intelligence Network monitors security events globally and provides early-warning alerts of attacks ■ Security, infrastructure, and global intelligence notifications are delivered via real-time, prioritized security news feeds ■ Prebuilt workflow templates allow out-of-the-box automation of common security processes

SPS Component	Description	Benefit
Endpoint Protection	Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, Mac and Linux computers, and servers in your network against malware. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your computers against known and unknown threats. This comprehensive solution protects confidential and valuable information by combining multiple layers of protection on a single integrated client. Symantec Endpoint Protection reduces management overhead, time, and cost by offering a single management console and a single client.	■ Virus and Spyware Protection detects new threats earlier and more accurately using not just signature-based and behavioral-based solutions, but the reputation-based security of Symantec Insight. ■ SONAR examines programs as they run, and identifies and stops malicious behavior of new and previously unknown threats. ■ A rules-based firewall engine shields Windows computers from malicious threats before they appear. ■ Intrusion Prevention scans network traffic and files for indications of attempted intrusions. ■ Browser Intrusion Prevention scans for attacks that are directed at Windows-based browser vulnerabilities. ■ Universal download protection monitors all downloads from the browser and validates that the downloads are not malware. ■ Application Control controls what applications are allowed to run or access system resources in a Windows environment. ■ Device Control manages the peripheral devices that users can attach to desktop computers. ■ Network Access Control and host integrity checking controls access to corporate networks and enforces endpoint security policy regardless of how endpoints connect to the network
Mail Security for Exchange and Domino	Symantec Mail Security provides real-time protection for email against viruses, spam, spyware, phishing, and other attacks while enforcing content policies. Powered by Brightmail technology, this email security software stops 99 percent of spam while making fewer than 1 false positive per million messages. It supports 64 bit and Virtualized server environments with easy installation and simple administration.	■ Protects against viruses, mass-mailer worms, Trojan horses, spam, spyware, phishing, and denial of service attacks ■ Stops 99 percent of spam while making fewer than 1 mistake per million messages. ■ Filters email content with pre-defined policies, regular expressions, attachment criteria and True File typing. ■ Management console provides centralized server group policy configuration, notifications, alerts, and reporting. ■ Integration with Microsoft Operations Manager and Systems Center v2 Operations Manager creates an email

SPS Component	Description	Benefit
		security software solution that enables end-to-end monitoring of your IT environment.
Messaging Gateway	Symantec Messaging Gateway 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. Defend your email perimeter, and quickly respond to new messaging threats with this market leading messaging security solution. Deploy Messaging Gateway as a virtual appliance or purchase a dedicated physical hardware appliance.	■ Detects spam, denial-of-service attacks, and other inbound email threats ■ Leverages a global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections ■ Filters email to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email ■ Protects sensitive client data and valuable confidential information, with the ability to fingerprint and identify actual company data within messages or attachments. ■ Obtains visibility into messaging trends and events with minimal administrative burden
Web Gateway	Symantec Web Gateway is an innovative Web security gateway appliance that protects organizations against Web threats, which include malicious URLs, spyware, botnets, viruses, and, other types of malware. Symantec Web Gateway provides controls for Web content and Internet applications. Backed by the Symantec™ Global Intelligence Network, Symantec Web Gateway is built on a scalable platform that quickly and simultaneously scans for malware and inappropriate Web content. Symantec Web Gateway helps organizations to maintain critical uptime and employee productivity by blocking attacks. Deploy Web Gateway as a virtual appliance or purchase a dedicated physical hardware appliance.	■ Fast protection at the Web gateway across multiple protocols for inbound and outbound web traffic ■ Protection against malware threats on all Web file transfer channels ■ Ability to inspect for, detect, and block active botnets ■ URL filtering with flexible policy controls and in-depth reporting (the URL filtering license is required) ■ Advanced application control capabilities with ability to monitor and control usage by end-users spanning multiple applications ■ Detection of compromised endpoints by network fingerprinting and behavioral modeling ■ Comprehensive Web reporting and alerting ■ Flexible policy controls, which allow policy creation on Web-based criteria and control over of how policies are applied across an organization ■ SSL-encrypted network traffic monitoring for URL content filtering, blacklisted-domain matching, and

