The logo features the text "F-SECURE" in a bold, sans-serif font above a stylized shield icon. The shield is composed of three overlapping, semi-transparent shapes that form a triangular pattern. The background of the logo is a circular, glowing effect with a radial gradient from yellow to blue.

***F-Secure Anti-Virus:
Functionality, Centralized
Policy-Based Management,
and Integration with EMS
Systems***

F-Secure Corporation

Securing the Mobile Distributed Enterprise

**WHITE PAPER
APRIL 2000**

F-Secure Anti-Virus: Functionality, Centralized Policy-Based Management, and Integration with EMS Systems

White Paper March 2000

All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure™ Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

The purpose of this document is to help you identify the strengths of the integrated security solutions the F-Secure product line provides. It is not a comparative review of competitor's products but it may provide valuable information that will assist you see what makes our offering different from all the others.

<p><i>USA</i></p> <p><i>F-Secure Inc.</i> 675 N. First Street, 5th floor San Jose, CA 95112, USA Tel (408) 938 6700 Fax (408) 938 6701 http://www.F-Secure.com/</p>	<p><i>Europe</i></p> <p><i>F-Secure Corporation</i> PL 24 FIN-02231 Espoo, Finland Tel +358 9 859 900 Fax +358 9 8599 0599 http://www.F-Secure.com/</p>
---	--

Copyright © 1995-2000 F-Secure Corporation. All rights reserved.

Contents

1. Executive Summary	1
2. Solution Overview	1
2.1 Introduction.....	1
2.2 Platform Support.....	6
2.3 Services	9
3. Centralized Policy-Based Management	9
3.1 Software Distribution.....	10
3.2 Alerts and Reports.....	11
3.3 Policies.....	12
3.4 Security of the Centralized Management Solution.....	14
4.0 Integration with IBM Tivoli TME 10.....	15
4.1 Tasks.....	16
4.2 File Packages.....	16
4.3 Monitors	16
4.4 Events, Event Adapter, and Rules	17
5. Integration with Microsoft Systems Management Server	17
5.1 Software Distribution.....	17

1. Executive Summary

F-Secure Anti-Virus 5 is the next-generation version of the award-winning F-Secure Anti-Virus 4 and F-PROT products, which have been on the market for more than eight years. F-Secure Anti-Virus equips you to manage virus protection over a whole network, centrally, from the F-Secure Administrator management console. The centralized management functionality includes software distribution, virus signature database updates, security policy enforcement, alerting, statistics, and reporting.

F-Secure Anti-Virus will work with networks of any size or shape, even multiple platforms, composed of Windows 95, 98, NT 4.0 workstations and servers. The F-Secure Anti-Virus product family also covers platforms like Linux, Solaris x86, NetWare, Windows NT 3.51, OS/2 and Windows 3.1. Windows 2000 will be supported and pre-release versions of F-Secure Anti-Virus for Windows 2000 are already available for customer evaluation.

F-Secure Anti-Virus for Firewalls scans traffic traveling through Check Point FireWall-1 and other CVP-compliant firewalls. F-Secure Anti-Virus for Microsoft Exchange and F-Secure Anti-Virus for Lotus Domino scan documents and executables stored within the mailboxes, shared folders and databases of these messaging servers. F-Secure Anti-Virus for MIMESweeper adds malicious code detection and disinfection services to Content Technologies' MIMESweeper product.

All these products are managed through a single management console, F-Secure Administrator. Further, F-Secure Anti-Virus supports enterprise management systems such as IBM Tivoli TME 10 for software distribution, monitoring and alerting.

