

**F-Secure® Protection Service™
for Business (PSB)
White Paper**

1. About This Document	3
2. Introduction	4
3. F-Secure Protection Service for Business	7
Security Software Components	8
Virus and Spy Protection	8
Internet Shield	8
Spam Control	8
Anti-Virus and Spam Control for Microsoft Exchange	8
Subscription Management	9
Automatic Updates	9
4. F-Secure Protection Service for Business Portal	10
License Management	10
Support for Several Users Types	10
Status of Network, Individual Computers and Installed Components	13
Security Profiles	13
5. System Requirements	16
Supported Operating Systems	16
Supported Browsers	18
A. Security Profile Configuration	19

1 About This Document

This document is intended for F-Secure partners and their small business customers. It provides an overview of F-Secure® Protection Service™ for Business security service solution.

2 Introduction

F-Secure Protection Service for Business (PSB) is a security solution that allows F-Secure partners to sell security services to their small business customers. It consists of four main components:

- F-Secure PSB Workstation Security
 - To protect desktops and laptops
- F-Secure PSB Server Security
 - To protect Microsoft Windows file servers
- F-Secure PSB E-mail and Server Security
 - To protect Microsoft Exchange servers
- F-Secure PSB Portal
 - To enable remote management and reporting of the network

F-Secure hosts and manages F-Secure Protection Service for Business which is available in two different options, standard and advanced.

In F-Secure Protection Service for Business –standard, F-Secure:

- provides Protection Service for Business online portal and security software for workstations, file servers and Microsoft Exchange servers for the small business customer
- provides automatic security updates, hotfixes, version upgrades and security news
- maintain the management portal and client software up to date for the latest security threats

In F-Secure Protection Service for Business –advanced, F-Secure:

- provides Protection Service for Business online portal and security software for workstations, file servers and Microsoft Exchange servers for the solution provider who offers the solution as a service
- provides automatic security updates, hotfixes, version upgrades and security news
- maintain the management portal and client software up to date for the latest security threats

In F-Secure Protection Service for Business –advanced, Solution provider:

- provides a turnkey security as a service solution to SMB customers
- manages direct customer relationship such as 1st level support, billing, service orders and subscription management
- is able to provide value added services like security audit, installations, security status reports and alarm management



Figure 1: F-Secure Protection Service for Business –standard security service solution

