AhnLab

V3Pro 2004 and AhnLab Policy Center 3.0

Security Target

v1.7

CONTENTS

1. Introduction

1 This chapter aims to identify Security Target and accurately describe typographic conventions and terms. IT security environments required for the TOE to provide a secure system solution and security obectives will be described in this TOE along with the IT security requirements that satisfy the security objectives to describe the security functions provided by the TOE.

2 The Security Target for the TOE consists as follows:

- Chapter 1 introduces the Security Target, identifies Common Criteria, and defines terms.
- Chapter 2 describes the TOE and defines scope and boundary of the TOE. This also overviews the security functions of the TOE.
- Chapter 3 describes assumptions, threats, and organizational security policies as the security environment of the TOE.
- Chapter 4 describes security objectives for the TOE and the environment
- Chapter 5 identifies security requirements of the TOE and IT environment, and assurance requirements.
- Chapter 6 describes the TOE summary specification for the requirements in the chapter 5.
- Chapter 7 describes protection profile's claim, description and other information. Since this Security Target does not claim any Protection Profile, the description is omitted.
- Chapter 8 provides the security objectives rationale, security requirements rationale, and TOE summary specification rationale for the Security Target.

1.1 Identification

- **Title** - V3Pro 2004 and AhnLab Policy Center 3.0 Security Target V1.7 AhnLab, Inc.
- **Common Criteria** – Common Criteria for Information Protection System (Announcement No. 2005-25 by Ministry of Information and Communication)
- **Written by** - AhnLab, Inc.
- **Created on** – July 10, 2007
- **Related Protection Profile** – None
- **TOE Identification** - V3Pro 2004 and AhnLab Policy Center 3.0

1.2 Overview

3 The TOE in this Security Target consists of V3 Pro 2004 (Hereinafter referred to as V3), the anti-virus program that protects computers from the intellectual attacks integrated with viruses, Trojan horses and worms, and the V3 management server program, AhnLab Policy Center 3.0 (Hereinafter referred to as APC or APC 3.0), which provides central management for anti-virus programs.

4 This Security Target accepts SOF-medium for the TOE.

1.3 Typographic Convention

5 This Security Target uses English words for clearer meaning of abbreviations and terms. Notations, forms, and typographic conventions conform to the Common Criteria for information protection systems and protection profiles for government agencies.

6 Iteration - Iteration is used when the same component is used repeatedly for multiple operations. The result of the Iteration operation is indicated by the iteration number within parentheses, (repeat number), following the component identifier.

7 Selection - Selection is used to select one or more options provided by the Common Criteria for the information protection system. The result of the Selection operation is indicated in *underlined italicized* characters.

8 Refinement - Refinement is used to further restrict any requirement by adding details to the requirement. The result of the Refinement operation is indicated in **bold characters**.

9 Assignment - Assignment is used to allocate a specific value to an unspecified parameter. (Example: Password length). The result of the Assignment operation is indicated by square brackets, [Assignment_Value].

10 Application Notes - Application note clarifies the meaning of a requirement, provides information on options upon implementation, and defines the "suitable/non-suitable" standard for the requirement. Application note may be provided with the corresponding requirement, if necessary.

1.4 Terms and Definitions

11 Terms and definitions in this Security Target and overlapping those in the Common Criteria for information protection systems follow the Common Criteria. Besides the Common Criteria, additional terms are added by the author.

12 Terms and definitions overlapping in the Common Criteria are follows.

13 Audit Trail – A set of disk records that generated by the access and behavior of the user.

14 Object – An entity within the TSF Scope of Control (TSC) that contains or receives information and upon which subjects perform operations.

15 Attack potential – The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources, and motivation.

16 Strength-of-Function (SOF) – The qualification of a TOE security function expressing the minimum effort assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

17 SOF-medium – A level of the TOE SOF(Strength of Function)-of-function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security function by attackers possessing a moderate attack potential.

18 Iteration – One of the operations defined in the Common Criteria for the information protection system. A component is used more than once in a variety of operations.

19 Security Target (ST) – A set of security requirements and functional specifications to be used as a basis for TOE evaluation.

20 Protection Profile (PP) – An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

21 Human User – Any person who interacts with the TOE.

22 User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

23 Selection – One of the operations defined in the Common Criteria for the information protection system. One or more items are specified from a list in a component.

24 Identity – A representation uniquely identifying an authorized user.

25 Element – An indivisible security requirement

26 Role – A predefined set of rules establishing allowed interactions between a user and the TOE. (Example: User, Administrator)

27 Operation – An operation ensures that a component can respond to a certain threat in the Common Criteria for the information protection system or to satisfy a certain security policy. (Example: Iteration, Assignment, Selection, or Refinement)

28 Threat Agent – Any unauthorized user or external IT entity which threatens to access, alter, or delete assets.

29 External IT Entity – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

30 Authentication Data – Information used to verify the claimed identity of a user.

31 Assets – Information or resources to be protected by TOE countermeasures.

32 Refinement – One of the operations defined in the Common Criteria for the information protection system whereby additional details are added to a requirement. The addition of details to a component.

33 Common Criteria for Information Protection System – It is the Common Criteria published on May 21, 2005 by the Minister of Information and Communication. It is the Korean translation of Common Criteria (CC) version 2.3 which is based on the criteria of many countries and has been developed based on a common language and common understanding.

34 Organizational Security Policies – One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

35 Dependency – A relationship between requirements such that the requirement depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

36 Subject – An entity within the TSC that causes operations to be performed.

37 Augmentation – The addition of one or more assurance components to an EAL or assurance package.

38 Component – The smallest selectable set of elements that may be included in a protection profile or Security Target.

39 Class – A grouping of families that share a common focus in the Common Criteria for the information protection system.

40 **Target of Evaluation (TOE)** – An IT product or system and its associated guidance documentation that is the subject of an evaluation.

41 **Evaluation Assurance Level (EAL)** – A package consisting of assurance components that represents a point on the predefined assurance scale in the Common Criteria for the information protection system.

42 **Family** – A group of components that share security objectives but may differ in emphasis or rigor.

43 **Assignment** – The specification of an identified parameter in a component.

44 **TOE Security Functions (TSF)** – A set of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

45 **TOE Security Policy (TSP)** – A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

46 **TSF data** – Data created by and for the TOE that might affect the operation of the TOE.

47 **TSF Scope of Control (TSC)** – The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

48 The following terms and definitions are added by the author:

49 **Management Server** – A server that provides central management and control for V3, a component of the TOE. The management server where APC (AhnLab Policy Center 3.0) is installed consists of Policy Server, Policy Center Admin, and Policy Agent.

50 **Update Server** – A distribution server that provides the V3 engine and patch files for updating.

51 **Engine file** – A file containing methods and patterns for V3 to detect malicious codes and define them as viruses.

52 **Patch file** – An execution code file in the update file that fixes vulnerabilies and bugs and an execution code file of the engine to detect malicious codes.

53 **Anti-virus** – An IT tool to detect and remove computer viruses based on virus detection patterns.

54 **Policy Center Admin** – A component of AhnLab Policy Center v3.0 (APC), which provides an interface for authorized administrators to manage policy servers from a remote place or local area network with a firewall.

55 **Policy Server** – A management server that provides central management of V3.

56 Policy Agent – A program that enforces the commands and information from the policy server on V3. The policy server delivers/installs a policy agent on the V3-installed system and manages V3 through the agent.

57 Authorized General User – A user who uses V3 in his own personnel computer. When using V3, the user is classified as authorized general user because the user is identified and authenticated in the V3-installed system. In other words, the authorized general user is the authorized V3 user.

58 Restricted General User – The operating system (Windows) where V3 is installed has restricted general user accounts without administrator's authority. When V3 run by the restricted general user account, it is also restricted to operate V3. The authority of the account is also restricted in using V3.

59 Authorized Administrator – Administrators in charge of security management of APC through Policy Center Admin for central management of V3 configuration. They are classified as authorized administrators since they connect to APC by identification and authentication of APC. The policy server provides the following types of administrators: server administrator, policy administrator, and monitor staff.

60 Monitor Center – A program that provides audit records of policy agents, policy servers, and V3 in real-time for authorized administrators. It is provided as a separate UI in Policy Center Admin.

1.5 Common Criteria Conformance

61 This Security Target complies with the following:

- Common Criteria for the information protection system (Notice 2005-25 by Ministry of Information and Communication, May 21 2005)
- Common Criteria (CC) V2.3 Part 2 Extended (FAV_ACT.1, FAV_ALR.1, FAV_SCN.1, FAV_SPM.1, FTA_SSL.4)
- Common Criteria (CC) V2.3 Part 3
- Evaluation Assurance Level 4
- SOF-medium

2. TOE Description

2.1 Product Type

62 The product type of the V3, a part of the TOE, is a software package, which is an anti-virus program that protects server machines from malicious codes such as viruses, Trojan horses, and worms. The other part of the TOE, APC is a management server that consists of policy server, policy center admin, and policy agent which are software products installed in the enterprise environment with the 3-tier architecture model to manage multiple V3 programs.

63 In the anti-virus software, V3, "Virus" is defined as any intrusion caused by worms and Trojan Horses including computer viruses. Computer viruses are classified as follows. The following viruses are defined and determined as 'malicious code' by AhnLab's engine. (Depending on the distinction of malicious code such as location and specific strings, the viruses are determined). Therefore, the malicious code is a general criterion known and reported to harm users, and V3 detects and diagnoses the malicious codes with V3-engine by AhnLab. The V3-engine awarded the certification Checkmark[1]' for test level 1[2]', level 2, and Trojan horse scans/repairs viruses.

- **File Infectors** - File Infectors infect executable program files. These viruses normally infect executable files such as .com and .exe files, however these files could infect other forms of executable code such as .sys and .vxd files. Many of these viruses become memory resident when run, once resident in memory, the virus will infect any non-infected executable that the system runs.
- **Boot Sector Infectors** - Boot Sector viruses infect the system areas of a disk. That is they infect the element known as a boot record on a floppy or hard disk. All floppy disks and hard disks contain a small program in the boot record that can be run when

[1] This certification guarantees the quality of Anti-Virus products, granted by West Coast Labs (http://www.westcoastlabs.org) located in England and specialized in functionality testing. WCL grants Checkmark certification to products that pass the tests that diagnose and repair 100% of Wildlist. (A virus list reported their detection or infection activities in the two or more locations throughout the world.)

[2] According to the testing targets and methods, West Coast Labs currently tests anti-virus programs on three levels: Level 1, Level 2 and Trojan Checkmark. The first stage (Checkmark Level 1) verifies that an anti-virus is able to detect all viruses "in the wild." The second stage ((Checkmark Level 2) verifies that an anti-virus is able to detect all those viruses which are actually causing infections in the real world, and in addition, disinfect all viruses "in the wild".

the computer starts up. Boot Sector Infectors attach themselves to this area of the disk and will execute when the machine is started up from the infected disk.

- **Master Boot Record Infectors**- Master Boot Record Infectors are memory resident viruses that infect disks in the same manner as Boot Sector Infectors. The main difference between these two virus types is where the virus code is located. Master Boot Record Infectors normally save a legitimate copy of the mast boot record in a different location.
- **Multi-Partite Viruses**– Multi-Partite viruses can infect both Boot Records and Executable Program files. These can be particularly difficult to repair. If the boot area is cleaned, but the files are not, the boot area will be immediately re-infected.
- **Macro Viruses** – These types of viruses infect other types of files. With the advent of Visual Basic scripting within Microsoft's Office 97 suite, a macro virus can be written that not only infects data files, but also can infect other files as well. Macro viruses can be written to infect Microsoft Office Word, Excel, PowerPoint, Project, Visio and Access. Macro Viruses can be written for any application that allows the use of a scripting language such as Visual Basic.
- **Worms** – Worms are programs that replicate themselves from system to system without the use of a host file. A very important distinction from a virus is that it requires the spreading of an infected host file. Worms are normally found in a document file that already has the worm macro. When the document is moved from a computer to another computer, it is considered to be a worm.
- **Trojan Horses** – Trojan horse is a destructive program that masquerades as a benign application, and it does not replicate them. Trojan horse contains malicious codes that cause loss or even theft, of data. In order for Trojan horse to spread for example, you must invite one onto a system as if opening an email attachment.[3]
- **Harmful Programs** – Harmful programs are developed for a normal purpose but can be used for a malicious purpose.

64 V3 provides scan/repair functions to detect and prevent viruses that inflow to the system. They perform the real-time scan (monitoring) on the system and also warn/repair the detected viruses.

- **Advance scan** – To detect memory viruses that exist only in the memory area, V3 detects network traffic and the memory area where other application use, and processes running in the system. V3 also scans file viruses of the Start program area (registry and start program folder), and boot record virus in the boot area before the scan/repair operation.
- **Scan** – You can scan the system by entering the shortcut command or entering the path (directory/folder provided by windows explorer) you want to scan in the scan user interface.