SPS Component	Description	Benefit
		malware ■ Flexibility to deploy as an appliance or as a virtual machine on VMware ESX/ESXi 4.1/4.0
System Recovery Desktop Edition	Symantec System Recovery 2012 delivers fast and reliable system recovery to help you minimize downtime and meet recovery time objectives with confidence. Quickly restore Windows desktops/laptops in minutes, even to bare metal, dissimilar hardware, remote locations, or virtual environments. Symantec System Recovery is one of the most proven, trusted, and reliable system recovery solutions. The Optional System Recovery Management Solution allows you to manage machines in a one-to-many configuration, simplifying administration. Systems can still be managed one-to-one without the Management Solution.	■ Dramatically minimize downtime and avoid disruption and employee productivity losses. ■ Replace time-consuming, manual and error-prone desktop/laptop recovery processes with fast, reliable, automated system recovery. ■ Recover what you need, when and where you need it, including individual files, folders or complete systems in minutes. ■ Eliminate the need to have duplicate hardware on standby for recovery purposes and save on hardware costs. ■ Easily perform hardware refreshes and migrations. ■ Centrally manage backup and recovery tasks for multiple desktops/laptops across your entire organization
Network Access Control (Self – Enforcement)	Symantec Network Access Control 12.1 is a network security solution that controls access to corporate networks, enforces endpoint security policy and easily integrates with existing network infrastructures. Regardless of how endpoints connect to the network, Symantec's award-winning network security solution discovers and evaluates endpoint compliance status, provisions the appropriate network access and provides automated remediation capabilities.	■ Blocks or quarantines non-compliant devices from accessing the corporate network and resources. ■ Hosts Integrity tests against pre-defined templates such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the enterprise environment. ■ Provides a seamless integration with Symantec Endpoint Protection - both 11.x and 12.1. ■ Works with the optional Symantec Enforcer Appliance to enforce security policies for both managed and unmanaged endpoints. ■ Helps ensures endpoint compliance with security policies. ■ Regulates and protects guest access to the network. ■ Reduces risk of botnets, Advanced Persistent Threats and other malware. ■ Greater network availability and reduced disruption of

SPS Component	Description	Benefit
		services for end-users.
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. 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.	■ Cube Reporting allows the user to build a report or graph from scratch by dragging and dropping selection criteria to discover and exploit information that might otherwise be missed. ■ Key performance indicators (KPIs) allow the management team to set specific performance criteria based upon any of the cube values and monitor progress daily. ■ Agent Population Dashboard provides a graphical breakdown of all the Symantec agents installed in the enterprise to view the breadth of agent coverage and the types of agents that are reporting back to the management servers. ■ Event Monitoring console captures specific operational events and consolidate them into a single tool for better monitoring and management of the infrastructure to provide a high-level graphical view of the environment and trends.
Workflow	Symantec Workflow is a graphical .NET application development tool that provides advanced logic and workflow to the Symantec Management Platform and the solutions that integrate with the platform. You can use it to edit and implement pre-built workflows or build your own workflows. Workflow can be used to create an application that may or may not require human interaction. You can also design your applications to communicate with disparate technologies. The applications that you design can create human interaction through a variety of user interfaces. You can create human interaction through email, Web forms, handheld devices, or a task list.	■ Breaks down complexity of automation ■ Integrates across Symantec™ products ■ Builds on existing systems ■ Deliver automation quickly – no coding ■ Automate many IT and business tasks ■ Find inefficiencies and bottlenecks ■ Easy to use, easy to change workflows ■ Enforces the process

SYMANTEC PROTECTION SUITE 4.0 ENTERPRISE EDITION REFERENCE ARCHITECTURE

When fully deployed, Symantec Protection Suite Enterprise Edition provides coverage across multiple attack vectors in the network, including web (via Symantec Web Gateway), email for both Exchange and Domino (via Symantec Messaging Gateway and Symantec Mail Security), and endpoints (via Symantec Endpoint Protection, Symantec

Endpoint Protection for Mac, and Symantec Antivirus for Linux). Additionally, endpoint host integrity can be checked using Network Access Control Self-Enforcement and Windows desktops and laptops can be quickly recovered in the event of a critical system failure.