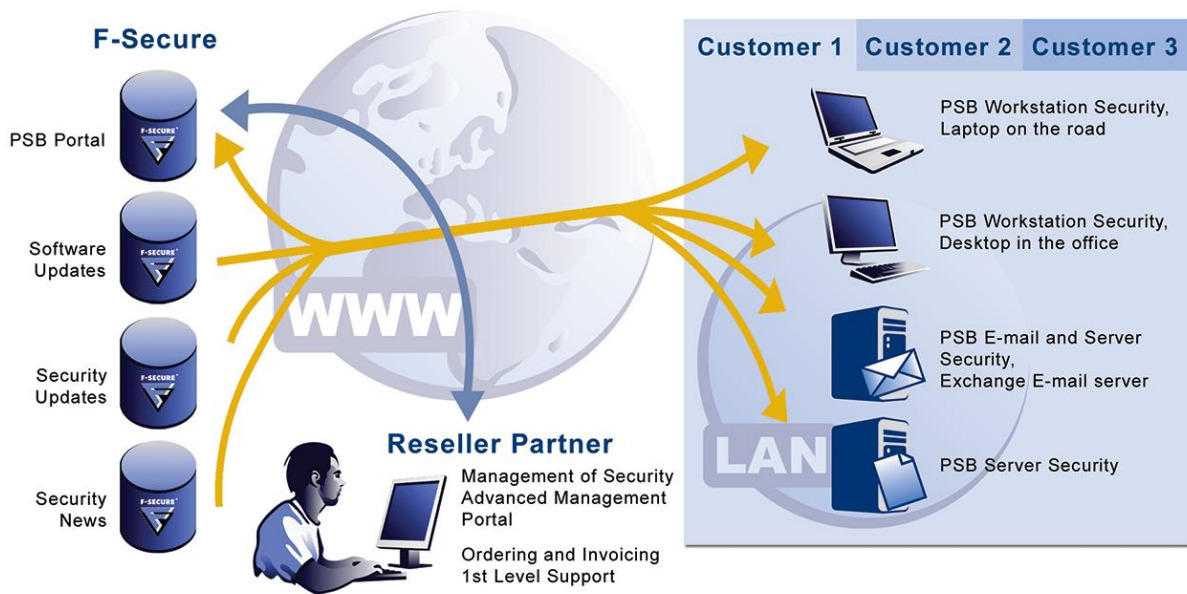


Figure 2: F-Secure Protection Service for Business –advanced security service solution

Terms and definitions

The following briefly defines the key terms used in this document.

Term	Definition
Solution Provider	F-Secure reseller partner
Service Partner	An internal or external sales channel associated with a particular solution provider
SMB	A Small and Medium Business -customer of a solution provider
MSP/VAR	Managed solution provider
Administrator	A company administrator of a SMB who subscribes and manages the service in the corporate network.
End user	An employee of a SMB who uses the client security software
F-Secure PSB Portal	F-Secure hosted web-based online management system for workstation and server security software provisioning, reporting, and management.
F-Secure PSB Workstation Security	Client security software for workstations
F-Secure PSB Server Security	Client security software for file servers
F-Secure PSB E-mail and Server Security	Security software for file servers and mail servers (MS Exchange)

3 F-Secure Protection Service for Business

F-Secure Protection Service for Business can be deployed on both workstations and servers. The product is available in three different modules:

- F-Secure PSB Workstation Security for Windows desktops and laptops
- F-Secure PSB Server Security for Microsoft Windows file servers
- F-Secure PSB E-mail and Server Security for Microsoft Exchange server

Comparison between the modules and descriptions of the security components can be viewed below

	F-Secure PSB Workstation Security	F-Secure PSB Server Security	F-Secure PSB E-mail and Server Security
Virus and Spy Protection	X	X	X
Internet Shield	X	-	-
Spam Control	X	-	X

Security Software Components

Virus and Spy Protection

Virus and Spy Protection detects and stops malware that can attack computer by e-mail, through removable media, or when content is downloaded from the Internet. It protects the privacy by removing secretly installed data tracking software from the computer. Virus and Spy Protection:

- quarantines and removes malware already installed on the computer,
- protects system settings, and
- detects riskware and quarantines or removes it.

Virus and Spy Protection also includes F-Secure DeepGuard 2.0 (Workstation Security): a new in-the-cloud technology that protects all F-Secure users in 60 seconds from the first confirmation of a new threat, and F-Secure Blacklight (Workstation Security, Server Security), a technology against concealed rootkits.

F-Secure Anti-Virus research lab publishes and updates virus definitions more frequently than any other vendor in the market. The users receive the latest virus definition and spyware database updates automatically.

Internet Shield

Internet Shield protects computer against unauthorized connection attempts, insider attacks and information theft, malicious applications, and other unwanted applications, such as peer-to-peer software. Firewall is an important part of Internet Shield. When Internet Shield is installed on the computer, firewall protection is enabled even when the computer is not connected to the corporate local area network (LAN). When an Internet connection is activated, the firewall software is automatically updated.

Spam Control

E-mail filtering monitors incoming e-mails and removes unsolicited e-mails (spam and phishing) from the e-mail inbox. Once an e-mail is identified as spam or phishing, it is tagged and filtered to a separate spam folder.

Anti-Virus and Spam Control for Microsoft Exchange

PSB E-mail and Server Security protects Microsoft Exchange servers from viruses, worms and Trojans, scanning both incoming and outgoing messages. The product scans not only e-mail attachments, but it also stops viruses in documents and notes posted to public folders. With E-mail and Server Security, antivirus protection is transparent and always on as the scanning is done on the e-mail server in real-time. In addition to virus protection, the solution provides spam filtering and other content filtering functionality.