[3] www.virus.org

- **Explorer Scan** – You can scan the path (directory/folder provided by windows explorer) you want by using the scan interface plugged in the windows explorer.
- **Scheduled Scan** – You can scan the path (directory/folder provided by windows explorer) you want when you want.
- **Policy Server Manual Scan** – Authorized administrator sends a manual scan command through the policy server for V3 to operate system scan.
- **Screen Saver Scan** – When the screen saver is on, V3 automatically scans the system.
- **Outlook Scan** – Outlook scan plugged in the MS Outlook program scan emails messages that are stored in the MS Outlook's inbox.
- **Real Time Monitoring** – Real time monitoring monitors the V3 installed system in real-time. Real time monitoring consists of system monitoring which provides real-time scanning of the file system's I/O in the V3 installed system, internet monitoring, instant messenger monitoring plugged in each application, startup program monitoring, outlook monitoring, POP3 monitoring (POP3 Protocol), office protector (Microsoft Office Program).

65 Besides the virus scan/repair function, V3 installed in the Windows server filters the specific port by incoming and outgoing connection to secure the server. This is to prevent worms from spreading through the specific port before the V3 engine is updated.

66 If viruses are detected in the above way, V3 sends the virus-infected object to the 'Quarantine' area to prevent the inflow/spread of the specific virus to any other areas, and repairs (restore them to their original files), leaves as is, or deletes (unrepairable virus) them according to the repair setting. If a virus is detected, V3 generates audit records and displays a security-warning message according to the configuration.

67 Moreover, V3 is able to detect viruses in a compressed file for file viruses. Before V3 starts running, it scans its own processes and repairs them in case of detecting viruses for its self-protection.

68 The management server, APC, provides centralized management for V3. APC transmits and enforces configurations for the scan/repair function to each V3. The centralized management for V3 users by the policy server may reduce probable threats from viruses.

69 The centralized management software, APC, manages V3 in 3-tiered architecture. A policy server manages V3 installed computers by installing a policy agent on each computer. The Authorized administrator installs policy center admin on his own computer to manage the policy server by accessing to the policy server from a remote place or local area network. The policy server enforces V3 to apply security configurations.

70 The asset protected by TOE is defined as data (particularly shared files) stored in users' computers and network in the enterprise environment because viruses like worms are spreaded through the Internet.

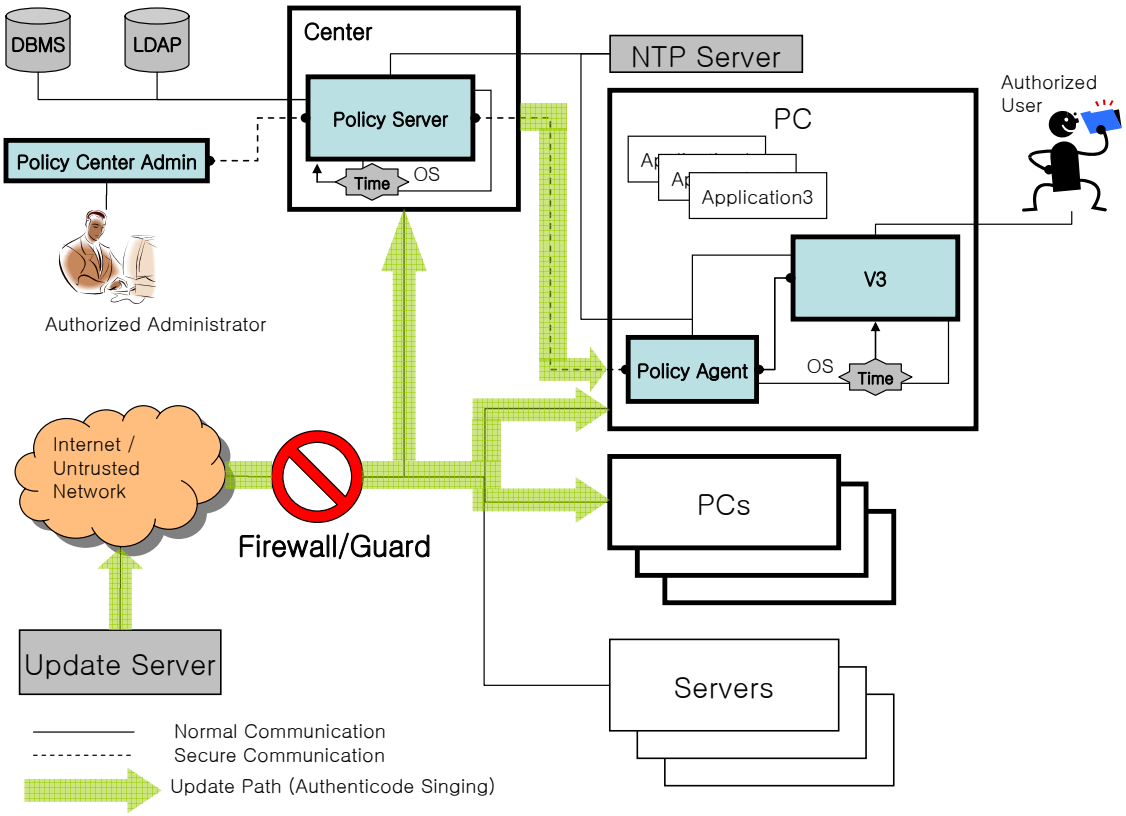
2.2 TOE Scope

2.2.1 Physical Scope and IT Operating Environment

71 As a component of the TOE, APC consists of policy server, policy center admin, and policy agent. The Security Target uses the name of each product rather than TOE. For the information about each product, refer to 1.4 Terms and Definition.

72 In the enterprise operating environment of the TOE[4], V3, anti-virus software, is a component of the TOE and installed on the user's computer. Policy server, another component of the TOE, is installed on the central management server, and manages the configuration and audit records of V3. Policy agent installed on the V3 installed system conveys configuration between policy server and V3 as an interface. Policy center admin that manages policy server is located on the trusted network with the policy server. All of TOE components are located on the trusted network and protected by network protection devices such as firewall or intrusion prevention system. The communication among components in the trusted network is encrypted, so the third party can understand the meaning. To manage the policy manager by authorized administrator of APC, the policy server allows authorized administrators to set up and apply configuration of V3 through the policy server by identifying and authenticating the administrators. Depending on the location of Policy Center Admin; installed on the trusted network, or installed on the local network, the policy server has remote access or local access from policy center admin. For the remote access, traffic is encrypted. The following figure is enterprise operating environment of the TOE.

[4] The V3 installed environment without APC is called the personal operating environment. The V3 installed environment with APC is called the enterprise-operating environment. This Security Target provides the enterprise-operating environment of the TOE.



[Figure 1] Enterprise Operating Environment of the TOE

73 Authorized administrators manage the configuration of V3 establishes security policies, and queries audit records through the policy center admin. Authorized administrators also apply Scan/repair policies for viruses to V3 systems through policy server and policy agent. Each V3 system run on the operating system by the configuration the authorized administrator set on the policy server. Authorized general users of V3 also can set scan/repair configurations for viruses. The Security Target introduces two types of V3 users; authorized general users and restricted general users. Restricted general users are allowed to scan/repair viruses but are restricted to set scan/repair configurations. Events and virus scan logs generated by V3 are transmitted to the policy server, and authorized administrators are able to query them and generate statistics/report.

74 Policy agent runs on active and passive mode. In passive mode, if an authorized administrator does not change the security configuration of V3 through the policy server, an authorized general user can operate V3 with his own policy for a long term. Consequently, in passive mode of the policy agent, authorized administrator should restrict the authorized general user by locking the security settings of V3 through the policy server so that an authorized general user cannot change the security settings.

75 To provide integrity and authentication of data transmitting from the update server in the TOE operating environment, The 'Authenticode Singing' verification technique of Microsoft is applied to the V3 and APC update function by using

WinTrust (WinVerifyTrust) API. Besides, a Hash table created by AhnLab and a Hash file for each file are embedded in the transmitted data to verify the integrity of patch and engine files. Also, V3 can be updated by receiving the update file from Policy Server in the same way it is updated in the update server.

76 Policy server uses open LADP v2.7 as a directory server to store configurations' of policy server and V3. As storage of status information and audit records of policy agent and V3, Microsoft SQL Server 2000 is used.

77 For the secure time stamp, policy server synchronizes the time with an NTP server. V3 does not synchronize the time with an NTP server directly but let the operating system where V3 is installed connect to a NTP server, and synchronize the time. V3 just applies to the time of the operating system.

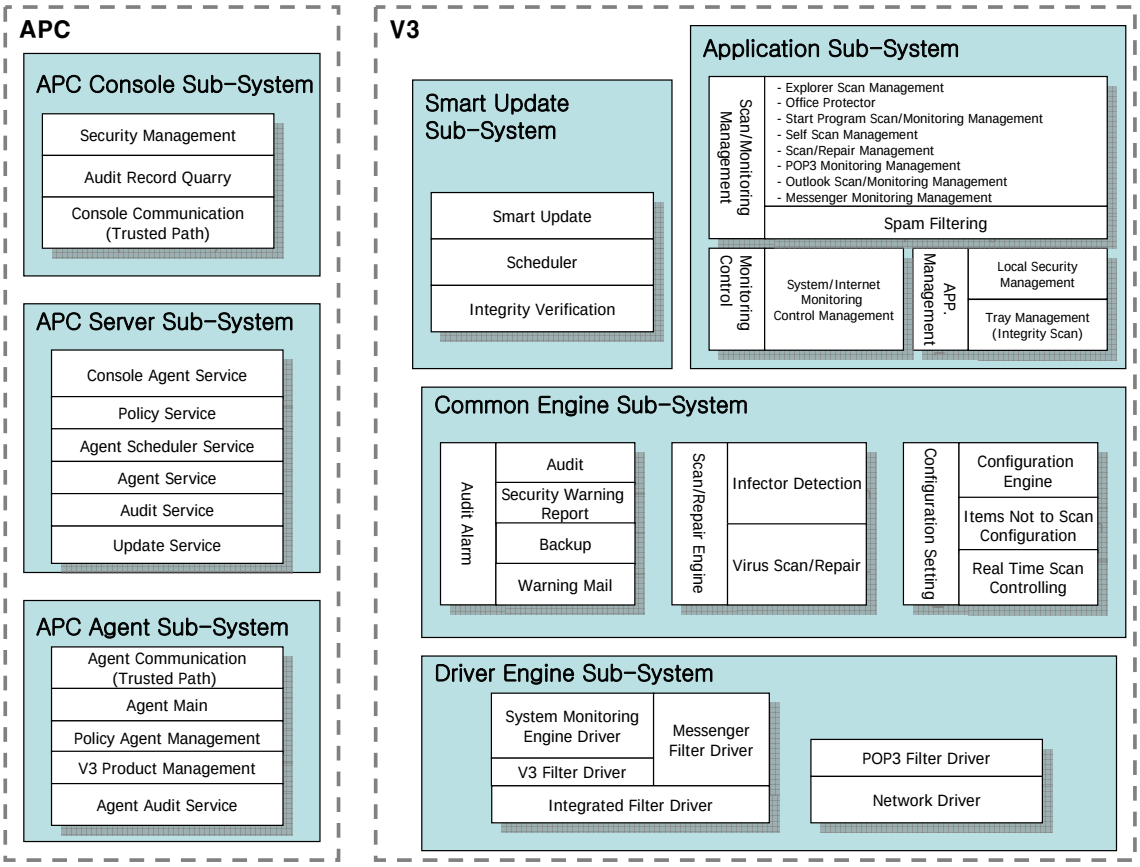
78 The components of the TOE are installed on the following operating systems, and are software that runs on the following hardware.

[Table 1] TOE Platform Environment (Operating System/Hardware)

TOE Component	OS (Required Software)	Hardware (Recommended)
V3	Microsoft Windows XP (Internet Explorer 6.0 or higher - WinSock 2.0 or higher)	CPU: Intel Pentium III or higher RAM: 256MB HDD: 200MB or more NIC : 10/100 Ethernet Card
Policy Agent	Microsoft Windows XP (Internet Explorer 6.0 or higher - WinSock 2.0 or higher)	CPU: Intel Pentium III or higher RAM: 256MB HDD: 200MB or more NIC : 10/100 Ethernet Card
Policy Server	Microsoft Windows 2003 Server (MS SQL Server 2000 SP3 or higher OpenLDAP 2.0 or higher - Windows Installer - WinSock 2.0 or higher)	CPU: Intel Pentium 1GHz or higher RAM: 1GB or more HDD: 5G or more NIC : 10/100 Ethernet Card
Policy Center Admin	Microsoft Windows XP (Internet Explorer 6.0 or higher - WinSock 2.0 or higher)	CPU: Intel Pentium 1GHz or higher RAM: 256MB or more HDD: 200MB or more NIC : 10/100 Ethernet Card

2.2.2 Logical Scope

79 The TOE consists of the logical structure as shown in [Figure 2].



[Figure 2] Logical Boundary of the TOE

80 The Application subsystem provides the authorized user interface (security management screen) to perform security functions of V3, and operates management function to scan/monitor viruses on the system with configuration by general users. The application subsystem requests scan/repair viruses to the common engine subsystem with the request by the plug-in scan on each application (Office Protector, Outlook) or the manual can request by authorized users. The application subsystem also requests to scan/repair its own execution files, and checks the integrity of executable files or configuration files of itself at startup. The subsystem provides not only the scan/repair function but also the port block function.