2. Solution Overview

This document describes the following features of F-Secure Anti-Virus:

- Basic functionality and platform support of workstation, server and gateway versions
- Centralized policy-based management provided by the F-Secure Policy Manager
- Integration with Enterprise Management Systems such as IBM Tivoli TME 10

2.1 Introduction

From the customer's point of view, the most important features of F-Secure Anti-Virus include:

Easy implementation

- World's only anti-virus solution to support policy-based management natively on all tiers
- Automated installation
- Total transparency to end users
- Scalable three-tier management architecture for LANs and WANs

Transparent and automatic protection

- On-the-fly real-time protection against all virus types
- Unparalleled malicious code detection and disinfection
- Detects also unknown Windows viruses and macro viruses
- Daily updated anti-virus solution
- Supports recursive scanning of archive files such as ZIP, ARJ and LZH

Complete Coverage

- Protect desktops and laptops in the LAN and on the road
- Protect file and print servers in real-time
- Protect traffic traveling through firewalls
- Protect mailboxes, shared folders and databases on mail servers
- Manage all of the above from a single management console

Support for Enterprise Management Systems

- IBM Tivoli TME 10 (software distribution, policy variable setting, alerts)
- Microsoft Systems Management Server (software distribution)
- Industry-standard SNMP protocol (on Windows NT 4.0)
- Support for CA Unicenter, IBM Netview and HP OpenView forthcoming

See these web pages for more information:

- <http://www.F-Secure.com/products/framework/>
- <http://www.F-Secure.com/products/white-papers/tivoli.htm>
- <http://www.F-Secure.com/solutions/tech-info/snmp.htm>

2.1.1 F-Secure Policy Manager

The F-Secure Policy Manager is built upon a comprehensive security management architecture. The main components of the Policy Manager are:

- The F-Secure Administrator, which provides a centralized management console for the security of the managed hosts in the network.
- The F-Secure Management Server, which is the repository for policies and software packages distributed by the administrator, and the status information and alerts sent by the managed hosts.
- The F-Secure Management Agent, which enforces the security policies set by the administrator on the managed hosts, and provides the end-user with a user interface and other services.

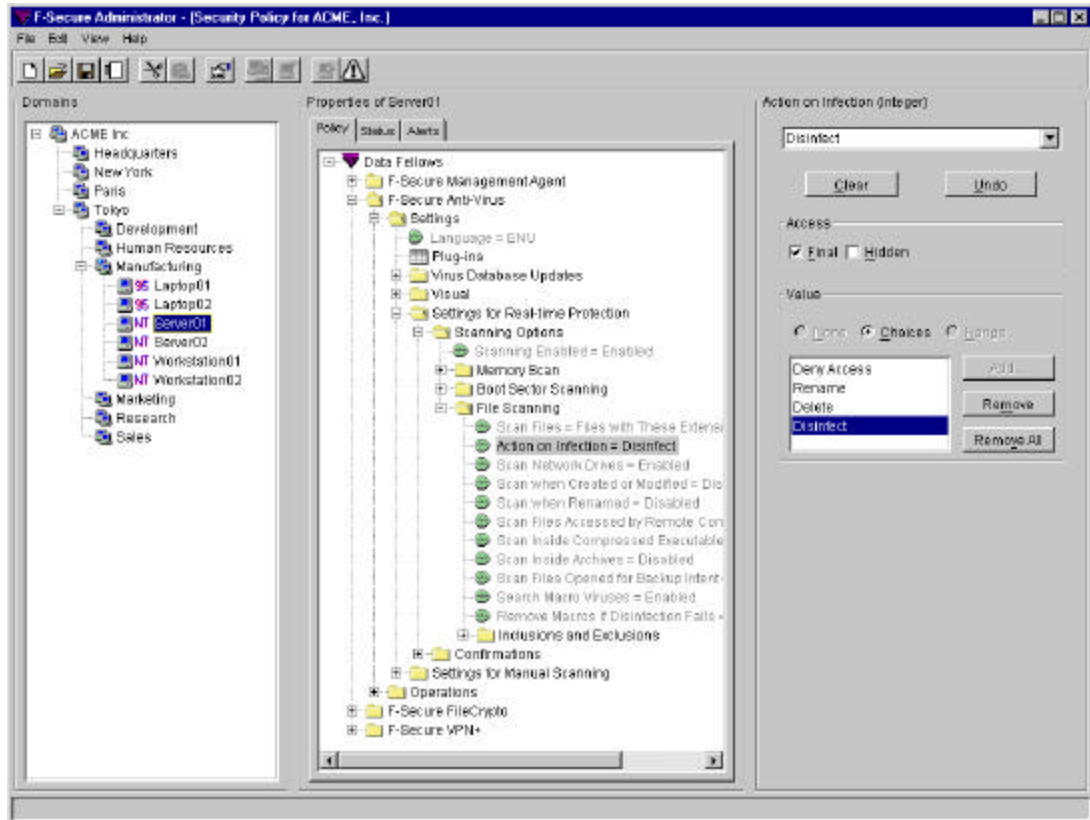


Figure 1. F-Secure Administrator

The F-Secure Administration Console is a Java-based application, which can be run on several different platforms. It can be used to remotely deploy the Management Agent on other workstations without the need for local login scripts, rebooting, or any intervention by the end user.