Subscription Management

Each managed client software type has its own subscription with independent validity period and size. Every SMB-customer gets one or more unique subscription keys - depending of which client applications are purchased. Each subscription key defines how many instances of the client software can be installed and a fixed validity period. Every time the client security software connects to check for updates, the corresponding subscription is checked for validity and all updates are provided for the valid client.

Automatic Updates

F-Secure hosts and maintains the update service of the client security software. When a computer with the client security software connects to the Internet, the client software connects the update service and checks for updates and possible changes in product configurations. Virus signature updates, security hotfixes, version upgrades, and updated security profiles are all downloaded and taken into use fully automatically.

Download control: When open-profile is in use, end user is able to switch off automatic updates. This can be done in a situation where low bandwidth connection, like GPRS, is the only option.

4 F-Secure Protection Service for Business Portal

The F-Secure Protection Service for Business Portal is a web-based software provisioning and security management system for Solution Providers, Service Partners and SMB administrators. It allows continuous follow-up of the computer network security, and enables administrators to take required action to help SMB end users when security problems are detected.

Through the portal, it is possible to monitor both the overall network security and the security status of individual PCs in the network. Administrator can assign each managed computer a suitable F-Secure predefined security profile. It is also possible to edit the predefined profiles or create new customized ones.

The portal allows small business customer administrators to view trend reports on:

- the overall protection status on a given period
- the number of scanned and blocked viruses and potentially malicious network connections
- the status of updates

License Management

PSB Portal offers a combined view to the subscription status of the whole customer base – with notifications when some specific subscriptions require a renewal. A Solution Provider can order new subscriptions, extend the subscription size, or extend the validity period through the portal. All administrators can track subscription usage, and remove legacy computers from the management in order to free licenses for reuse.

Support for Several Users Types

The F-Secure Protection Service for Business portal supports the following user types:

F-Secure: F-Secure creates subscription keys, manages and maintains the F-Secure Protection Service for Business hosted service.

Solution Provider: If you are a solution provider, your sales or technical support personnel, or administrative staff can search for subscribers and change their information, and add users to subscriber accounts. You can manage your customer subscriptions by creating new keys or extending the existing ones.

Service Partner: If you are a partner of a solution provider, for example, a reseller, you can search for subscribers associated with you and change their information, and add users to subscriber accounts.

Company Administrator: Small business customer administrators, who manage their own computer network through the portal can monitor the security status of the corporate network, and enforce security profiles on workstations. You can assign some remote commands and even remove computers from the subscription.

The following table shows the functionalities that are available for different users:

Available functionalities for:	F-Secure	SP	Partner	SMB
System administration				
SP account and user management	X	X		
Partner account and user management	X	X	X	
SMB account and user management	X	X	X	X
Removal of computers	X	X	X	X
Subscription key creation/management	X	X		
Automatic client upgrades from F-Secure				X
Web-based management	X	X	X	X
Security administration				
Online monitoring of security status of computers	X	X	X	X
Assigning of security profiles	X	X	X	X
Creation/editing/deletion of Security Profiles	X	X	X	X
Automatic definition updates from F-Secure				X
Reporting				
On-line portal report: Overall host protection	X	X	X	X

Available functionalities for:	F-Secure	SP	Partner	SMB
On-line portal report: Anti-Virus protection	X	X	X	X
On-line portal report: Firewall protection	X	X	X	X
On-line portal report: Product installations	X	X	X	
On-line portal report: License usage	X	X	X	
Information feeds				
Portal: Mobile threats information	X	X	X	X
Client: Security News				X
Documentation				
On-line help				X
Context sensitive on-line help	X	X	X	X
Portal Getting Started Guide		X	X	X
Customization (Only for ISP's with dedicated systems)				
Client software customization				X
Portal customization		X	X	X
Integration to other systems				
Overall protection status as RSS feed		X	X	X
Web Services API (Only for ISP's with dedicated systems)		X		

Status of Network, Individual Computers and Installed Components

The F-Secure Protection Service for Business portal gives SMB customers' administrators access to critical security information about their corporate network. The portal provides in-depth information about individual computers in the network, and status information on the installed security services, such as anti-spyware, e-mail scanning, real-time scanning, and firewall. Based on the information, the administrators can quickly assess the security status of the corporate network and pro-actively solve possible risks before they become critical.