81 The common engine subsystem applies configurations from users and the APC Server subsystem and security management command (from APC Agent subsystem) to the system. It also scans and repairs viruses, backs the original infection files up, generates audit records, and scans system vulnerability.

82 The Driver Engine subsystem monitors the file system on the V3 installed system, and when an I/O event occurs on a file, the subsystem scans the file in real-time.

V3 registers the information of the monitoring target to the filter driver to support system/Internet/ instant messenger monitoring. After register, the subsystem hooks the data up in case that the transmitting data is scan target. The hooked data by system/Internet monitoring is scanned/repaired. To perform POP3 monitoring, the subsystem hooks up the POP3 packets from the network driver, changes the port number of the packets, and forwards them to the application subsystem to scan.

83 The Smart Update subsystem applies the smart update configurations from authorized general users to the system, and handles update requests. Depending on the update configuration, update files are downloaded from the Internet or network shared folders. Once completing download, integrity scan operates, signatures and patch files are updated. At startup of the operating system, the subsystem requests the operating system to execute real-time scans. The scheduler function runs scheduled scan, screen saver scan, and real-time system scan according to their scheduled time, checking for their scheduled time periodically.

84 The APC Console subsystem transmits policies from authorized administrators to the APC server subsystem, and displays the result. To provide the secure channel for the communication, transmitting data are encrypted (except audit data) with embedding the integrity value. Authorized administrators are allowed to queries audit records of APC and V3.

85 The APC Server subsystem handles commands or policies from authorized administrators. The subsystem exchanges a key for the secure channel with the APC Console subsystem, identifies and authenticates administrators. Direct-commands from the APC Console subsystem are stored in DB and forwarded to the APC Agent subsystem. The results of commands from the APC Agent subsystem are forwarded to the APC Console subsystem. The subsystem stores policies of V3 and the policy agent in LDAP, and sends the command to the APC Agent subsystem to apply the policies. The subsystem stores audit data from APC to DBMS. If V3 requests updates, the subsystem sends the patch/engine files of V3 from the update server.

86 The APC Agent subsystem forwards new or urgent policies from APC server subsystem to V3. By scheduler, the APC Agent subsystem get policies or update information from APC Server subsystem, updates its status on a specific time. If policy Agent installation program or V3 is installed, the APC Agent subsystem registers its own status to APC Server subsystem. Data encryption (except audit records) integrity is provided for the secure channel with the APC Server subsystem. The APC Agent subsystem transmits audit records of V3 which are filtered by log filtering rules to the APC Server subsystem.

87 The TOE provides the following security functions:

- **Update** – Operates auto-update by checking the update information of engine/patch files periodically. To protect engine/patch files for update, authentication and integrity verification are provided. V3 is updated from the update server or the policy server.
- **Virus Scan/Repair** – Operates scan by user, plug-in (windows explorer, Internet explorer, Outlook), scheduler, manual scan by authorized administrators of the policy server, and screen saver scan for the viruses defined by V3-engine. System and application (Outlook, POP3, Instant Messenger, Office, Internet Explorer, Startup Program, and Screen Saver) real-time scan are provided. V3 blocks the detected viruses by moving them to the quarantine station, repairs viruses according to the repair settings, and generates warning alert and audit records for the detection and repair. V3 can restart real-time system scan (monitoring) after a specified time when real-time system scan (monitoring) stops.
- **Spam-mail Filtering and Warning Mail** – During POP3/Outlook real-time scanning (monitoring), V3 blocks mails according to specified rules with subject, message, sender, and recipient. If attachment is infected, V3 sends a warning mail to the sender for notification.
- **Self-Protection** – V3 blocks malicious codes to access V3 during real-time system scanning (monitoring). V3 protects itself by scanning its own processes at startup and system scan and by verifying the integrity of files from the update server. V3 and APC verify integrity and authentication of TSF data, execution files that operates TSF.
- **Audit Record and Report** –V3 generates event log for configuration, scan log for virus scan. It also provides virus and security vulnerability diagnosis result and a report with response information. To protect the audit record trail, V3 allows the authorized administrator to specify the space.
- **Configuration** – V3 allows authorized general user to configure the scan and repair function by providing configuration interfaces, which prevents duplicated scan by allowing authorized general users to set files, folders, and extensions as items not to scan. Easy configuration provides High/Medium/Low/Customized levels for easy and quick configuration. V3 general users are limited to modify their configurations in case that the configuration is locked by APC. If a V3 authorized general user locks his own configuration with the password, other users cannot the configuration. Even though the configuration is not locked by the password, the configuration from APC overwrites the configuration of the system because APC has the highest priority. V3 provides user interfaces to set the configuration related to update such as update method for engine/patch files, scheduled interval.
- **Central Management** – APC (AhnLab Policy Center) provides central management for V3 installed on users' computers. APC sends configuration to a policy agent on the V3 installed system to enforce security policies, and collects virus warnings and events. The policy agent is created by authorized administrator from the policy server, and delivered and installed on the V3 installed system by a web server or an authorized administrator. Authorized administrators queries/set the configuration of V3 through the policy center admin, enforces security policies by checking the latest engine update. As generating, storing, and querying audit data of V3, policy servers is able to queries audit data of themselves. TSF data to set the configuration of policy agents and V3 are transmitted among components (Policy Center Admin-Policy

Server-Policy Agent) of APC with encryption/Hash to protect against exposure. A policy server provides the following functions:

- Identification and Authentication: Identifies and authenticates administrators (including monitor center) of the policy server.

- V3 Configuration: V3 configuration is operated not only by local authorized general users but also by policy servers in the enterprise environment. V3 limits authorized general users to modify configuration of the policy server according to organizational security policies by locking configurations with password. With the locking function, the central management is implemented by pushing configurations from the policy server to V3 periodically to overwrite the local authorized general user's configuration. The update configuration of V3: engine/patch files, update method, update scheduled time, interval time, and operating setting, is operated by an authorized administrator of the policy server. The policy server applies the common configurations to V3 by sending configuration though policy agents in the same domain.

- Policy Agent Management Key Setting: The policy server locks configurations with the password to protect central management via policy agents from the modification of general users: stop, terminate, and delete the policy agent.

- NTP Server Settings: The policy server sets a NTP server to provide a trusted time-stamp by synchronizing not only its own time but also V3 user's system time via policy agents.

- Backup Settings: The policy server provides backup settings to back up configurations of policy agents, V3, and all audit data regularly.

- Notification Settings: The policy server provides the notification status configuration and notice configuration by mail or windows according to the virus infection configuration.

- V3 Group/Policy Agent Management: The policy server creates a group, sends and applies configurations to policy agents in a group consistently. Control management: Installation program management, operating mode, and restarting a policy agent, is provided by a group. Therefore individual configurations of V3 will be consistent by setting and applying configurations by group. The first created group for the configuration of V3 or policy agent takes over the V3 and policy agent's configuration of the default group. Setting and applying configurations by V3 and policy agent is allowed, which means that authorized server/policy administrators are able to set the common configuration by group or individual policy.

- Server Management: Provides APC update configuration, Task Manager (including monitor center), and service operation control.

- Monitor Center: Provides an integrated audit viewer of V3

- Update: Updates V3 engine/patch files from the update server. Therefore, V3 can update v3 engine/patch files from the policy server. The policy

agent checks if the policy server has the latest version of configuration files periodically or updates itself by the policy server's command.

2.2.3 Out of Coverage

88 The following functions are out of scope of V3

Run as a Update Server

89 Without APC, V3 runs as an update server for the other V3s.

V3 + Neo File Update

90 If the operating system is Windows' 9x, they are additional files for support of V3+ Neo. Since the operating system of the TOE is Windows XP, This is out of scope.

91 The following functions are out of scope for policy server.

Hierarchical Domain Management

- **Setting Domain** - Modification of the current domain name, Inherit Parent Domain's configurations' and commands, and Forward Data to Parent Domain. The TOE operating environment does not have multiple policy servers.
- **Setting Parent Domain** - Defines the hierarchy between two or more policy servers in the same network environment. The TOE operating environment does not have multiple policy servers.
- **Log Forwarding Policy** - Sets whether to send logs and events from V3 managed by APC to the parent domain policy server or the domain policy server that manages the policy agent directly. The TOE operating environment does not have multiple policy servers.
- **Setting Auto Grouping** - The registered agent to the policy server will be included in a group according to the auto grouping policy by defined the administrator. The TOE operating environment does not have multiple policy servers.
- **Setting Red Group** - Setting the red group condition for policy agents which can not communicate with the policy server for a specified time. The TOE operating environment does not have multiple policy servers.
-

- **Setting Relay Server Option** - Sets the length of the time limiting communication with the relay policy server. The TOE operating environment does not have multiple policy servers.
- **Management Product Settings** - TOE does not select all management products (V3Net 6.0, V3Pro 2002, V3Net SE, APF 2004, SpyZero, and V3 Internet Security) but select only V3Pro 2004 to manage.
- **Setting Parent Domain as Time Server** - The TOE operating environment does not have multiple policy servers.
- **Domain Status Summary** – Views the domain summary information: domain name, settings, and service status. The TOE operating environment does not have multiple policy servers.

OutBreak Function

92 Requires additional service authentication. This manages the policy of outbreak management service product. The TOE manages only V3Pro 2004.

Proactive Defense Function

93 The functions to set a vulnerable shared folder, block network, set the common configuration and enable the interoperation with TrusGuard by AhnLab are additional features that are irrelavant to Policy Server setting the V3 configuration.

SpyZero Management::

94 APC configures SpyZero, one of products by AhnLab, Inc., controls the commands of SpyZero, and generates reports using audit records. The TOE manages only V3Pro 2004.

V3 Internet Security Management:

95 APC configures V3 Internet Security, one of products by AhnLab, Inc., controls the commands of V3 Internet Security, and generates reports using audit records. The TOE manages only V3Pro 2004.

APF 2004 Management:

96 APC configures APF 2004, one of products by AhnLab, Inc., controls the commands of APF 2004, and generates reports using audit records. The TOE manages only V3Pro 2004.

V3Pro 2002 / V3Net SE Management:

97 APC configures V3Pro 2002 / V3Net SE, the old version of V3Pro 2004 by AhnLab, Inc. The TOE manages only V3Pro 2004.

Group / Policy Agent Additional Function Management:

- **Relay Server Installation / Configuration** - After installation of a relay server, it helps to find the server easily from the group of multiple relay servers. The TOE operating environment does not have multiple policy servers.
- **Secondary Update Server Configuration** - Configures the secondary server to switches in case of failing update from a policy server with multiple policy servers. The TOE operating environment does not have multiple policy servers.
- **Shared Folder Management** - The function to control the shared folder provided by the OS of Policy Agent, which is irrelevant to the function to set the V3 settings.
- **Asset Management** – Fetches the hardware and software installation information from the agent computer to generate a report that is irrelevant to the V3 report.
- **Policy Agent Communication Server Settings** – Sets a new policy server for the policy agent. The TOE operating environment does not have multiple policy servers.
- **Executing Policy Agent Command** – Execute a specific file in the policy agent that is irrelevant to configuring V3.
- **Enforce Policy Agent Registration** - Sets a new policy server for the policy agent. The TOE operating environment does not have multiple policy servers.
- **Unregistered Group Settings** - Displays the information of the V3 installed system without running the policy agent in the domain: IP address, computer name, NT domain name, MAC address, which is irrelevant to configuring V3Pro 2004.
- **Relay Server Patch Upload** – Uploads patch files of the policy server running as a relay server. The TOE operating environment does not have multiple policy servers.

SMS Notification

98 APC uses SMS for notification on the situation that authorized administrator is set. This is out of scope because additional contract with a mobile service provider is necessary for this function.

APC Report

99 APC creates reports with pre-defined formats and audit records. This function is out of scope since it is independent with generating and storing audit records.

APC General Software Distribution

100 APC distributes software or files to V3 installed systems via network, and performs forced installation. To do it, APC manages (adds/deletes) software/files to distribute. If an authorized general user deletes V3, APC can distribute and install V3 on the user's system in case that the system has been registered on the APC.

101 The following functions are out of scope for policy agent.

User Information Input

102 An additional feature for the Policy Agent user (General user authorized by V3) to input the Policy Agent information.

View Notice

103 An additional feature to the text-based notice from the policy server.

Vulnerable Account / Folder Scan

104 An addtional feature for the Policy Agent user (General user authorized by V3) to scan the information of Policy Agent itself.

NAT Configuration

105 An addtional feature to set NAT required for network environment of Policy Agent and the server.

2.2.4 IT Environmental Security Functions

106 V3 and APC provide the following IT environmental security functions:

- **V3 Audit Record Protection (e_V3AuditStorage)** - Audit records from V3 are stored on the file system of the operating system as file type and protected according to the policy of the file system.
- **APC Audit Record Protection (e_APCAuditStorage)** – Audit records from APC are stored in the DBMS, which provides access control to the audit record storage.