The F-Secure Management Server provides scalability by working as an extension to the Microsoft Internet Information Server (IIS). The communication between F-Secure Management Server and the managed hosts is done through the standard HTTP protocol, which ensures trouble-free performance in the LAN as well as global internetworks. In a small LAN, the active components of F-Secure Management Server can optionally be left out, and the policy and software package distribution can be handled through a shared

folder on a regular file server. This folder is also referred to as the communication directory.

The F-Secure Management Agent handles all management functions on the local workstations. It provides a common interface for all F-Secure applications, and operates within the policy-based management infrastructure.

The basic architecture used by these components relies on a concept known as policy-based management. A security policy is a set of well-defined rules that regulate how sensitive information and other resources are managed, protected, and distributed. The policy-based management architecture of F-Secure software uses policies that are centrally configured by the administrator for best possible control over the security issues in a corporate environment. Policy-based management implements many functions:

- Remotely controlling and monitoring the behavior of the products
- Monitoring statistics provided by the products and the Management Agent
- Remotely starting predefined operations
- Transmission of alerts and notifications from the products to the system administrator
- The transfer of policy files exchanges information between the F-Secure Administrator and the hosts.

2.1.2 Support for Multiple Scanning Engines

F-Secure Anti-Virus provides you with CounterSign technology, which integrates multiple scanning engines within a single product:

- F-PROT — best-of-breed macro virus detection and disinfection, world-class file and boot sector detection with highest disinfection rates available.
- AVP — best-of-breed polymorphic file virus detection and disinfection, world-class macro virus detection and disinfection
- ORION — world's first and only scanning engine to provide heuristic and emulation-based detection of polymorphic Win32 device driver based viruses

The technology includes signature-based scanners, heuristic analysis and checksum verification. Furthermore, it offers all anti-virus products a common framework to operate within, (and provides superior detection rates) as multiple built-in scanning engines deploy several detection technologies placing the viruses under severe scrutiny. F-Secure Anti-Virus is a completely modular anti-virus program, where the separate modules can be maintained and updated independently. This means that the engines can be updated without requiring the user to reboot the computer.

To witness the effectiveness of this technology, F-Secure Anti-Virus has received phenomenal success in comparative reviews conducted by the leading computer industry

magazines. F-Secure Anti-Virus has consistently outscored competing products from NAI, Symantec, Trend and other vendors.

2.1.3 Complete Coverage

Some vendors of anti-virus products have argued that the best solution to the virus problem is to stop the viruses at the firewall or email server level, and not install any software on the workstations since the end-user will just uninstall or configure it incorrectly.

F-Secure provides you with protection at the server and gateway level, but it's important to realize that this isn't enough. Today's workforce is increasingly mobile and you can't protect a laptop on the road with the firewall at the office. Therefore, it is imperative that the information is protected where it's created and processed — on the desktop, the laptop, or the PDA. Otherwise, it's impossible to make sure that viruses don't get in through floppies, CD-ROMs, encrypted emails, or protected documents.

The real question is the management of the solution. F-Secure answers this question by providing you with centralized policy-based management for all the layers, including the workstations, the servers, and the gateway computers. The protection is automatic and transparent, so the end-user doesn't need to be concerned about scanning the hard disk or checking email attachments — the user is always protected.

The F-Secure solution gives the administrator control over the security policy, and enables the administrator to enforce that policy throughout the organization.