Security Profiles

The portal has predefined security profiles for desktops, laptops and servers. The profiles are created as a result of thorough research by F-Secure on the current software security threats. The profiles give users a certain level of rights for adjusting their own security settings.

You can create new profiles or edit existing ones. Your SMB customers assign different profiles to workstations in their corporate network and control what the end users are able to do with the security settings on their computers.

The following profiles predefined by F-Secure are currently available:

- **Office open:** for accessing the Internet from a fixed location, such as office premises; end users are allowed to change security settings
- Office locked:** for accessing the Internet from a fixed location, such as office premises; end users are not allowed to change security settings
- Laptop open:** for connecting to networks outside office premises; end users are allowed to change security settings. The 'Mobile' setting is for laptops that access the Internet from unsafe locations, for example, from conferences or from home, and that are not protected by the corporate firewall
- Laptop locked:** for connecting to networks outside office premises; end users are not allowed to change security settings. The 'Mobile' setting is for laptops that access the Internet from unsafe locations, for example, from conferences or from home, and that are not protected by the corporate firewall
- Server:** only for servers; for accessing the Internet from a fixed location, such as office premises; end users are allowed to change security settings
- Office open with neighborcast:** for accessing the Internet from a fixed location, such as office premises; enables workstations within the same local area network (LAN) to share F-Secure database updates; end users are allowed to change security settings
- Office locked with neighborcast:** for accessing the Internet from a fixed location, such as office premises; enables workstations within the same local area network (LAN) to share F-Secure database updates; end users are not allowed to change security settings

The following shows the available settings for each profile:

		Profiles						
		Office open	Office locked	Laptop open	Laptop locked	Server	Office open with Neighborcast	Office locked with Neighborcast
Virus and Spy Protection settings								
	High	x	-	x	-	x	X	-
	Normal (default)	x	x	x	x	x	X	x
	Off	x	-	x	-	x	X	-
	Custom	x	-	x	-	x	X	-
Internet Shield settings								
	Block All	x	-	x	-	N/A	X	-
	Mobile	-	-	x	x	N/A	-	-
	Office (default)	x	x	x	x	N/A	X	x
	Office, Printer/File sharing	x	-	x	-	N/A	X	-
	Allow All	x	-	x	-	N/A	X	-
Changing of critical security settings allowed		x	-	x	-	x		-

Virus & Spy Protection settings:

- High** - The highest level of protection; may slow down the system performance considerably.
 NOTE: Some of the critical security settings, such as real-time scanning, disabling updates or firewall, cannot be changed at this security level.
- Normal** - (default) The recommended level; protects the computer against malware with the minimal effect on the system performance.
 NOTE: Some of the critical security settings, such as real-time scanning, disabling updates or firewall, cannot be changed at this security level.
- Off** - Turns off Virus&Spy Protection.
 WARNING: When Virus&Spy Protection is turned off and you connect to the Internet or access

your e-mails or files on different media, your computer is vulnerable to viruses, worms and other malicious code.

- **Custom** - Allows configuration of advanced settings, including critical security settings; recommended for advanced users only.

Internet Shield settings:

- **Block All** - Blocks all traffic to and from the Internet.
- **Mobile** - Allows normal web browsing, file retrievals (HTTP, HTTPS, FTP), e-mail and Usenet news traffic, and encryption programs, such as VPN and SSH. Everything else is denied. The denied inbound TCP traffic generates alerts. Local rules can be added after the malware probes detection.
- **Office** – For use in office environment. With this setting, an external firewall is required to protect the network from hackers.
- **Office Printer/File Sharing** – For use in protected office networks only; allows a computer to share files or printers or both with other computers in the same office (Local Area Network). Recommended only for computers that must share files or printers.
NOTE: If you are trying to access files or printers in another computer, you do not need to choose this security level.
- **Allow All** - Allow all traffic to and from the Internet.
NOTE: When 'Allow All' is selected, the computer may become a target for attacks. Do not activate this setting when you are connected to the Internet.