The solutions in Symantec Protection Suite 4.0 Enterprise Edition can be grouped into four categories:

Management and Reporting

- Symantec Protection Center v2
- IT Analytics for Symantec Endpoint Protection
- Symantec Workflow

Endpoint Security

- Symantec Endpoint Protection
- Symantec Network Access Control Self-Enforcement
- Symantec Endpoint Protection for Mac
- Symantec Antivirus for Linux

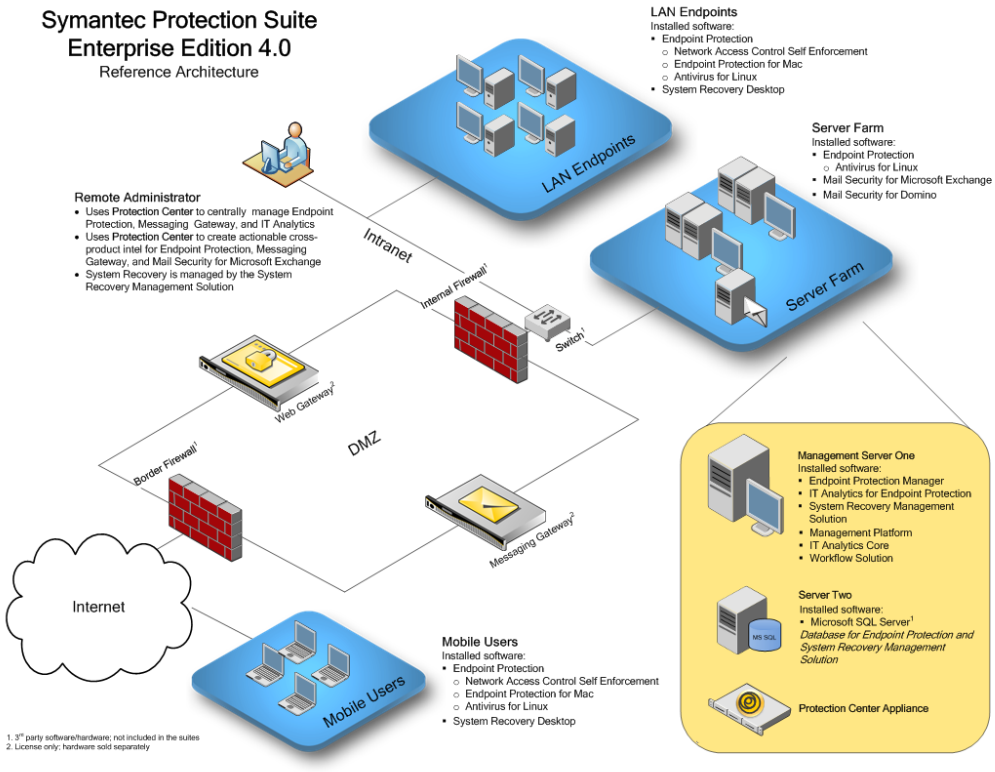
Messaging and Web Security

- Symantec Messaging Gateway software license
- Symantec Web Gateway software license
- Symantec Mail Security for Microsoft Exchange
- Symantec Mail Security for Domino

Backup and Recovery

- Symantec System Recovery Desktop Edition

Figure 1-1 Reference Architecture



GETTING STARTED WITH SPS EE 4.0

Before beginning the deployment of Symantec Protection Suite 4.0 Enterprise Edition you should assess your security requirements and prioritize the installation of critical technologies. In this section we will describe how to implement a total solution and take advantage of the full value that Symantec Protection Suite 4.0 Enterprise Edition provides.

For further details on any of the actions or descriptions listed below see the individual point-product Getting Started and Implementation/Installation guides.