2.1.4 Performance

Through advanced kernel-level device driver technology, F-Secure Anti-Virus provides you with lightning-fast real-time response times with its transparent protection. The three scanning engines in the product use the operating system's cache functionality, which means that the real-time performance is not affected noticeably even when all the engines are running simultaneously. The hard disk is in any case the bottleneck, not the virus scanners.

Please note that F-Secure Anti-Virus 5 for Workstations is designed for real-time virus detection. For peace of mind, the administrator can also start a virus scan task on the computers on-demand, but this feature is designed for background execution and minimal impact on foreground applications. The same holds for the "right-click" based on-demand scanning feature. Scan tasks started this way will take a long time to complete, and it must be noted that this is caused by the transparent protection strategy designed into the product. Transparent real-time scanning provides the user with much better protection in the real world than GUI based on-demand scanning.

2.1.5 In-place Quarantine

When a virus is detected, access to the file is denied, and the virus is disinfected (unless the policy set by the administrator defines another action). This in-place quarantine

ensures that the user cannot open the file or copy it elsewhere until it has been disinfected.

The same functionality is available on workstations and servers.

2.2 Platform Support

2.2.1 Desktop Platforms

The regular F-Secure Anti-Virus Total Suite license covers the following desktop platforms:

- Windows 95, 98, NT 4.0, and 2000
- Windows 98
- Windows NT 4.0
- Windows 2000
- Linux
- Solaris x86
- Windows 3.1
- Windows NT 3.51
- OS/2
- Macintosh

The modern Windows platforms are managed directly through the F-Secure Policy Manager, while Windows 3.1, NT 3.51 and OS/2 are managed through the F-Secure Management Adapter for FSAV 4. All of these products can be managed centrally with the F-Secure Administrator management console. The Linux and Solaris x86 versions are managed using Unix command-line tools. The Macintosh version is a desktop solution with no centralized management features.

For more information, see:

- <http://www.F-Secure.com/products/anti-virus/>

2.2.2 Server Platforms

The regular F-Secure Anti-Virus Total Suite license covers the following server platforms:

- Windows NT 4.0 Server
- Windows 2000 Server
- Linux

- Solaris x86
- Novell NetWare
- Windows NT 3.51
- OS/2

The following gateway server level products are also included:

- F-Secure Anti-Virus for Firewalls (Check Point FireWall-1, TIS Gauntlet, AltaVista Firewall)
- F-Secure Anti-Virus for Microsoft Exchange (versions 5.0 and 5.5)
- F-Secure Anti-Virus for Lotus Domino (versions 4.5 and 4.6)

Windows NT and 2000 based servers, together with the firewall and email servers, are managed centrally with the F-Secure Administrator management console. F-Secure Anti-Virus for NetWare is managed through NWADMIN. The Linux and Solaris x86 versions are managed using Unix command-line tools.

For more information, see:

- <http://www.F-Secure.com/products/anti-virus/>

2.2.3 F-Secure Anti-Virus for MIMESweeper

With F-Secure Anti-Virus for MIMESweeper, you can combine the power of F-Secure anti-virus detection and disinfection with the MIMESweeper functionality in an integrated solution. The MIMESweeper family provides defenses against threats in email such as spamming and hostile attacks.

2.2.3.1 DLL or Command Line?

There are many options to consider when choosing an anti-virus product to integrate with MIMESweeper, these include virus detection rates, ease of integration, speed of scanning, and disinfection of viruses.

Command line scanners are currently the most popular products to integrate into MIMESweeper. However, there are a couple of problems with this approach. The first problem is that command line scanners are slow and cumbersome. To understand this in more detail, consider the process flow of using a command line scanner with MAILsweeper:

1. Email is received by MIMESweeper
2. MIMESweeper decodes the mail and places it into a temporary directory
3. MIMESweeper calls the command line scanner
4. The command line scanner is launched (only one instance of the command line scanner can typically be loaded at any one time)

5. The command line scanner checks the email in the temporary directory
6. The command line scanner returns an error code on the outcome of its operation
7. MIMESweeper examines the error code and determines what to do with the email

As you can see, this is a lengthy process involving many tasks and the process has to be repeated every time an email is received. This becomes a problem if a large volume of email is received. In that situation, the incoming email would need to be queued for scanning, as only one instance of the command line scanner can be launched at any given time.