- **Review Audit Record of APC (e_APCAuditSearch)** – Querying audit records is operated by not TSF of APC but DBMS since APC uses DBMS as an audit record storage.
- **V3 Identification and Authentication (e_V3AccessINA)** – **V3 Identification and Authentication (e_V3AccessINA)** – V3 users must login to the operating system where V3 is installed to scan/repair settings. If screen saver is enabled on the V3 installed system, V3 users must re-login to the system to use V3. If a V3 user does not use the V3-installed operating system for a specified time set by the authorized/restricted general user, V3 enables screen saver to lock the session of the user's computer.
- **Reliable Time (e_TimeStamp)** – Uses NTP or OS system time to provide reliable time stamps for V3.
- **Secure Certificate Verification Structure (e_TrustCertFrame)** –In updating, the TOE use Microsoft Code Signing technique to verify authentication and integrity of update files. Since the authentication is performed based on the certificate, V3 uses Internet Explorer for verifying the certificate. The TOE also performs self-verification which verifies its own files by using the Code Signing technique

3. TOE Security Environment

107 This chapter defines security threats, assumptions, and organizational security policies related to the TOE

3.1 Assumptions

Assumption	Description
A.NO_EVIL	The authorized general users (V3) and authorized administrators (APC) of the TOE shall not have any malicious intention, receive proper training on TOE management, and follow the user (V3)/administrator (APC) guidelines.
A. PHYSICAL	The policy server is installed in physically safe environment, and protected by un-authorized access.
A.SAFEITENTITY	The update server for the TOE, administrator's computers for security management functions, and the NTP server are secure.
A.TIMESTAMP	The time stamp referred to the NTP server or operating system is reliable.
A.CERT	The certificate being used to verify engine/patch files from the update server are issued in a secure manner and stored/managed by AhnLab, Inc. To verify engine/patch files signed by the certificate, the reliable authentication agency of the Internet Explorer on the V3 or policy server installed system must be up-to-date.
A.GUARD	The TOE is installed on the trusted network where is protected by network security devices (firewall). The trusted network is protected by the security policies of network security devices.
A.INTERNALENTITY	IT entities connected to the trusted network and interoperate with the TOE are run with the same security level according to the security policies of network security devices.
A.AVCONFLICT	The V3 installed system does not have any other anti-virus software, and software with POP3 real-time scan (monitoring), and spam mail filtering.

3.2 Threats

108 The threat agent possesses a low level of knowledge, resource, and motivations. The threat agent is a user without authority for using the TOE or a process.

Threat	Description
T.AUDIT_COMPROMISE	The threat agent may damage or modify audit records taking unauthorized access authority for the audit trail or prevent security related events from being recorded.
T.MASQUERADE	The threat agent may take unauthorized access authority for data or

	TOE resource by masquerading as other entity.
T.TSF_COMPROMISE	The threat agent may access (views, modify, or delete) TSF data or executable code irrelevantly by simple attack.
T.UNATTEND_SESS	The threat agent may take unauthorized access for idle sessions.
T.UNIDENTIFIED_ACTIONS	Authorized administrator may not response for potential security violations which are not identified or warned by authorized administrators or authorized general users
T.VIRUS	Virus may come into user's computer via network traffic or removable media, which may harm his own computer and other computers.
T.DOWN_INTERFERENCE	The TOE may receive wrong update files from threat agent when updating engine/patch files from the update server.
T.TRANS_DESTORY	The threat agent may expose and modify TSF data between policy server and policy center admin, and policy server and policy agent by using unauthorized methods.
T.RESIDUAL_DATA	Unauthorized subject may access TSF data by re-allocating memory used for scan/repair process or handling request of authorized general users (V3) or authorized administrators (APC).

3.3 Organizational Security Policies

Policy	Description
P.ROLES	The TOE provides authorized security management roles to manage the TOE in a secure manner: server administrator, policy administrator, monitor center, authorized general user, and restricted general user. These roles shall be separated clearly from other users.
P.AUDIT	To trace responsibilities of all security-related behaviors, all security-related events shall be stored, maintained, and the record data shall be reviewed in a variety ways.
P.MANAGEUTIL	Management tools are provided for authorized general users (V3) or authorized administrators (APC to manage the TOE in a secure manner, and V3 policies set by authorized administrators has higher priority than by authorized general user.
P.ANTIHAMFULL	The TOE shall filter 'Advertisement, Adult Advertisement" by spam prevention rules, and scan key logger programs defined as harmful program by AhnLab, Inc.
P.STRENGTHENOS	Authorized general users or authorized administrators shall review the vulnerabilities to guarantee the normal operation and stability by reinforcement of vulnerabilities of the operating system and applications which are necessary to run the TOE.

4. Security Objectives

4.1 TOE Security Objectives

Objective	Description
O.ADMIN_ROLE	The TOE shall provide security management roles to separate management behaviors.
O.MANAGE	The TOE shall provides secure means and management functions for authorized general users (V3) or authorized administrators (APC) to efficiently manage the TOE
O.SELF_PROTECTION	The TOE shall provide protect TSF and TSF resource from unauthorized modification via TSFI.
O.VIRUS	The TOE shall identify and response for well-known viruses that come from removable media or network traffic, and filter spam mails.
O.AUDIT	The TOE shall provide store and maintain security-related events to trace responsibilities of security-related behaviors, and provide means for the authorized users to review the audit data.
O.ALARM	The TOE shall provide methods to alert authorized general users and authorized administrators for security threats.
O.TSFDATA_PROTECT	The TOE shall protect TSF data transmitted between separated TOEs from the exposure and modification.
O.INA	The TOE shall identify and authenticate authorized administrators (APC).
O.SECURE_UPDATE	The TOE shall store engine/patch files from the update server, check their integrity, and verify whether they are developed by AhnLab, Inc.
O.STRENGTHENOS	The TOE shall provides means to review if vulnerabilities to guarantee the normal operation and stability, and the reinforcement of vulnerabilities of the operating system and applications which are necessary to run the TOE.

4.2 Security Objectives for the Environment

Objective	Description
OE.AUDIT_STORAGE	The IT environment shall provide means to store audit files of the TOE in a secure manner.
OE.NO_EVIL	The authorized general users (V3) and authorized administrators (APC) of the TOE shall not have any malicious intentions, receive proper training on the TOE management, and follow the user (V3)/administrator (APC) guidance.
OE.PHYSICAL	The TOE shall be located in a physically safe environment, and protected from the unauthorized access.
OE.CERT	The certificate being used to verify engine/patch files from the update server is issued in a secure manner and stored/managed by AhnLab, Inc.

	To verify engine/patch files signed by the certificate, the reliable authentication agency of the Internet Explorer on the V3 or policy server installed system must be up-to-date.
OE.SAFEITENTITY	The update server for the TOE, administrator's computers for security management functions, and NTP server (or operating system providing the time stamp) shall secure.
OE.TIMESTAMP	The IT environment shall provide reliable time stamps from the NTP server or the operating system.
OE.TOE_ACCESS	The IT environment shall provide means to control logical access of users to the TOE.
OE.GAURD	The TOE is installed on the trusted network where is protected by network security devices (firewall). The trusted network is protected by the security policies of network security devices.
OE.INTERNALENTITY	IT entities connected to the trusted network and interoperate with the TOE are run with the same security level according to the security policies of network security devices.
OE.AVCONFLICT	The V3 installed system does not have any other anti-virus software, and software with POP3 real-time scan (monitoring), and spam mail filtering.
OE.AUDIT_SEARCH	The IT environment shall provide the search function for the audit records.
OE.RESIDUAL_INFO	The IT environment shall protect resources in the scope of control of the TOE from exposing them to users when re-allocating the memory.
OE.DOM_SEPARATION	The IT environment shall provide separated areas for executing of the TOE.
OE.NO_BYPASS	The IT environment shall not allow the bypass of the security mechanisms since the access authority to the TOE resource can be taken.

5. IT Security Requirements

109 This chapter specifically describes security functions and assurance requirements for the TOE. The author depicts all requirements by referring to the Common Criteria [1].

5.1 TOE Security Requirements

5.1.1 Overview

5.1.1.1 Summary

110 The components shown [Table 2] are referred to the part 2 of the Common Criteria [1], and the following is extended components of the part 2 of the Common Criteria [1].

- FAV_ACT.1 Anti-Virus Response
- FAV_ALR.1 Anti-Virus Alert
- FAV_SCN.1 Anti-Virus Scan
- FAV_SPM.1 Spam Mail Block
- FTA_SSL.4 Administrator-initiated Termination

[Table 2] Security Functional Requirements

Component ID	Component Name
FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAA.1	Potential Violation Analysis
FAU_SAR.1(1)	Audit Review (General User-V3)
FAU_SAR.1(2)	Audit Review(Authorized Administrator-APC)
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_STG.4	Prevention of Audit Data Loss
FAV_ACT.1 (extension)	Anti-Virus Response
FAV_ALR.1 (extension)	Anti-Virus Alert
FAV_SCN.1 (extension)	Anti-Virus Scan
FAV_SPM.1 (extension)	Spam Mail Block

FIA_AFL.1	Authentication Failure Handling
FIA_SOS.1	Verification of Secrets
FIA_UAU.2	User Authentication before any action
FIA_UAU.6	Re-authenticating
FIA_UID.2	User Identification before any action
FMT_MOF.1	Management of Security Functions Behavior
FMT_MTD.1	Management of TSF Data
FMT_MTD.2	Management of Limits on TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_AMT.1	Abstract Machine Testing
FPT_ITI.1	Inter-TSF Detection of Modification
FPT_ITT.1(1)	Basic Internal TSF Data Transfer Protection(Policy Server-Policy Center Admin)
FPT_ITT.1(2)	Basic Internal TSF Data Transfer Protection(Policy Server-Policy Agent)
FPT_TST.1	TSF Testing
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4(extension)	Administrator-initiated Termination

5.1.1.2 TOE SOF (Strength of Function)

111 Security functional requirements' in this Security Target conform to SOF-medium specified in the Common Criteria for the Information Protection System.

5.1.2 TOE Functional Requirements

FAU_ARP.1 Security Alarms

Hierarchical to: No other components'.

Dependencies: FAU_SAA.1 Potential Violation Analysis

112 FAU_ARP.1.1 The TSF shall take [the following responses] upon detection of a potential security violation.

a) Sending e-mail to authorized administrators.

b) Sending notification (Policy Server)

c) Alarm on the security management screen or by using a tray message.

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components'.

Dependencies: FPT_STM.1 Reliable Time Stamps

113 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit function.

b) All events subject to auditing according to the *None* audit level.

c) [See [Table3] Audit Target Events]

114 FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identify, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the Security Target, [the following information related to the audit target events]

- Virus scan and response log: Infection Owner, Access, infector
- Task Management: Target, Task ID
- Update Service: Management Product, Components

[Table3] Audit Target Events

Component	Audit Target Event
FAU_ARP.1	N/A
FAU_GEN.1	N/A
FAU_GEN.2	N/A
FAU_SAA.1	Enabling and disabling of and of the analysis mechanisms' (Start-up and shut-down of the audit function).
FAU_SAR.1(1)	N/A
FAU_SAR.1(2)	N/A
FAU_SAR.2	N/A
FAU_SAR.3	N/A
FAU_STG.4	N/A
FAV_ACT.1 (extension)	Virus Repair
FAV_ALR.1 (extension)	N/A
FAV_SCN.1 (extension)	Virus Scan
FAV_SPM.1 (extension)	Spam Mail Block
FIA_AFL.1	N/A
FIA_SOS.1	N/A
FIA_UAU.2	All use of the authentication mechanism.
FIA_UAU.6	All attempts of re-authentication
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.
FMT_MOF.1	All behaviors of the update function. Start/stop Virus scan and real-time scan Start/stop of the successful self-protection function Start/stop of the successful integrity scan Succeed/Fail of start/stop/restart a service Agent restart/activation mode/status check/delete successful Policy Agent and V3 configuration
FMT_MTD.1	All modification of the administrator account and password.
FMT_MTD.2	N/A
FMT_SMF.1	N/A
FMT_SMR.1	Modification to the group of users that are part of a role.
FPT_AMT.1	N/A
FPT_ITI.1	N/A
FPT_ITT.1(1)	The detection of modification of transmitted TSF Data.
FPT_ITT.1(2)	The detection of modification of transmitted TSF Data.
FPT_TST.1	Verification of integrity
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.
FTA_SSL.4(extension)	Termination of an interactive session by the session locking mechanism.

FAU_GEN.2 User Identity Association

Hierarchical to: No other components'.

Dependencies: FAU_GEN.1 Audit Data Generation, FIA_UID.1 Timing of Identification

115 FAU_GEN.2.1 The TSF shall be able to associate each auditable event which the identity of the user that caused the event.

FAU_SAA.1 Potential Violation Analysis

Hierarchical to: No other components'.

Dependencies: FAU_GEN.1 Audit Data Generation

116 FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

117 FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [the following events] known to indicate a potential security violation:

- Failure of starting a service in the Policy Server
- The authorized server administrator in the V3 installed system transmits the 'scan log' of the virus to the policy server.
- Failure of the V3 engine update
- One or more items whose level of security vulnerability is 'dangerous', and the priority is higher than 'medium' exist.
- Other processes except the V3 process access V3 installation directory.

b) [Completion of V3 update download, completion of the policy server update download]

FAU_SAR.1(1) Audit Review(authorized general user/restricted general user-V3)

Hierarchical to: No other components'.