Table 1-2 – Getting Started

Action	Description
Prerequisites Plan your Architecture	Make sure you have appropriate hardware resources for the Protection Suite technologies. ESX or ESXi are recommended for a full implementation of the Protection Suite technologies. ■ Protection Center v2 requires dedicated physical or virtual hardware (ESX/ESXi). ■ Messaging and Web Gateway can be deployed to virtual hardware (ESX/ESXi). ■ Mail Security for Exchange and Domino are installed to the respective mail servers. ■ IT Analytics for Symantec Endpoint Protection and the System Recovery Management Solution both use the Notification Server, which requires Windows 2008 Server. ■ While the Endpoint Protection Management server can use the default embedded database for a standalone solution, SQL server is required to implement IT Analytics and System Recovery Management Solution. For best performance use an off-host SQL server. *Please see the point product Getting Started and Implementation guides for complete system requirements.*

Security Management and Reporting Install the Security Management solutions and Endpoint Protection Manager	Install the security management technologies first to make sure you will be collecting all relevant information. The Protection Center v2 will only collect data from the time of installation on. No historical data will be collected from existing security solutions. ■ Install the Symantec Protection Center v2 to virtual hardware (larger environments may require physical hardware). Very few administrative actions can be performed directly from the SPC server. All administration will use a supported web browser from a networked computer. ■ Install the Symantec Endpoint Protection Manager. The SEPM server can be installed to a shared resource server but make sure the system requirements are appropriate for all server activities. ■ Install the Network Access Control Self-Enforcement Manager. This adds a section to the Endpoint Protection Manager and does not require a separate console. ■ Register the Endpoint Protection Manager with the Symantec Protection Center v2. ■ Install the Symantec Management Platform. The Notification Server is the main component of the Symantec Management Platform and is required for IT Analytics for Endpoint Protection and the System Recovery Management Solution. The Symantec Management Platform can also be used to simplify the agent rollout for Endpoint Protection by using the Symantec Endpoint Protection Integration Component (SEPIC).
Messaging and Web Security Install the Mail, Messaging and Web Gateway solutions	Install the gateway servers next to protect web and mail traffic at the network perimeter. ■ Install the Messaging Gateway to virtual hardware (ESX/ESXi). ■ Install the Web Gateway to virtual hardware (ESX/ESXi). ■ Install Mail Security to your existing Exchange or Domino mail server. Although the Messaging Gateway will catch inbound and outbound threats, installing protection to the mail server will catch threats between internal users as well as scan historical data already in the mail stores. ■ Register the Mail, Messaging and Gateway solutions with the Symantec Protection Center v2.

Security Configuration Configure policies	Identify any special requirements your organization may need. Although the default policies for the Protection Suite technologies are very robust and effective your environment may have unique requirements that are not covered in the default templates and policies. Try to minimize any unnecessary changes to simplify troubleshooting steps if required. ■ Endpoint Protection policies: client groups and locations, scanning exclusions for special file types or directories, communication settings, etc. ■ Messaging Gateway: Scan inbound and outbound, unique IP addresses for better performance, configure regular backups and updates, etc. ■ Mail Security: Endpoint Protection exclusions, thread tuning, etc. ■ Web Gateway: enable application control, content filter, bypass whitelist modules, policy precedence order, etc.
Backup & Recovery Install the System Recovery Management Solution	Installing the System Recovery Management Solution has a number of benefits. It allows you to run a Discovery to identify endpoints on your network (including virtual systems). It also allows you to centrally manage your endpoints to simplify configuration and administration. Note that only status and configuration data is exchanged between the Management Solution and endpoints. Backup data gets written directly to storage and doesn't travel through the Management Solution. System Recovery Management Solution requires the Symantec Management Platform.
Client Deployment & Configuration Discover clients and deploy the System Recovery agents	After the Management Platform has been installed, run a discovery to identify endpoints on the network. ■ Deploy the Symantec Management Agent (SMA) to the desired target systems. ■ Deploy the System Recovery Agent. This can be installed in either full or "headless" mode (no local UI).
Configure System Recovery storage and backup policies	■ Identify the storage locations for your endpoint backups. Storage locations can be local (directly attached to the endpoint) or on a network resource that the endpoint can access. Performance will depend on transfer rates of the network or hardware devices. Backups can be password protected and backup data can be compressed. Note that compression levels may affect backup performance. ■ Backup policies can be configured to perform a full with incremental to reduce the amount of time that subsequent backups will take.
Perform a full endpoint backup	■ Having a full endpoint backup can simplify troubleshooting or recovery in the case of failures during client agent implementation or migration. ■ Create and test the Symantec Recovery Disk to ensure you can perform a system recovery if necessary.