Other problems with command line scanners are found in the virus detection rates. Some command line scanners are DOS-based, and therefore use different anti-virus engines than their Windows' counterparts. This often leads to difficulty in detecting Windows' specific viruses (such as PE infectors). Furthermore, DOS-based engines have not proven very effective with polymorphic viruses.

The DLL based solutions offer many benefits over command line solutions. The greatest benefit is speed, which can be understood by considering the process flow of using the DLL solution:

1. MIMESweeper receives an email
2. The integrated DLL passes the email to the anti-virus scanner
3. The anti-virus Scanner checks the email
4. The result is passed back to MIMESweeper
5. MIMESweeper carries on with the email in a normal fashion

The improved process flow, coupled with the fact that the "on-demand" DLL scanner can process multiple files at once, provides enormous speed improvements over the command line scanner.

2.2.3.2 Functionality Overview

The F-Secure solution is a DLL solution with the following additional functionality:

- **Administration:** F-Secure Anti-Virus for MIMESweeper provides central administration for anti-virus signatures and application updates, as well as software configuration changes. The solution operates on a central HTTP server, making it easy to place the MIMESweeper box on the DMZ of a Firewall, and it adds a lock down feature so that changes cannot be made to the MIMESweeper system.
- **Reporting and alerting:** F-Secure Anti-Virus for MIMESweeper can be configured to send all reports and alerts to the central administration machine.
- **Scanning and disinfection:** F-Secure Anti-Virus for MIMESweeper incorporates F-Secure's unique ability to use three different anti-virus engines (F-Prot, AVP and Orion) at the same time.

2.3 Services

F-Secure provides support and services to F-Secure Anti-Virus customers through its Professional Services team and the chain of F-Secure Business Partners, which covers more than 90 countries globally.

2.3.1 Installation and Deployment

The Professional Services Team at your local F-Secure Business Partner provides you with help when implementing and deploying F-Secure Anti-Virus in your network.

2.3.2 Technical Support

Telephone and email support are included in the F-Secure licenses for the duration of the maintenance contract (renewable every one or two years depending on your choice). On-site consulting is available for a separate fee.

F-Secure Corporation has a comprehensive chain of Certified Anti-Virus Centers that provide customers with around-the-clock global response services. All of the partners are committed to give support to international customers in their respective area free of charge.

2.3.3 Anti-Virus Signature Database Updates

The F-Secure Anti-Virus macro virus signature database is updated every day during the business week, tested, and made available to customers over the Internet from F-Secure web servers. The full virus signature database, including polymorphic Win32 viruses, is updated once a week. All updates can be totally automated using F-Secure BackWeb.

2.3.4 Software Maintenance

F-Secure software upgrades are delivered on CD-ROM, diskettes or through the Internet. Each F-Secure Anti-Virus upgrade comes with a technical virus bulletin stating the current global virus situation.

3. Centralized Policy-Based Management

Everything in the F-Secure management framework is based on policies. Policy-based management is better suited for security enforcement than traditional network management methods. The software and policy file distribution is based on public-key cryptography, which ensures that the commands distributed across the network reach their goal, insuring their integrity.

3.1 Software Distribution

3.1.1 Initial Installation

There are several options for doing a first-time installation of F-Secure Anti-Virus:

- F-Secure Intelligent Installation. This method “pushes” the software from a central location to selected computers in a Windows NT network. You don’t need to visit the workstations or set them up in any special way. This option is only available in Windows NT networks for installing F-Secure Anti-Virus 5 on Windows NT and Windows 2000.
- Login scripts. The setup program is started in silent mode from a network logon script. This option can always be used for installing F-Secure Anti-Virus to Windows 95 and Windows 98. For Windows NT workstations, this option is normally not used because the setup program will require local administration rights on the target computer.
- Microsoft Systems Management Server (SMS). See section below for more information.
- IBM Tivoli TME 10. See section below for more information.
- ZENworks (in Novell NetWare networks). Go to <http://www.novell.com/coolsolutions/zenworks/> for more information.
- On peer-to-peer networks, no centralized management functionality or logon scripts are available. In such networks, installation sets should be first created as if using a logon script based installation. Users must then be instructed through email, or a similar method, to manually execute the command that would otherwise be inserted into a logon script. The administrator can create a shortcut file with the proper command line and attach it to an email message for the users’ convenience.
- The easiest way to install F-Secure Anti-Virus on computers, which aren’t networked at all, is to run the setup program directly from the CD-ROM.