5 System Requirements

Supported Operating Systems

F-Secure Protection Service for Business supports the following operating systems:

- Windows 2000 Professional SP4 and newer
- Windows XP 32-bit: Home, Professional and Media Center editions. All Service Packs
- Windows Vista 32-bit and 64-bit: Starter, Home Basic, Home Premium, Business, Ultimate, Enterprise. All Service Packs
- Windows 2000 Server, Windows Server 2003 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit) (PSB Server Security only)
- Windows Small Business Server 2003 32-bit
- Microsoft Exchange Server 2003
- SQL servers (for quarantine database in E-mail and Server Security):
 - Microsoft SQL Server 2005 (Enterprise, Standard, Workgroup or Express edition) - recommended
 - Microsoft SQL Server 2000 (Enterprise, Standard or Workgroup edition) with Service Pack 4
 - Microsoft SQL Server 2000 Desktop Engine (MSDE) with Service Pack 4

System Requirements

Your computer must meet the following requirements for installing and running the F-Secure Protection Service for Business client security software:

PSB Workstation Security

Minimum (Vista)

- Processor: Capable of running Microsoft Vista 32bit
- Memory: 512MB
- Operating System: Microsoft Vista RTM versions
- Disk space: 600MB free HD space (300 MB for Anti-virus only)
- Display: 16-bit or more (65000 colors)
- Internet Connection: An Internet connection is required in order to validate your subscription and receive updates

- Browser: Internet Explorer 7.0 or newer is required

Recommended (Vista)

- Processor: Intel Pentium 4 2GHz or higher
- Memory: 1GB or more
- Disk space: 800MB free HD space (500 MB for Anti-virus only)
- Display: 16-bit or more (65000 colors)
- Internet Connection: An Internet connection is required in order to validate your subscription and receive updates
- Browser: Internet Explorer 7.0 or newer

Minimum (Windows 2000 and Windows XP)

- Processor: Intel Pentium III 600Mhz or higher
- Memory: 256MB
- Operating System: Microsoft Windows 2000 SP4 or Microsoft Windows XP
- Disk space: 600MB free HD space (300 MB for Anti-virus only)
- Display: Min. 8-bit (256 colors)
- Internet Connection: An Internet connection is required in order to validate your subscription and receive updates
- Browser: Internet Explorer 5.0 or newer is required

Recommended (Windows 2000 and Windows XP)

- Processor: Intel Pentium III 1Gz or higher
- Memory: 512MB or more
- Operating System: Microsoft Windows 2000 SP4 Update Rollup 1 or Microsoft Windows XP SP2
- Disk space: 800MB free HD space (500 MB for Anti-virus only)
- Display: 16-bit or more (65000 colors)
- Internet Connection: An Internet connection is required in order to validate your subscription and receive updates
- Browser: Internet Explorer 6.0 or newer

PSB Server Security

Minimum hardware

- Processor: Intel Pentium III 800Mhz or higher
- Memory: 512 MB
- Disk space: 300MB free HD space

Recommended hardware

- Processor: Intel Pentium III 2Gz or higher
- Memory: 1 GB
- Disk space: 800MB free HD space

PSB E-mail and Server Security

Recommended hardware

- Processor: Intel Pentium 4 2GHz or higher
- Memory: 1 GB of RAM
- Disk space to install: 260 MB free hard disk space
- Disk space for processing: 10 GB or more free hard disk space
- Note: The required disk space depends on the number of mailboxes, amount of data traffic, and the size of the Information Store.