Endpoint Security Deploy the Endpoint Protection Agent	■ Once the systems have been backed up deploy the Endpoint Protection Agent. The SEP agent can be deployed in a number of ways but one of the most flexible is to use the Symantec Endpoint Protection Integration Component with the Symantec Management Platform. This allows you to identify and group endpoints and to perform additional steps during the install. For instance, in organizations where an existing security solution or antivirus technology is already installed, the SEPIC can be used to run uninstall scripts of the older technologies before installing the SEP agent. This reduces potential risk of failed upgrades. *See the Endpoint Protection Implementation Guide for other deployment options.*
Update definitions and run a full system scan on the endpoints	■ Run a full system scan on the endpoints with the latest virus definitions to identify any threats that may be dormant on the endpoint. This can be a manual or scheduled scan that is defined in the SEP protection policies.
Expanded Reporting on trends/Key Performance Indicators Install IT Analytics for Symantec Endpoint Protection	■ Now that the endpoints are reporting to the Endpoint Protection Manager, install ITA for SEP. ITA for SEP requires SQL to be configure with Analysis and Reporting Services for the IT Analytics Cube database and Reports.
Security Automation Install Workflow server	■ Install Workflow to enable process automation. See the Workflow SWAT resource page at http://www.workflowswat.com to learn more about tying solutions together using Symantec Workflow.
Security Administration Use the Protection Center v2 for ongoing security administration	■ The Symantec Protection Center v2 allows for centralized security management and provides the ability to identify emerging threats across local and global environments. Protection Center v2 also allows you to prioritize security information based on user roles and to accelerate time to protection with relevant, actionable intelligence.

WHERE TO GET MORE INFORMATION

Your first stop for the Protection Suites once you receive your licensing information should be fileconnect.symantec.com. Full product documentation for each point product is available for download along with the installation media.

The individual point-products also include several sources of information. The primary documentation is available in the Documentation folder on the product disc.

Updates to the documentation are available from the Symantec Technical Support Web site at http://www.symantec.com/business/support

The Protection Suites include the following point product documentation:

- *Implementation and Installation Guides*

  These guides include procedures to install, configure, and manage the product.

- *Client and User Guides*

  These guides include procedures for users to use and configure client software.

- *Schema Reference (where available)*

  These guides include the database schema for solutions that use databases.

- *Migration Guides*

  These guides explain how to migrate from previous versions.

- *Online Help*

  Online Help systems contain the information that is in the guides plus context-specific content.

Document Locations

Symantec Protection Center v2

http://www.symantec.com/business/support/index?page=landing&key=60247

Symantec Endpoint Protection

http://www.symantec.com/business/support/index?page=landing&key=54619

Symantec Messaging Gateway

http://www.symantec.com/business/support/index?page=content&key=53991&channel=DOCUMENTATION&locale=en_us

Symantec Web Gateway

http://www.symantec.com/business/support/index?page=landing&key=58161

Symantec Mail Security for Exchange

http://www.symantec.com/business/support/index?page=landing&key=51980

Symantec Mail Security for Domino

http://www.symantec.com/business/support/index?page=landing&key=51977

Symantec System Recovery Desktop Edition

http://www.symantec.com/business/support/index?page=landing&key=53847

IT Analytics
http://www.symantec.com/business/support/index?page=landing&key=56005

To provide feedback on SPS EE 4.0 or this document please visit:

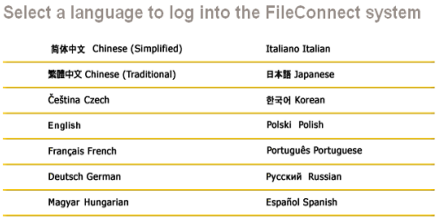
Symantec Connect SPS Forums
https://www-secure.symantec.com/connect/security/forums/symantec-protection-suites-sps

Symantec Ideas
https://www-secure.symantec.com/connect/security/ideas

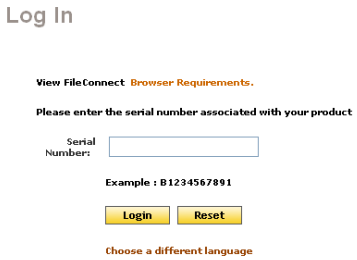
ACCESSING THE SUITE SOFTWARE

Symantec™ uses the FileConnect website at *https://fileconnect.symantec.com*, which allows customers to download electronic media. FileConnect also provides the ability to request physical media.