3.1.2 Anti-Virus Signature Database Updates

Anti-virus signature database updates are pulled from F-Secure Management Server by the computers as specified by the policy defined by the administrator. The updates are downloaded by the F-Secure Management Server from the F-Secure web site either automatically by F-Secure BackWeb or on demand by the administrator.

3.1.3 F-Secure BackWeb Push Technology

F-Secure BackWeb provides you with automatic transparent updates directly from the F-Secure web site. BackWeb downloads files automatically, using bandwidth left unused by your other Internet applications. So, you are automatically alerted when new

information has been received, making sure you have the latest updates, without having to search the Web.

The free BackWeb agent can be downloaded from the F-Secure Website as well.

3.1.4 Software Upgrades

Software upgrades are received from F-Secure on CD-ROM or through the web, and distributed by the administrator to end-users in digitally signed Jar packages to ensure their integrity. F-Secure Administrator includes all the necessary functionality for managing software packages.

3.1.5 Support for Enterprise Management Systems

F-Secure Anti-Virus supports several Enterprise Management Systems for software distribution. This includes first-time installation, software upgrades, and anti-virus signature database updates. See sections below for more information.

3.2 Alerts and Reports

Event handling covers both alerting and logging activities. The primary requirement for events is that they must be configurable, based on experience. The system policy will reflect the administrators' knowledge of what kind of alerts are required and what kinds are undesirable. This knowledge is part of the general security policy of the entire network.

With a properly configured alerting policy, the administrator can tell the workstation agents to send their alerts to a management server. This server can then cross-reference the incoming alerts and send the administrator one single alert instead of a thousand.

The management module API of the agent contains a section for alerting-method plug-ins. When an alert is raised, the agent knows the current state of the workstation and can use the appropriate plug-ins. There are a large number of possible alerting methods.

The F-Secure Management Agent has a number of alerting plug-ins:

- F-Secure Administrator
- F-Secure Manager, the end-user workstation user interface
- Event/alert agents; Event Viewer, local and remote logs, SMTP
- Event/alert gateways; fax, pager and GSM short messages
- Enterprise management systems:
 - Event adapters for Tivoli TME 10 and CA Unicenter
 - Support for SNMP TRAPS and support packs for SNMP based network managers like OpenView and NetView.

- Possibility to integrate to third-party management system alerts.

3.3 Policies

A security policy is a manifestation of laws, rules and practices that regulate how sensitive information and other resources are managed, protected or distributed.

Policy based management includes:

- Remotely controlling and monitoring the behavior of the products
- Monitoring statistics provided by the products and the Management Agent
- Managing alerts
- Starting predefined operations remotely

3.3.1 F-Secure Framework Policy Types

The information flow between the Administrator and the hosts is done by transferring policy files. There are three kinds of policy files: Default Policy Files, Base Policy Files, and Incremental Policy Files.

3.3.1.1 Default Policy

The Default Policy file is an unsigned policy file that contains the default values *for one product*. Default Policies are used only in the host end. If neither the Base Policy nor the Incremental Policy file contains an entry for a variable, then the Default Policy file is utilized. There may be different default policies for different configurations of the product. A normal networked configuration will not use default policies after the F-Secure Administrator has received information of a successful installation and has distributed new base policies for those product versions.

3.3.1.2 Base Policy

The Base Policy files contain the administrative settings and restrictions for all variables on all F-Secure products at one specific host (in some special cases a group of hosts may share the same file). The file is signed by the F-Secure Administrator and is therefore protected against changes during network transfers or changes while in the host file system. These files are sent from the Administrator to the hosts.

3.3.1.3 Incremental Policy

The basic use of an Incremental Policy file is to store the changes to the base policy at the end-user workstation. Only changes that are within the Base Policy limits are allowed. These Incremental Policy files are then sent to the Administrator for status viewing purposes. Status information includes both the local configuration changes and statistics.