Dependencies: FAU_GEN.1 Audit Data Generation

118 FAU_SAR.1.1 The TSF shall provide [authorized general user/restricted general user] with the capability to read [all audit records] from the V3 installed-system.

119 FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1(2) Audit Review(authorized administrator-APC)

Hierarchical to: No other components'.

Dependencies: FAU_GEN.1 Audit Data Generation

120 FAU_SAR.1.1 The TSF shall provide [authorized administrator] with the capability to read [V3 and APC audit records] from the policy server.

121 FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

122 Application Note: Authorized server administrators are allowed to view the details of audit records generated from 'Server Task Control', 'Task History Management', 'Update Server Setting Management', and 'Backup Management'.

FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components'.

Dependencies: FAU_SAR.1 Audit Review

123 FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components'.

Dependencies: FAU_SAR.1 Audit Review

124 FAU_SAR.3.1 The TSF shall provide the ability to perform [searches, sorting] of audit data based on [the following criteria with logical relations].

a) Event log

- Search: Period AND Type (normal AND error AND warning)
- Sorting: Date AND (type OR time OR function name OR message)

b) Scan log

- Search: Period AND Status (Before Repair-Repairable AND Scheduled to Repair AND New Virus AND Compression File AND After Repair-Repair Completed AND Failed to Repair AND Deleted AND Change Name)

- Sorting: Date AND (Time OR Infected File Name OR Virus Name OR Status OR Scan Method OR Owner OR Access OR infector)

125 Application Note: This security functional requirement is only applied to V3. Since the policy server store/search audit records by using DBMS, the policy server is not applied to this requirement.

FAU_STG.4 Prevention of Audit Data Loss

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected Audit Trail Storage

126 FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [None] if the audit trail is full.

127 Application Note: The audit trail is full means that the amount of audit records exceeds the space set by the server administrator/policy administrator (APC) or authorized general user (V3).

FAV_ACT.1 Anti-Virus Response

Hierarchical to: No other components'

Dependencies: FAV_SCN.1 Anti-Virus Scan, FAV_ALR.1 Anti-Virus Alert, FMT_SMR.1 Security Roles

128 FAV_ACT.1.1 The TSF shall the following responses for the file viruses, which may be set by authorized general users or authorized server administrator and policy administrator

a) Backup infected original files

b) Leave as is

c) Repair

d) Delete

e) Recompress

f) Repair after forced termination

g) Restart the system after the Repair

h) Change the extension of the file

i) Block

129 FAV_ACT.1.2 The TSF shall block the viruses in the advance scan as follows:.

a) Memory Virus – blocks/repairs viruses which run in the memory.

b) Boot Sector Virus – blocks/repairs viruses which run at the next boot.

c) Process Virus – blocks/repairs viruses which run on the process.

d) Startup Program Virus – blocks/repairs viruses registered/installed on the startup program

e) TSF executable code virus – blocks/repairs viruses before V3 execution codes (files) execute.

FAV_ALR.1 Anti-Virus Alert

Hierarchical to: No other components'.

Dependencies: FAV_SCN.1 Anti-Virus Scan, FMT_SMR.1 Security Roles

130 FAV_ALR.1.1 The TSF shall display warning window or alarm when a virus is detected. The warning windows shall show the virus name and response list.

131 FAV_ALR.1.2 The TSF shall keep the warning window until the authorized user recognizes it or the user session is closed.

132 FAV_ALR.1.3 The TSF shall send a warning mail to the recipient when receiving an infected mail.

FAV_SCN.1 Anti-Virus Scan

Hierarchical to: No other components'.

Dependencies: FMT_SMR.1 Security Roles

133 FAV_SCN.1.1 The TSF shall provide the following scans based on the well-known virus engine for the file viruses.

a) Scan requested by security roles in FMT_SMR.1

b) Scheduled scan at a specified interval in FMT_SMR.1

c) Scan when the windows screen saver runs

d) Manual scan requested by the following software's plug-in

- Microsoft Outlook
- Windows Explorer

e) Real time scan during the following software are running (Monitoring)

- System: File I/O
- Internet Explorer
- Instant Messenger
- Windows Startup Program

- Mail Client using the POP Protocol
- Microsoft Office
- Microsoft Outlook

134 FAV_SCN.1.2 The TSF shall perform advance scan based on the well-known virus engine for the following viruses.

a) Memory Virus

b) Boot Sector Virus

c) Process Virus

d) Startup Program Virus

e) TSF executable code virus

FAV_SPM.1 Spam Mail Block

Hierarchical to: No other components'.

Dependencies: FMT_MTD.1 Management of TSF Data

135 FAV_SPM.1.1 The TSF shall enforce the [spam block] based on the following subject and information security attributes:

a) Subject: security attributes of mail – sender, account of the sender

b) Information: Outlook or security attribute of email transferred via POP3 – subject, message, and recipient

136 FAV_SPM.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [if the security attribute of the subject or information coincides with words defined by the authorized general user with the following conditions, the mail is blocked]

a) Include any OR

b) Include all OR

c) Not include any OR

d) Not include all

137 FAV_SPM.1.3 The TSF shall explicitly authorize an information flow based on the following rules: [authorized sender account list]

138 FAV_SPM.1.4 The shall explicitly deny an information flow based on the following rules:

a) Unauthorized sender account list

b) The default rule

FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components'.

Dependencies: FIA_UAU.1 Timing of Authentication

139 FIA_AFL.1.1 The TSF shall detect when *[3]* times of unsuccessful authentication attempts occur related to [administrator's authentication attempt].

140 FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [delay authentication for 1 – 60 minutes defined by the authorized administrator].

141 Application Note: This requirement is only applied to APC.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components'.

Dependencies: No dependencies.

142 FIA_SOS.1.1 TSF shall provide a mechanism to verify that secrets meet [the following limit].

a) The password must be more than 6 and less than 40 characters with combination of alphabetic characters, one or more numbers and special characters.

b) The following characters are available: (Total: 94)

- a – z (26)
- A – Z (26)
- 0 – 9 (10)
- Special Symbol: ~ ! @ # $ % ^ & * ( ) _ + | ` – = ₩ { } : ” < > ? [ ] ; ’ , . / (32)

143 Application Note: The policy server shall provide a mechanism which meets SOF-medium for the password, secrets of the authorized administrator used for login.

FIA_UAU.2 User Authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 Timing of Authentication

144 FIA_UAU.2.1 The TSF shall require each administrator to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that administrator.

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components'.

Dependencies: No dependencies.

145 FIA_UAU.6.1 The TSF shall re-authenticate the administrator under the conditions [session termination by FTA_SSL.3, and FTA_SSL.4(extension)].

FIA_UID.2 User Identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

146 FIA_UID.2.1 The TSF shall require each **administrator** to identify itself before allowing any other TSF-mediated actions on behalf of that **administrator.**

FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components'.

Dependencies: FMT_SMF.1 Specification of Management Functions,
FMT_SMR.1 Security Roles

147 FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior, stop, and start* the functions [function list on the following table] to [authorized roles on the following table].

Function \ Authorized Role	Authorized General User	Restricted General User	Authorized server administrator	Authorized Policy Administrator	Authorized monitor staff
Virus Scan/Repair	*stop, start, determine the behavior*	*stop, start, determine the behavior*	*stop, start, determine the behavior*	*stop, start, determine the behavior*	-
Advance Scan	*stop, start*	-	*stop, start*	*stop, start*	-
Spam Mail Filtering	*stop, start*	-	-	-	-
Warning Mail	*stop, start*	-	*stop, start*	*stop, start*	-
Alert Icon Indication	*stop, start*	-	*stop, start*	*stop, start*	-
Self Scan	*stop, start, determine the behavior*	-	*stop, start, determine the behavior*	*stop, start, determine the behavior*	-
Setting Disk Space to Prevent the loss of TSF data - Whether to save the scan logs - Space to save scan logs - Space to save event logs	*stop, start, determine the behavior*	-	-	-	-

- Space to save backup folders					
V3 Engine/Patch file Update	*stop, start, determine the behavior*	-	*stop, start, determine the behavior*	*stop, start, determine the behavior*	-
Update Integrity Scan	*stop, start*	-	*stop, start*	*stop, start*	-
security warning report	*determine the behavior*	*determine the behavior*	-	-	-
View Update Information	*stop, start*	-	*stop, start*	*stop, start*	-
V3 Configuration Security (Setting Password)	*stop, start*	-	*stop, start*	*stop, start*	-
V3 Integrity Scan by User's Request	*determine the behavior*	*determine the behavior*	-	-	-
Use Items Not to Scan	*stop, start*	-	*stop, start*	*stop, start*	-
Check System Restore Folder	*stop, start*	-	*stop, start*	*stop, start*	-
Self Protection	*stop, start*	-	*stop, start*	*stop, start*	-
APC Log Forwarding Policy Setting	-	-	*determine the behavior*	-	-
APC Time Stamp Server Configuration	-	-	*stop, start, determine the behavior*	-	-
APC Notification	-	-	*determine the behavior*	-	-
APC Integrity Scan	*determine the behavior*	-	*determine the behavior*	*determine the behavior*	*determine the behavior*
Restart Policy Agent Policy Agent Mode Check Policy Agent Status Delete Policy Agent Check and Request Policy Agent Update Version	-	-	*determine the behavior*	*determine the behavior*	-
Policy Agent Configuration	-	-	*determine the behavior*	*determine the behavior*	-
Stop Policy Server Service Start Policy Server Service Restart Policy Server Service	-	-	*determine the behavior*	-	-
APC Update			*determine the behavior*		

148 Application Note: An authorized general user is allowed to perform integrity scan for the policy agent on 'APC integrity scan', and an authorized administrator is allowed to perform integrity scan for the policy server and policy center admin.

FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components'.

Dependencies: FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security Roles

149 FMT_MTD.1.1 The TSF shall restrict the ability to [operations on the following table] to [authorized roles on the following table].

Authorized Role / TSF data List	Authorized General User	Restricted General User	Authorized server administrator	Authorized Policy Administrator	Authorized monitor staff
Home Information - Engine Update Date - Real Time Monitoring Status - Schedule Setting - Last Scan Activities	*[view]*	*[view]*	*[view]*	*[view]*	*[view]*
event log data	*delete, [save as file]*	*delete, [save as file]*	-	-	-
scan log data	*delete, [save as file]*	*delete, [save as file]*	-	-	-
quarantine station Information	*query, delete, [view, Restore, Restore to the temporary folder, Submit to AhnLab Security E-Response, View Properties]*	*query, delete, [view, Restore, Restore to the temporary folder, Submit to AhnLab Security E-Response, View Properties]*	-	-	-
Security warning report	*[view, save as file]*	*[view, save as file]*	-	-	-
V3 Virus Scheduled Scan - Schedule List Data (Schedule Interval, Scan List)	*modify, delete, [view, add]*	-	*modify, delete, [view, add]*	*modify, delete, [view, add]*	*[view]*
Items Not to Scan	*modify, delete, [view, add]*	-	-	-	-
V3 Configuration Security Functional Data (Configuration Password)	*modify*	-	*modify*	*modify*	-
Warning Mail	*modify, [view]*	-	*modify, [view]*	*modify, [view]*	-
V3 Update Configuration Data	*modify, delete, [view, add]*	-	*modify, delete, [view, add]*	*modify, delete, [view, add]*	*[view]*
Spam Prevention Rule Data	*modify, delete, [view, add]*	-	-	-	-

POP3 Real Time Scan – Port, Timeout Setting	*modify, [view]*	–	–	–	–
Administrator Account Information	–	–	*modify, delete, [view, add]*	–	–
APC Update Configuration Data	–	–	*modify, [view]*	–	–
Authorized Administrator Account Password	–	–	*modify*	*modify*	*modify*
Policy Agent Management Key Data	–	–	*modify*	–	–
Notification Configuration	–	–	*delete, [view, add]*	–	–
Policy Agent Management Information	–	–	*[view, Save as File]*	*[view, Save as File]*	*[view]*
Hardware/Software Information	–	–	*[view]*	*[view]*	*[view]*
APC Status Summary Information	–	–	*[view]*	–	–
Backup Configuration	–	–	*modify, delete, [view, add]*	–	–
Audit data stored in the Policy Server	–	–	*delete, [view, Save]*	*delete, [view, Save]*	*[view]*
Policy Server Service Status Policy Agent Policy Status	–	–	*[view]*	–	–
Policy Server Service Setting	–	–	*modify, [view]*	–	–
Policy Agent configuration policy file			*delete*	*delete*	

150 Application Note: The authorized server administrator is able to modify the password of all administrators, and the authorized policy administrator and the authorized monitor staff are able to modify only their own password.

FMT_MTD.2 Management of Limits on TSF Data

Hierarchical to: No other components'.