Note: The minimum requirements are for system that only has clean operating system installation with standard software (web browser, email, etc.) installed.

Supported Browsers

The F-Secure Protection Service for Business portal supports the following Web browsers:

- Internet Explorer 6.x or newer
- Firefox 1.5 or newer

NOTE: JavaScript and cookies must be enabled in the browser

A. Security Profile Configuration

The following table shows available security profiles and their settings.

Profiles								
	Office open	Office locked	Laptop open	Laptop locked	Server	Office open with Neighborcast	Office locked with Neighborcast	
General								
users allowed to unload product	yes	no	Yes	no		yes	no	
Virus and Spy Protection security levels								
users allowed to override any settings	yes	critical settings locked	Yes			yes	critical settings locked	
High	X	-	X				-	
Normal (enabled by default)	X	X (enabled and locked)	X				X (enabled and locked)	
Off	X	-	X				-	
Custom	x	-	X				-	
Real-time scanning default settings								
Scan defined file types	enabled	enabled (locked)					enabled (locked)	
scan inside compressed files	disabled	disabled (locked)				disabled	disabled (locked)	
excluded applications, objects and file types	-	disabled (locked)					disabled (locked)	
action when virus is found	ask what to do	ask what to do				ask what to do	ask what to do	
action when spyware is found	ask what to do	ask what to do				ask what to do	ask what to do	
Email scanning default settings								
Scan incoming and outgoing mail	enabled	enabled (locked)				enabled	enabled (locked)	
Email scanning default settings (cont'd)								
Scan defined file types (locked)	enabled	enabled (locked)					enabled (locked)	

		Profiles						
		Office open	Office locked	Laptop open	Laptop locked	Server	Office open with Neighborcast	Office locked with Neighborcast
scan inside compressed files (locked)	enabled	enabled (locked)					enabled	enabled (locked)
excluded objects	-	disabled (locked)						disabled (locked)
action on incoming infected files	disinfect	disinfect					disinfect	disinfect
action on incoming malformed message parts	remove	remove					remove	remove
on outgoing infected files and malformed message parts	block	block					block	block
Scheduled scanning	disabled	disabled					disabled	disabled
Manual scanning default settings								
Scan defined file types	enabled	enabled					enabled	enabled
scan inside compressed files	enabled	enabled					enabled	enabled
action when virus is found	ask what to do	ask what to do					ask what to do	ask what to do
action when spyware is found	ask what to do	ask what to do					ask what to do	ask what to do
System Control	enabled	enabled					enabled	enabled
Internet Shield default settings								
users allowed to override any settings	yes	critical settings locked					yes	critical settings locked
Internet Shield default settings (cont'd)								
Block All		-						-
Mobile		-						-
Office (default)		(locked)						(locked)

		Profiles						
		Office open	Office locked	Laptop open	Laptop locked	Server	Office open with Neighborcast	Office locked with Neighborcast
	Office, Printer/File sharing		-					-
	Allow All		-					-
	Firewall engine	enabled	enabled (locked)				enabled	enabled (locked)
	users can own rules	-	No (locked)					No (locked)
	trusted network adapter	-	disabled (locked)					disabled (locked)
	Application control	enabled and in prompt mode	enabled and in prompt mode (engine locked, mode not)				enabled and in prompt mode	enabled and in prompt mode (engine locked, mode not)
	Intrusion prevention	enabled and in block and log mode	enabled and in block and log mode (locked)				enabled and in block and log mode	enabled and in block and log mode (locked)
	Dial-up control	enabled	enabled				enabled	enabled
Spam Control default settings								
	users allowed to override any settings	yes	yes				yes	yes
	Spam control	enabled	enabled				enabled	enabled
	Filter mode	medium	medium				medium	medium
	RBL scanning	enabled	enabled				enabled	enabled
Automatic Updates default settings								
	users allowed to override any settings	yes	critical settings locked				yes	critical settings locked
	Automatic updates	enabled	enabled (locked)				enabled	enabled (locked)
	Neighborcast	-	-				enabled	enabled