3.3.1.4 F-Secure Management Agent Internal Structure

In the F-Secure Management Agent there are two components that are concerned with policy files. The Network Request Broker is responsible for all network accessing and it periodically tries to fetch new policy files from the F-Secure Management Server. The Configuration Handler provides the functionality of getting and setting policy variables to other user mode modules and products. It communicates with a kernel mode component called the Policy Driver. This driver will maintain the current policies and provide the information both to the Configuration Handler and to other drivers that will need this information.

3.3.2 Policy File Contents

3.3.2.1 Management Information Base

The Management Information Base (MIB) is a hierarchical structure that defines what *can* be stored in the policy files, but not the actual policies that the files contain. The MIB concept was originally established by the SNMP protocol. Each variable has a unique Object Identifier (OID).

The following categories are defined in the MIB of an F-Secure product:

- Settings: The managed products have to operate within the limits set in this section.
- Statistics: The statistics part brings information to the Administrator.
- Operations: Operations are one-time tasks for the host.
- Private: The MIB can also contain variables that the product stores for its internal use between sessions.
- Traps: These are alerts (or events) sent to the local console, a log file, some remote administration process etc.

3.3.2.2 Policy Variables

All policy variables have an associated type. The basic non-aggregate types come directly from the SNMP world. The type of a basic policy variable can be one of the following:

- Integer: Normal integer number
- Display String: 7-bit ASCII text string
- IP Address: Four octet IP address
- Counter: Increasing integer
- Gauge: Non wrapping integer
- TimeTicks: Elapsed time in hundredths of a second since some epoch

- Octet String: Binary data. This type of data is also utilized in UNICODE text strings.
- OID: Object identifier
- Opaque: Binary data that can represent additional data types
- Table: two-dimensional collections of the basic types

A policy variable may have a predefined default value in the MIB. The administrator can use the base policy file to deliver either that default or some other value to the hosts. It is also possible to define whether the end-user or some software in the end-user workstation can further change the value.

Integer-type (Integer, Counter, Gauge and TimeTicks) variables may have their value set restricted with a range definition. Variables of any type may have an associated list of acceptable values, i.e. choice definition. This means that the administrator can enforce limits to the choices the users can make.

3.4 Security of the Centralized Management Solution

In regard to security, the F-Secure Policy Manager accomplishes two things:

- All data that is accepted from the network to the workstation, has originated from the administrator and is current.
- The user of the workstation cannot circumvent an administrative policy without detection.

3.4.1 Integrity, Authenticity and Up to Date Data

The information flow from the Administrator to the Workstation consists of base policy files and installation packages. Both are signed using public key cryptography. This signature ensures integrity and authenticity. The up to date nature of the base policy files is accomplished using an increasing counter inside the file. Each host checks this serial number each time it fetches policy files and does not accept new policies if the serial number is less than the previously used one.

The software updates are triggered using information in the base policy file. The installation package is verified to be the same as the one specified in the policy, so the up to date nature of the installation package is actually tied to the same counter information as the triggering policy.

The base policy files are signed using the management private key. The installation packages use JAR (Java Archive) as the package format. In JAR, the signature is not done to the package as a whole, but a separate signature file contains signatures of individual files. Some of the files are signed using the management private key and some of the files are signed using the F-Secure private key.

Both the management key pair and the F-Secure key pair use the DSS (Digital Signature Standard) Algorithm with a key length of 1024 bits, which is currently considered unbreakable.

3.4.2 Preventing the User from Circumventing Policies

The main tool used to prevent users from circumventing policies is the signed base policy file. The base policy file also contains the ID of the host, so that files meant for another host cannot be used. There is a counter inside the policy file, which prevents old policies from being installed.

The users are only allowed to change values within the limits given in the base policy. The same restriction applies to all software in the end-user workstation. These user-made changes are stored in the incremental policy file.

The F-Secure Management Agent component Policy Driver is a kernel-level device driver that cannot be modified by normal end-users. The driver keeps critical files open to prevent other processes from accessing them while the system is running. Writing to the base policy and both, reading and writing of the incremental policy, are denied. The management public key file is also made non-accessible using this same method.