1. Upon navigating to FileConnect you will be prompted to choose your language.



2. Next you will be prompted to log in.



3. Enter your product serial number. The serial number will be located on the certificate you received from Symantec.
4. Read and agree to the terms of the end user license agreement.

5. The most up-to-date full build Maintenance Releases are available from this site.
6. Select the product suite and language you wish to download
   Two download methods are available:

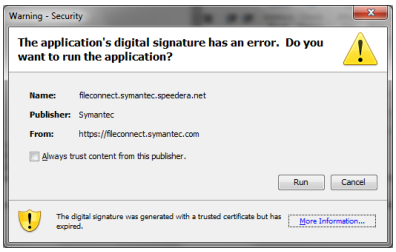
   HTTP Download:

   Although the HTTP download allows one file to be selected for download at a time, it is a browser controlled download, and as such does not use the Java Runtime Environment or require the installation of any applets on your computer. The HTTP download uses HTTP 1.1 allowing browsers to resume an interrupted download in most cases. This method does, however, require that cookies be enabled, to transmit an encrypted hash code to the download server. Without this code, your download will fail.

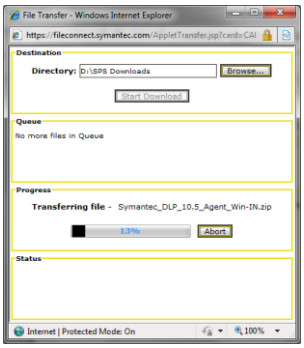
   Managed FTP Download:

If you wish to begin downloading multiple files at the same time, this method allows you to select as many files as you wish, begin the download, and go on to other areas of business. The process requires that a Java Applet be installed on your machine that manages the download process, so that when one file completes its download, the next in the queue is initiated. It also allows for the use of the "Resume Downloads" feature on the web site. We recommend the use of the Java Runtime Environment (JRE) version 1.4.2, as there is a bug, documented on the Sun site, between Verisign certificates and certain other versions of the JRE. This bug will still allow the download, but a warning will appear stating that it is not a trusted source.

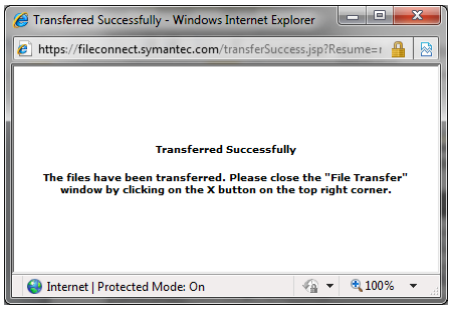
7. Select the Suite components you wish to download. If you chose “Managed Download” you will be able to select multiple options, if you chose “HTTP Download” you can only choose one option at a time.
8. When you have made your choice, click “Begin Downloading”
9. If you have chosen components which either have dependencies or multiple components, you will be prompted to add them to your download
10. If you wish to download further components, you can choose them here. Once again, if you chose the Managed download, you can select multiple options. If you chose HTTP Download, you will only be able to choose one option at a time.
11. Once you have made your choices, click Continue Downloading.
12. If you chose HTTP Download, then your browser will prompt you for a location to save the download file.
13. If you chose Managed Download, the download manager will launch. You may be prompted with security prompts; you will need to accept these to continue.



14. Once the download manager has launched, you click Browse and specify a location to save the downloads. Then click Start Download – your download progress will be shown.



15. Once the download has completed, you will see the screen below. At this point, you may close your browser and start installation of the suite products


Transferred Successfully - Windows Internet Explorer
https://fileconnect.symantec.com/transferSuccess.jsp?Resume=
Transferred Successfully
The files have been transferred. Please close the "File Transfer" window by clicking on the X button on the top right corner.
Internet | Protected Mode: On
100%

This document may include information about pre-release software. Any unreleased update to the product or other planned modification is subject to ongoing evaluation by Symantec and therefore subject to change. This information is provided without warranty of any kind, express or implied. Customers who purchase Symantec products should make their purchase decision based upon features that are currently available.

About Symantec
Symantec is a global leader in providing security; storage and systems solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in more than 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
www.symantec.com