Dependencies: FMT_MTD.1 Management of TSF Data,
FMT_SMR.1 Security Roles

151 FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [as follows] to [authorized general user, authorized server administrator].

a) Space for V3 scan log – authorized general user

b) Space for V3 event log – authorized general user

c) Space for V3 file backup folder – authorized general user

d) CPU/Memory/Hard disk threshold of Notification Status Settings – Authorized server administrator

152 FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed the indicated limits: [the following].

a) Space for V3 scan log – Response specified in FAU_STG.4

b) Space for V3 event log – Response specified in FAU_STG.4

c) Space for V3 file backup folder – Overwrite the oldest backup file.

d) CPU/Memory/Hard disk threshold of Notification Status – sending email to the accounts specified by the authorized server administrator, notice notification

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components'.

Dependencies: No dependencies.

153 FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) TSF behavior management

b) TSF data management

c) Management of limits on TSF data

d) Easy Configuration – V3 security level (Customized, Low, Medium, High)

e) Create, delete, search policy agent installation program

f) Register and delete policy agent patch program

g) Set and apply the default of V3 configuration and policy agent

FMT_SMR.1 Security Roles

Hierarchical to: No other components'.

Dependencies: FIA_UID.1 Timing of Authentication

154 FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator (server administrator, policy administrator, and monitor center), authorized general user, and restricted general user].

155 FMT_SMR.1.2 The TSF shall be able to associate users with roles.

156 Application Note: Authorized administrator (server administrator, policy administrator, and monitor center), authorized general user, and restricted general user can be associated with the roles.

FPT_AMT.1 Abstract Machine Testing

Hierarchical to: No other components'.

Dependencies: No dependencies.

157 FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, at the request of an authorized user* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlines the TSF.

FPT_ITI.1 Inter-TSF Detection of Modification

Hierarchical to: No other components'.

Dependencies: No dependencies.

158 FPT_ITI.1.1 The TSF shall provide the capability to detect the modification and masquerade of all TSF data during transmission between the TSF and a remote trusted update server within the following metric: [The digital signature created by the corresponding private key shall be verified by the certificate, and the received Hash and the Hash of the original integrity verification target file shall be identical].

159 FPT_ITI.1.2 The TSF shall provide the capability to verify the modification and masquerade of all TSF data transmitted between the TSF and a remote update server within the following metric: [Stop update after generating audit record and delete engine/patch files].

FPT_ITT.1(1) Basic Internal TSF Data Transfer Protection(Policy Server-Policy Center Admin)

Hierarchical to: No other components'.

Dependencies: No dependencies.

160 FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

161 Application Note: TSF data transfer protection is required between the policy server and the policy center admin.

FPT_ITT.1(2) Basic Internal TSF Data Transfer Protection(Policy Server-Policy Agent)

Hierarchical to: No other components'.

Dependencies: No dependencies.

162 FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

163 Application Note: This requirement is to implement the secrecy of the TSF data between the policy agent on the V3 installed system and the policy server.

FPT_TST.1 TSF Testing

Hierarchical to: No other components'.

Dependencies: FPT_AMT.1 Abstract Machine Testing

164 FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, at the request of the* **authorized general user, server administrator, and policy administrator** to demonstrate the correct operation of the *parts of TSF*.

165 FPT_TST.1.2 The TSF shall provide **authorized administrators and restricted general users** with the capability to verify the integrity of *parts of TSF data*.

166 FPT_TST.1.3 The TSF shall provide **authorized administrators and restricted general users** with the capability to verify the integrity of stored TSF executable code.

167 Application Note: The self tests to demonstrate the correct operation of TSF shall run before the TSF processes are operated. This allows you to test all processes of V3 at start-up, or individual process of V3 at the request of user, which are interpreted as the start-up self test. The authorized server administrator verifies the integrity of the policy server, and the authorized/restricted general user verifies the integrity of V3.

FTA_SSL.3 TSF-initiated Termination

Hierarchical to: No other components'.

Dependencies: No dependencies.

168 FTA_SSL.3.1 The TSF shall terminate an interactive session after an [idle time (minute) set by authorized server administrator].

FTA_SSL.4 Administrator-initiated Termination

Hierarchical to: No other components'.

Dependencies: No dependencies.

169 FTA_SSL.4.1 The TSF shall terminate an interactive session after [logout request from the authorized administrator through the security management].

5.1.3 IT Environment Requirements

170 This Security Target provides functional requirements for IT environment. The requirements are referred to the part 2 of the Common Criteria [2].

[Table 3] IT Environment Requirement

Component	Name
FAU_SAR.3	Selectable Audit Review
FAU_STG.1	Protected Audit Trail Storage
FIA_UAU.2	User Authentication before any action
FIA_UAU.6	Re-authenticating
FIA_UID.2	User Identification before Any Action
FPT_STM.1	Reliable Time Stamps
FTA_SSL.1	TSF-initiated Session Locking

FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components'.

Dependencies: FAU_SAR.1 Audit Review

171 FAU_SAR.3.1 The **IT environment** shall provide the ability to perform *searches, ordering* of audit data based on [standard for the following logical relations].

a) Event log – Period, Type (Normal, Error, Warning)

b) Scan log – Period, Status (Before Repair-Repairable, New Virus, Compressed File, After Repair-Repair Completed, Failed to Repair, Deleted, Change Name)

172 Application Note: The audit searching security function is provided by the IT environment since the policy server stores audit data in SQLDB via DBMS.

FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components'.

Dependencies: FAU_GEN.1 Audit Data Generation

173 FAU_STG.1.1 The **IT environment** shall protect the stored audit records from unauthorized deletion.

174 FAU_STG.1.2 The **IT environment** shall be able to *prevent* unauthorized modification to the stored audit records in the audit trail.

175 Application Note: This requirement provides access control of the audit records for DBMS if APC is the IT environment for V3.

FIA_UAU.2 User Authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 Timing of Authentication

176 FIA_UAU.2.1 The IT environment shall require each general user to be successfully authenticated before allowing any other TSF-medicated actions on behalf of that user.

177 Application Note: This applies to the IT environment of V3.

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components'.

Dependencies: No dependencies

178 FIA_UAU.6.1 The IT environment shall re-authenticate the user under the conditions [session locking during the idle time].

179 Application Note: This applies to the IT environment of V3.

FIA_UID.2 User Identification before Any Action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

180 FIA_UID.2.1 The IT environment require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

181 Application Note: Before using V3, the V3 user shall be identified on the operating system.

FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components'.

Dependencies: No dependencies.

182 FPT_STM.1.1 The IT environment shall be able to provide reliable time stamps for its own use.

183 Application Note: The time stamps which guarantees the sequential generation of audit data shall be provided for this requirement.

FTA_SSL.1 TSF-initiated Session Locking

Hierarchical to: No other components'.

Dependencies: FIA_UAU.1 Timing of Authentication*

* - [This Security Target selects FIA_UAU.2 which is hierarchical to FIA_UAU.1.

184 FTA_SSL.1.1 The IT environment shall lock an interactive session after [the idle time set by the user].

a) Clearing or overwriting display devices, making the current contents unreadable

b) Disabling any activity of the user's data access/display devices other than unlocking the session.

185 FTA_SSL.1.2 The IT environment shall require the following events to occur prior to unlocking the session: [re-authentication].

6. TOE Summary Specification

186 This chapter describes the security functions of the TOE and how the functions meet the security requirements described in chapter 5.

6.1 TOE Security Functions

6.1.1 V3 Update (V3_SmartUpdate)

187 V3 receives engine/patch files from the update server or the policy server. The smart update program, one of the subsystems of V3, performs auto-update receiving engine and patch files from the update server at a schedule time by the scheduler. What is more, the update is performed at a request of an authorized general user of V3. The smart update program operates the scheduled tasks in the logged-in session of authorized/restricted general users on the operating system.

188 If an authorized server/policy administrator requests the 'manual update', V3 connects to the update server to perform the update. The policy server stores the latest engine/patch files through the APC update (APC_Update) security function, and works as the update server when receiving the update request from V3.

189 The smart update carries out by comparing the engine versions in the update server and V3 and registers itself to the scheduler to run in the next cycle.

190 The smart update must authenticate the license of V3 before receiving engine/patch files from the update server. The smart update system on V3 requests authentication by transmitting V3 user information such as the product number of V3 to the update server. The update server confirms the user information and returns the result to the smart update subsystem on V3. V3 whose product number is authenticated conducts the update by connecting to the update server.

191 V3 also performs the update through the network drive shared folder. It means that in addition to the update server or APC server of V3, it can be the V3 system with engine/patch files already received or the secure network server that independently stores the engine/patch files only. The corresponding system shares the folder in which the V3 engine is located to connect every time performing the update by setting UNC (Universal Naming Convention) information), user account ID, and password for the connection to the network drive shared folder.

192 After the successful download, V3 verifies the integrity of the downloaded files by comparing the Hash list and Hash of the downloaded files. The verification method

is V3_CodeSigning. If the verification succeeds, the smart update program applies the downloaded files to V3.

193 V3 provides the following configurations for the update:

- Selecting the update target: products (V3, smart update) or files (engine, patch) for the update.

- Selecting an update method: Update through the Internet, or Update the shared network folder. When selecting Update through the Internet, you can set the maximum retires. When selecting Update through the shared network folder, you can set user name, password, and shared folder information to access the shared folder.

- Displaying the version and the contents of updated V3 engine. Configurations of authentication/integrity scan.

- Update configurations: schedule setting (time and interval) for the auto-update or update at an authorized general user's request

194 Authorized general users set the update configuration by using the smart update utility, and authorized server/policy administrators set the update configuration by using the APC_Agent of the policy server.

195 Security Functional Requirements Mapping: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.2 Code Signing (V3_CodeSigning)

196 The following files are transmitted from the update server to V3.

– 'Hash list file' with the Hash value of the files to be transmitted.

– 'Engine/patch files' for the update

197 First of all, V3 receives the 'Hash list file' that has the Hash value of the files to be transmitted from the update server, and verifies authentication and integrity by using code signing (The authentication and integrity of the Hash list file must be verified ahead). V3 uses HAS-160, which is used when creating 'Hash list file', to verify the integrity of transmission from the update server.

198 Before uploading engine/patch files to the server, update files are created by using Microsoft code signing based on digital signature, and uploaded to the update server. The purpose of the code signing is to verify the authentication and integrity of the files while they are being operated on V3. The updates files with code signing on the update server are transmitted at a request of V3. The Hash list file with code signing is also uploaded to the update server.

199 Microsoft code signing verification functions are used to verify authentication and integrity of update files transmitted from the update server to V3. Consequently, the winstrust.dll file, which Internet Explorer includes, must be installed to verify Microsoft code signing.

200 Each file and signature from the update server includes the signing information by the certificate issued by certificate authority. V3 searches the structure of the reliable CA certificate at the certificate storage of Internet Explorer, and verifies it by checking the signing information of update files exists in the certificate, which will be conducted V3_SmartUpdate function.

201 After applying downloaded files from the update server, network drive shared folders or the policy server, V3 verifies if the files are created by AhnLab and the integrity of the files by code signing. If the signing verification fails, audit records are generated, the update stops, and engine/patch files are deleted, understanding e files are modified and masqueraded. The audit records are exempt from the verification target.

202 Security Functional Requirements Mapping: FPT_ITI.1, FPT_TST.1

6.1.3 V3 Configuration Management (V3_CM)

203 The authorized general user can manage all security functions (TSF) provided by V3 through the security management interface (described in each of the security function description in this 'TOE overview Summary'). The authorized server/policy administrator can set them in Policy Server to apply them to V3. However, when setting password for the security management interface provided by V3 in Policy Server, the authrized general user cannot recognize the password and as a result, cannot use the security management interface.

204 The authorized general user of V3 may set the password for his own configurations to prevent modification from other users. If the password set on the configurations, users may not modify them without knowing the password. The policy server controls the password set by the authorized general user, it means that the authorized server/policy administrator resets the password. Therefore, an authorized general user of V3 cannot modify the configurations of V3. Although an authorized user of V3 modifies the configuration, V3 keeps the configuration set from the policy server because the policy server transmits the configuration to V3 periodically.

205 The password is set by the cryptographic mechanism and meets SOF-medium.

- The password must be more than 6 and less than 40 characters with combination of alphabetic characters, one or more numbers and special characters.

- Authentication Delay Time: If the authentication failure count is more than 3, the TOE will reject the user's login for 10 seconds.
- The following characters are available: (Total: 94)
  - a - z (26)
  - A - Z (26)
  - 0 – 9 (10)
  - Special Symbol: ~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } : < > ? [ ] ; , . / " ' (32)

206 For the file protection by the password, the permutation mechanism is used. The security management function is not accessible for the authentication delay time.

Easy Configuration

207 V3 provides easy configuration to set the security level to High, Medium, Low, or Customized by using the configuration wizard. Easy configuration allows authorized general users to set virus scan/repair configuration with the quick and easy way by providing the following four security level.

- **Customized** – Blocks viruses based on customized scan/repair settings.
- **Low** – Minimal blocking of virus infections with only enabling real-time system monitoring. Recommended for system with a low risk of virus infection. This option makes V3 not to detect viruses in application level, but to detect and block viruses in the system level. This option has nothing to do with system performance.
- **Medium** – Blocks most virus infections with enabling all of real-time monitorings and sets auto-repair, and enables scan for all types of files including compressed files. It is recommended for general user to prevent the system from virus attacks, and the system performance may be affected.
- **High** – Blocks all viruses by enabling all of scan settings. It is recommended for system with a high risk of virus infection, and affected to the system performance.