The F-Secure Management Agent component Configuration Handler keeps a backlog of used policies for error situations. In the Windows NT environment with an NTFS partition, the files are granted read-only access to the local administrator's group, and full control to the local system account.

4.0 Integration with IBM Tivoli TME 10

A module called F-Secure Plus for Tivoli Enterprise enables the integration of Tivoli TME 10 with F-Secure products. The integration consists of all the operating and network parameters monitored by Tivoli TME 10 and security related information monitored and managed by F-Secure Suite Plus. The F-Secure Suite Plus provides integration with:

- Tivoli Management Framework and *Tasks*
- Tivoli Software Distribution and *File Packages*
- Tivoli Enterprise Console (TEC) and *Events, Event Adapter and Rules*
- Tivoli Distributed Monitoring and *Application Monitors*

The F-Secure Management Agent has native support for forwarding F-Secure alerts to the Tivoli Event Server. This is done by simply setting the appropriate policy variables and distributing the new policy using the F-Secure Administrator.

4.1 Tasks

The F-Secure Suite Plus Tasks are commands that execute without user intervention on selected remote workstations. The Tivoli Management Framework executes these tasks on Tivoli managed workstations and displays the results on the Tivoli desktop. Results can also be stored or redirected to a file.

Tasks in the F-Secure Suite Plus include:

- Virus scanning remotely
- Show reports of the executed virus scanning
- Show the statistics for selected F-Secure Workstation Suite product
- Reset statistics for selected F-Secure Workstation Suite products
- View security related statistics
- Launch F-Secure Administrator
- Read and write policy values directly

Note: for security reasons, changing some policy values is not allowed unless the F-Secure Administrator has allowed the write operation on those variables.

4.2 File Packages

Tivoli Software Distribution uses file packages to install software on remote workstations. The F-Secure Plus includes the following software distribution combinations:

- F-Secure Workstation Suite installation
- F-Secure Tivoli Management Extension Handler installation
- F-Secure Workstation Suite version updates
- Anti-virus signature database updates

4.3 Monitors

F-Secure Workstation Plus Monitors extend the management capabilities of Tivoli Distributed Monitoring. The plus module monitors check the status of the different F-Secure Workstation Suite resources and define what to do if certain conditions are met. Administrators can monitor the status of the following resources:

- F-Secure Management Agent
- F-Secure Manager
- F-Secure Gatekeeper

- F-Secure Anti-Virus
- F-Secure VPN+

An example of application monitoring would be a case for the F-Secure Management Agent, FSMA. If, for some unknown reason, FSMA gets terminated in a workstation, the distributed monitor notices this within one minute by default, and sends an event to the Tivoli event server.

4.4 Events, Event Adapter, and Rules

Integration with the Tivoli Enterprise Console (TEC) consists of events, an event adapter, and rules. The administrator can do a severity-based selection on what kinds of events are sent to the TEC. Some examples of the large amount of available events and alerts are:

- Not enough free disk space to install the selected products, Management Agent
- A virus was found and disinfected, Anti-Virus
- Anti-Virus signature database file is corrupted or outdated, Anti-Virus
- A file or directory has been removed from TopSecret list, FileCrypto

An example of a rule is that if an event occurs stating that the FSMA went down in some workstation, the Tivoli event server automatically applies a rule that executes a task to restart the FSMA immediately in the workstation.

5. Integration with Microsoft Systems Management Server

Integration of the Microsoft Systems Management Server with F-Secure products, such as F-Secure Anti-Virus 5, F-Secure FileCrypto, F-Secure VPN+ and F-Secure Workstation Suite, can be accomplished through support files and documentation provided by F-Secure Corporation. For more information, see the F-Secure Website.

5.1 Software Distribution

F-Secure fully supports the software distribution methods provided by the Microsoft Systems Management Server versions 1.2 and 2.0. The installation is completely transparent to end users at their workstations.

F-Secure provides pre-prepared Package Definition Files and instructions on how to apply them to distribute the initial installation kits and/or updates to the target computers through the SMS system.