208 The above settings are defined and classified into 3 settings (low, medium, and high) to help users easily configure settings. The authorized general users of V3 can configure all environment settings in the 'Customized' setting.

209 Security Functional Requirements Mapping: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.4 Scan/Repair (V3_Medic)

210 At a start-up of the operating system on the V3-installed system, V3 runs as a start-up program. At an initial start-up, V3 conducts real-time system scan and other real-time scan according to the configuration. V3 displays the status of itself

at the system tray icon, and a security warning report by the V3-Alert function after scan the vulnerabilities of the system by the V3-Report function.

211 Authorized/restricted general users (V3) or authorized server/policy administrators (APC) request scan/repair to the V3-installed system. Otherwise, authorized general users of V3 or authorized server/policy administrator of the policy server request scan/repair by setting security configurations such as scheduled scan and real-time scan (monitoring). Scan/repair is conducted by [Table 6-1] scan setting, and repair setting. The flow of scan/repair in general is as follow:

① Scan Request – Scan/repair for malicious codes are requested by the several methods (interfaces), and conducted according to the scan setting of authorized general users of V3 or authorized server/policy administrators. Scan setting will be described later.

② Advance Scan – Before starting all of scan except explorer scan and Outlook scan, the following scan will be conducted selectively. (Authorized general user's settings of V3 and authorized server/policy administrator's setting of the policy server): memory scan, self scan, boot sector scan, process scan, and startup program scan.

- Memory Scan: V3 provides scan/repair for memory-resident viruses that cannot be detected by the file-scan. The Memory Scan checks if processes are infected by scanning the reserved memory for processes: code area, stack area, and allocated memory. To repair the detected virus, V3 deletes or modifies it or forces a thread or a process where the virus lives to be terminated and deletes the virus.

- Self Scan: V3 scans its own processes before operating the scan/repair process. If the scan/repair process (file-binary) is infected, V3 repairs and restarts it.

- Boot Sector Scan: Scans the boot area of the operating system for viruses.

- Process Scan: Scans running processes on the V3 installed system.

- Startup Program Scan: Scans the start-up programs on the V3 installed system. V3 scans system files, main registry, and files registered on the start-up program folder.

③ Check Items Not to Scan – Before scanning, V3 exempts the Items Not to Scan set by authorized general users (V3) or server/policy administrators (APC) from the file scan list. The Items Not to Scan is set by folder, file, and extension. V3 does not scan items in the Items Not to Scan. The purpose of the Items Not to Scan is to avoid duplicating the scan area when other products by AhnLab, Inc. are installed on the same system.
Authorized general users (V3) or authorized server/policy administrators (APC) may delete items from the Items Not to Scan. V3 sets whether to scan the system restore folder by managing the Items Not to Scan. If the Items Not to Scan function is enabled, the system restore folder is included in the Items Not to Scan by default. If an authorized general user (V3) or authorized server/policy administrator (APC) deletes the system restore folder from the Items Not to

Scan, V3 scans/repairs the system restore folder at the next scan.

④ File Scan – Scans file types set by users in the scan setting ((All Files, or Execution Files, Script, Macro, Files set by an authorized general users (V3) or authorized server/policy administrators (APC)), Compressed File (Multi-Compressed files, Executable Compressed files, All types of Compressed Files, Compressed File Types set by authorized general users (V3) or authorized server/policy administrators (APC)), and harmful programs.

⑤ Repair Response – If a virus is detected in the previous step, V3 displays the name, time, and repair status (according to the repair setting) of the virus for authorized/restricted general users. The result of scan/repair keeps at the screen of the session to take actions. The repair response is conducted by the repair setting. The infected executable file is leaved as is according to the repair setting, or repaired by the method that an authorized/restricted general user chooses at the scan/repair result window. If the infected file is a system file, it is forced to stop, repair, or restart the system after repair according to the repair setting. If it is a repairable file, it may be repaired, left as is, or deleted. If it is unrepairable (a new virus), it may be left as is, or deleted.
If a file is infected by macro virus, users may response to it as the following settings:

- Repair Detected Macro Virus: V3 repairs the detected macro virus.
- Block the Use of Macro: V3 blocks the use of macro. Macro may not run on the processes or applications in the user system.

⑥ Terminate Scan – Generates audit records, and terminates scan. Authorized general users or restricted general users may terminate the scan at any time after the Scan Request (①).

212 Scan/repair on the V3 installed system are requested by the following interfaces, and run by the scan setting. The followings are interfaces of the Scan Request (①).

Quick Scan

213 V3 provides the Quick Scan command interface that users specify devices to scan and scan methods in a command to conduct the quick scan. This interface allows users to enter a command for conducting the quick scan as running a command in DOS environment.

Scan in the Main Window

214 System scan – system scan/repair in the main window provides an interface for authorized/restricted general users (V3) to request scan by the scan list, drivers or folders. V3 displays all drivers (including network drivers) in the system for users to select to scan. Users can select drivers/folders and request to scan them.

'Virus Scan' in the Windows Explorer

215 V3 is plugged in the windows explorer, and allows users to request the system scan by right-clicking on the windows explorer. This is the same as running the scan/repair function for a specific folder from the system scan menu of the main screen.

216 V3 is also installed on the Internet web browser as a plug-in which allows user to scan virus through the browser as through the Windows Explorer. The V3 plug-in interface of the web browser have the following functions:

- **Execute** – Displays the main screen of V3 which provides all interfaces of functions.
- **Configuration** – Provides an interface for configuring of V3. If the password is set by a server/policy administrator, the configuration is limited.
- **Smart Update** – Provides an interface for updating V3 by receiving the latest anti-virus engine (signatures).
- **Homepage** – Displays the AhnLab, Inc. Homepage.
- **Virus Scan** – Executes a virus scan/repair for selected drives, folders or files.

Scheduled Scan

217 V3 provides the auto-scan/repair function by scheduling the time. An authorized general user of V3 is allowed to scan the system automatically at scheduled times by adding/deleting/modifying scheduled scan rules. The following scheduled scan intervals are available: On every system start-up, daily, weekly, monthly, and once. V3 provides the scheduled scan wizard interface for authorized general users to conduct the effective scheduled scan.

218 The scheduled scan includes the Set Permission function which sets ID/password of authorized general users to taking approval of users from the operating system in case that the user of V3 is logged off at the scheduled scan time. V3 conducts the scheduled scan after taking user approval from the operating system by using ID/password. Because the scheduled scan is operated automatically, when scanning network drivers, users must set the ID/password of users to access network drivers.

Customized Scan

219 V3 provides an interface for authorized general users to customize a list to scan. Authorized general users of V3 can set multiple lists and add/delete folders and files in the V3-installed system. Authorized general users and restricted general users select the customized lists to perform the customized scan.

Policy Server Manual Scan

220 Authorized server/policy administrators of the policy server may transmit a manual scan command to the policy agent via policy center admin. V3 conducts the manual scan by receiving the command from the policy agent.

Screen Saver Scan

221 If the screen saver is enabled on the V3 installed system, V3 scans the scan list set by an authorized general user. If the scan list is not specified, V3 scans local hard drives automatically.

Outlook Scan

222 V3 scans MS Outlook's inbox (Outlook 2000 or higher). V3 is plugged in the Outlook, and authorized general users or restricted users may scan the inbox of the Outlook through the plug-in interface. Outlook scan provides the following plug-in interfaces for scan/repair.

- **V3 All Folders Scan** – Requests scan/repair all folders (including the personal folder) of Outlook.
- **V3 Selected Folders Scan** – Requests scan/repair selected folders in Outlook.
- **V3 Configuration** – Runs V3 configuration interface program.

Real Time Scan (Monitoring)

223 When an I/O event occurs on a file, V3 requests scan/repair, scanning (monitoring) the V3 installed system in real-time. V3 provides not only real-time system scan (monitoring) which provides real-time scan (monitoring) in the system level but also the following real-time scan (monitoring) interfaces by application: Internet, instant messenger, start-up program, Office, Outlook, and POP3:

- **System** - V3 scans/repairs all files and data accessing applications in the system in real-time, scanning (monitoring) its own system in real-time. V3 restarts the real-time system scan (monitoring) automatically, detecting the exceptional termination of real-time system scan (monitoring) by malfunction or reboot of the system. Authorized general users or authorized server/policy administrators (APC) are able to auto-restart interval by minutes. The default interval is 60 minutes.
- **Internet** – Requests scan/repair for files uploaded or downloaded via Internet Explorer.

- **Instant Messenger** – V3 supports the following instant messengers: MSN messenger v5.0 or higher, AOL messenger, Yahoo messenger, Daum messenger. V3 requests scan/repair for files transmitted by messengers above. V3 provides an configuration interface to recognize the messengers automatically by selecting them.
- **Start-up Program** – V3 scans (monitors) start-up program area: registry, start-up program folder, and system file in real-time, so when a key or file is stored in the start-up program area, it is scanned (monitored) in real-time. The default is 'Select All'.
- **Outlook** - V3 request scan/repair for attachment of email via Outlook.
- **POP3** - V3 requests scan/repair for attachment of email by intercepting all connections via POP3 from the mail program installed in the V3 installed system. The default POP3 protocol uses 110, and secures connection uses 995. V3 allows a configuration interface for authorized general users (V3) and authorized server/policy administrators (APC) to set POP3 protocol ports scanned (monitored) in real-time because in a special case, other port numbers may be used except 110 and 99. For provision against POP3 protocol timeout due to massive email during POP3 real-time scan (monitoring), V3 sends timeout prevention messages to POP3 clients and servers at the POP3 timeout set by an authorized administrator or authorized general user.
- **Office** - When MS office opens, downloaded, OLE (Object Linking & Embedding) files on the V3 installed system, V3 scan the files. V3 is plugged in the Office, and requests scan/repair when a file I/O event occurs on the Office program.

224 V3 provides the following interfaces to start/terminate scan:

- Starts/terminates screen saver scan.
- Starts/terminates Outlook scan.
- Shows/hides Windows Explorer scan.
- Starts/terminates real-time scan (monitoring): system, Internet, instant messenger, start-up program, Office, Outlook, and POP3.

225 With the configurations above, users may enable or disable real-time scan for file system or applications, and screen saver scan when the screen saver is on.

Scan Setting

226 The scan operation is conducted according to the following scan settings which are set by authorized general users of V3 or server/policy administrators of the policy server. The following settings are mapped to scan/repair functions mentioned above.

Scan Setting	Description	Interface
Close the Scan View window automatically if	Closes the Scan window automatically. If scanning is completed without detecting	System Scan Screen Saver Scan

viruses are not detected	any viruses, the Scan window will automatically close.	
Auto Repair	If a virus is detected, it is automatically repaired according to the repair configuration without alerting user.	System Scan Screen Saver Scan System Real Time Scan (Monitoring) Internet Real Time Scan (Monitoring) Instant Messenger Real Time Scan (Monitoring) Startup Program Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring) POP3 REAL TIME SCAN (MONITORING)
Scan Compressed File	Scans compressed files. It is set on the File Types to Scan under the Compressed File option.	System Scan Screen Saver Scan Instant Messenger Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring) POP3 REAL TIME SCAN (MONITORING)
File Types to Scan	V3 scans files according to file type: execution files, macros, script files, and customized files, or all files. The customized file type consists of multiple extensions divided by "/", and V3 scans the files with the extensions in the customized files. Select Execution files or All files as the file type to scan. Scan is conducted according to the setting, and All files is divided into as follows:	System Scan Screen Saver Scan System Real Time Scan (Monitoring) Internet Real Time Scan (Monitoring) Instant Messenger Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring) POP3 REAL TIME SCAN (MONITORING)
	File Types to Scan: V3 scans files according to file type: execution files, macros, script files, and customized files, or all files. The customized file type consists of multiple extensions divided by "/", and V3 scans the files with the extensions in the customized files.	System Scan Screen Saver Scan System Real Time Scan (Monitoring) Internet Real Time Scan (Monitoring) Instant Messenger Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring) POP3 REAL TIME SCAN (MONITORING)

	Compressed File Types: V3 supports 10 times of decompression for multi-compressed files to scan. V3 also supports scanning executable compressed files created by such programs as PKLITE, LZEXE, and DIET. V3 does not scan previously scanned compressed files for multi-compressed file to provide efficient performance. V3 supports the following compressed file types: Ace, Bhx, Hqx, Pak, Zip, Alz, Bz2, Ice, Rar, Zoo, Arc, Cab, Jar, Tar, SFX, Arj, Enc, Lha, Uue, B64, Gz, Lzh, Xxe, Bh, Ha, Mime, and Z. An authorized general user is allowed to scan all types or selected types. By default, Ace, Zip, Rar, Arj, and Lzh types are selected.	System Scan Screen Saver Scan Instant Messenger Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring)
	Scan Method: Select a method from the followings: • Scan after disabling shared files/folders: Disables all shared folders of the system and starts scanning for viruses. The disabled shard folders will not be recovered after scanning. • Scan after closing shells: Closes the shell program (Windows Explorer), and starts scan.	System Scan

	Scan Method: V3 provides the following scan methods: Scan Floppy Disc, Scan Range to specify the range for the real-time system scan (Monitoring), and Warning Message. • Scan Floppy Disc – If a floppy disk is detected on the system, V3 scans (monitors) the boot sector of the floppy disk in real-time. When closing the Windows, V3 scans the whole floppy disk. • Scan Range – An authorized general user or authorized server/policy administrator select the scan range. Scan local drive reading, Scan local drive writing, Scan network drive reading, and Scan network drive writing are set by default. • Warning Message: Displays a warning message when a virus is detected.	System Real Time Scan (Monitoring)
	Harmful Programs: V3 blocks harmful program such as key logger, ad ware, and joke. The scanned harmful programs can be added/deleted to the ignore list.	System Scan
infector detection	V3 displays the name of virus, owner, accessor, and infector (IP address or NetBIOS name) to trace the infector of the detected virus during real-time scan (monitoring). Especially, it displays the infection route of the virus spreading through network shared folders. If real-time system scan (monitoring) detects malicious codes, V3 gets the information of the sessions which are currently accessing shared folders, and compares the information of the folder where malicious codes are detected and the whole shared folders information in the system. V3 decides infector's folders from the result of comparison and gets the IP address or the computer name of the session. System real-time scan (monitoring) with auto repair generates audit records, and real-time system	System Real Time Scan (Monitoring)

	scan (monitoring) with manual repair generates audit records and display the information of the infector in the scan/repair window.	
Incremental Scan	V3 does not scan previously scanned Outlook file. Modified or newly created Outlook files are scanned only once	Outlook Scan

Repair Setting

227 After scanning according to the scan setting above, system san is terminated if no virus is detected. If a virus is detected, V3 responses it according to the repair setting by authorized general users of V3 or server/policy administrators of the policy server. The following table shows the system repair setting.

repair setting	Description	Interface
Backup files before repairing or deleting	In repairing an infected file, V3 backs the file up before repairing or deleted the infected file according to the setting. The backup file moves to the quarantine station, can be deleted by users.	System Scan Screen Saver Scan System Real Time Scan (Monitoring) Internet Real Time Scan (Monitoring) Instant Messenger Real Time Scan (Monitoring) Startup Program Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring) POP3 Real Time Scan (Monitoring)
Repairable Files	In repairing an infected file, V3 leaves as is, repairs or deletes the file.	System Scan Screen Saver Scan System Real Time Scan (Monitoring) Internet Real Time Scan (Monitoring) Instant Messenger Real Time Scan (Monitoring) Startup Program Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring) POP3 Real Time Scan (Monitoring)
Unrepairable Files	In repairing an infected file, if the file is unrepairable, V3 leaves as is or deletes the file.	System Scan Screen Saver Scan System Real Time Scan (Monitoring) Internet Real Time Scan (Monitoring) Instant Messenger Real Time Scan (Monitoring) Startup Program Real Time Scan (Monitoring)

		Outlook Scan Outlook Real Time Scan (Monitoring) POP3 Real Time Scan (Monitoring)
Compressed File	In repairing an infected file, if the file is compressed, and system scan setting includes compressed file scan, V3 leaves as it or deletes the file. In scanning a compressed file, V3 decompresses it, scans/repairs the virus, and recompresses the file. Only ZIP files are applied to this.	System Scan Screen Saver Scan Instant Messenger Real Time Scan (Monitoring) Outlook Scan Outlook Real Time Scan (Monitoring) POP3 REAL TIME SCAN (Monitoring)
Executing Files	In repairing an infected file which is currently running on the system, V3 scans it after user verification (Except System Real Time Scan (Monitoring), Instant Messenger Real Time Scan (Monitoring), and Startup Program Real Time Scan (Monitoring)), repairs after forced termination, or restarts the system after the repair. In case of user verification, users may leave as is, repair after forced termination, or restart the system after the repair the file. When repairing after forced termination for running viruses, if they are system processes, V3 restarts the system after the repair them. In case of restart the system after the repair, V3 copies the original files of the running malicious codes to temporary files, repairs them, and changes the original files to the repaired files. This is the case for the running processes which should not be terminated. Repairing executing files runs according to the repair setting for reparable files or unrepairable files.	System Scan Screen Saver Scan System Real Time Scan (Monitoring) Instant Messenger Real Time Scan (Monitoring) Startup Program Real Time Scan (Monitoring)
Block Files	If files whose extensions are set by user's scan setting are detected during System Real Time Scan (Monitoring), V3 changes the extensions of files by the repair setting, deletes the files, or prevents the files from occurring I/O (Except Outlook Real Time (Monitoring), POP3 Real Time Scan (Monitoring)).	System Real Time Scan (Monitoring) Outlook Real Time Scan (Monitoring) POP3 Real Time Scan (Monitoring)

228 V3 displays configuration, and scan history of scanning and repairing for authorized general users. Authorized general users may see the following information:

- **Engine Update** – The date of the engine applied to the current V3

- **Real Time Monitoring Status** – Displays the status (on/off) of System Real Time Scan (Monitoring), Internet Real Time Scan (Monitoring), Instant Messenger Real Time Scan (Monitoring), Start-up Program Real Time Scan (Monitoring), POP3 Real Time Scan (Monitoring), Outlook Real Time Scan (Monitoring), and Office Real Time Scan (Monitoring).
- **Schedule Setting** - Scheduled scan interval Information
- **Last Scan Activities** – Displays the latest scan activity information including the simple result of scan (number of scanned, infected, and repaired).

229 Security Functional Requirements Mapping: FAV_ACT.1, FAV_ALR.1, FAV_SCN.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FPT_TST.1

6.1.5 Self Protection (V3_SelfProtect)

230 V3 scans its processes (executable files) using the real-time scan (monitoring) of V3_Medic, and the self scan function. If viruses are detected on the executing processes of V3, V3 scans/repairs them according to the settings by authorized general users (V3) or authorized server/policy administrators (APC). After that, V3 displays an alert message for virus detection by using V3_Alert. V3 also scans/repairs its processes before startup. V3 provides the setting interface that can enable or disable the virus scan function of the self program file by the authorized general user and authorized server/policy administrator.

231 V3 provides an interface for authorized/restricted general users to perform integrity scan. TSF execution codes, update files whish are V3 engine/patch files (TSF execution codes and data files), from the update server, and TSF data files such as configuration files of V3 are integrity scan targets.

232 V3 configuration files are verified by comparing their Hash values that were created by the HAS-160 algorithm and attached to the files when they were modified the current Hash values because V3 configuration files keep being modified from authorized security management.

233 Code Signing is attached to TSF execution codes, ASCII files. At the integrity verification, Code Signing verification is carried out as the same way of V3_CodeSigning. Alerted integrity is detected by creating Hash of the current TSF execution codes and data types and comparing the Hash and integrity value of the CodeSigining, which are carried out at a start-up of V3, and a request of authorized general users via security management interface.

234 V3 provides the self protection function that prevents other processes from accessing its own installation directory. This function prevents other processes except the secure processes defined by V3 from accessing the V3 installation directory, and displays an alert message to authorized/restricted general users

according to the configuration, which means that the self protection function prevents malicious codes from accessing V3 execution files. Displaying alert messages is carried out by the V3_Alert function.

235 Security Functional Requirements Mapping: FMT_MOF.1, FMT_SMF.1, FPT_TST.1

6.1.6 Warning Mail (V3_WarnMail)

236 V3 sends email to the sender of the email. If an email messages is infected by a virus detected by Outlook real-time scan (monitoring) and POP3 real-time scan (monitoring) of scan/repair (V3_Medic).

237 V3 sets the IP address and port of the SMTP server, email address for this function. This function is disabled by default, and works with the settings by authorized general users (V3) or authorized server/policy administrators (APC).

238 The authorized general user (V3) or server/policy administrator specifis the SMTP server IP address, mail address, mail server port for this.

239 Security Functional Requirements Mapping: FAV_ALR.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.7 Spam Mail Filtering (V3_SpamFilter)

240 V3 scans email virus through Outlook real-time scan (monitoring), POP3 real-time scan (monitoring) of the V3_Medic function, and conducts spam mail filtering. Authorized general users of V3 defines spam mail filtering rules, V3 filters spam mails with the rules. If a spam is detected by the rules, the '[SPAM]' phrase is added to the subject of the email, the email is moved to the Deleted items folder.

241 V3 provides a spam mail filtering configuration interface for authorized general users (V3). The default rule of spam mail filtering is to block email including 'Advertisement' or 'Adult Advertisement' on the subject of the email. The default spam mail filtering rule can not be deleted or modified but disabled.

242 If authorized general users-specified words conform to the subject of email, body of the text, recipients, or senders, the email is filtered by the spam mail filtering function.

1) Include any or
2) Include all or
3) Not include any or

4) Not include all

243 Each spam filtering rule is applied by priority, and , authorized general users are allowed to modify its priority.

244 Authorized general users are able to set rules to allow or deny by email accounts. Email messages from the allowed email account will be passed, and email messages from the denied email account will be classified as spam mail.

245 Security Functional Requirements Mapping: FAV_SPM.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.8 Quarantine Backup (V3_FileBackup)

246 When viruses are detected, V3 quarantines them in 'Quarantine' to stop them from spreading. Quarantine backs up the infected files to a specific location to prevent spread/inflow of the virus files and restore the original files before repairing/deleting them. If V3 damages the original files during repair, authorized general users can restore the original infected files from Quarantine. That is, Quarantine Backup is to store the infected files to a specific location to restore the infected files themselves. V3 provides the following functions that can be run by the authorized general user for the files to be stored in quarantine.

- **Restore** – Repairing (Delete the infected file or delete the virus from the infected file - repair) and restoring the backup files, return the files to the location where they are infected. However, if you perform system scan (V3_SystemScan), the viruses are detected again because the viruses were also restored.
- **To Temporary Folder** – Moves the files to the folder you specified.
- **Submit to AhnLab Security E-Response (ASEC)** – V3 provides an interface to submit failed-to-repair files to ASEC.
- **Delete** – Deletes the infected files backed up in Quarantine.
- **Backup Properties** – Displays the detailed information about the infected file including the name, location, size, backup date, created date of the infected file, as well as the name and the status of the virus, file properties (read only, hidden, archive, and system)

247 Security Functional Requirements Mapping: FAV_ACT.1, FMT_MTD.1, FMT_SMF.1

6.1.9 Alarm Management (V3_Alert)

248 According to the settings by authorized general users (V3) or authorized server/policy administrators (APC), V3 displays an alert message for authorized general users in the following cases:

- When update error or a virus is detected on V3
- When smart update completion event is generated
- When a security warning report message is generated
  (When one or more items whose security vulnerability level is danger, and priority is medium or higher exist)
- Displaying access prevention alert message by the self projection function

249 At start-up, V3 displays messages of security warning report in the task bar as an alert icon, and displays the result of vulnerability analysis by authorized general users or restricted general users. V3 displays an alert message to inform users the events such as update error, virus detection, smart update, and accessing the V3 installed directory by other processes except the V3 process by the self protection function. V3 is able to make an alarm with a sound file at virus detection, which authorized server/policy administrators of APC and authorized general users of V3 are able to enable/disable.

250 Security Functional Requirements Mapping: FMT_MOF.1, FMT_SMF.1, FAU_ARP.1, FAU_SAA.1, FAV_ALR.1

6.1.10 V3 Disk Cleanup (V3_Disk)

251 V3 provides an interface to specify the space for the following backup files and audit data in Quarantine for the authorized general users of V3.

- Whether to save the scan logs
- Space to save the scan logs
- Space to save the event logs
- Space to save the backup folders

252 This function can be on/off to use the space for audit data and backup files. To set the space for audit data, the function shall be enabled.

253 User specifies the location and size of the space for scan log and event log by the V3_Log function, and backup files by V3_FileBackup. If audit data exceeds the specified space, V3 overwrites the oldest audit records for the prevention of audit data loss. In the same way as audit data, V3 overwrites the oldest backup files for

the prevention of backup file loss if backup files created by V3_FileBAckup exceed the specified space.

254 If the use of each space is disabled, V3 stores audit data or backup files until the physical space is full.

255 Security Functional Requirements Mapping: FAU_STG.4, FMT_MOF.1, FMT_MTD.2, FMT_SMF.1

6.1.11 Security Warning Report (V3_Report)

256 V3 scans the system status of the authorized/restricted general user (V3) and informs the user through the security warning report if the defined vulnerabilities are detected. The security warning report runs on the authorized/restricted general user (V3)'s request and the start-up. It is displayed in the security management screen on the authorized/restricted general user (V3)'s reauest and in the tray alarm on the start-up. The display in the serurity management screen or in the tray alarm is performed in the V3_Alert function.

257 The security warning report consists of items that are defined based on the virus analysis by V3. V3 scans the following vulnerabilities:

- Checking for shared folders
- Checking the security level of Macro Virus in MS Word 2000
- Checking the security level of Macro Virus in MS Excel 2000
- Checking the security level of Macro Virus in MS PowerPoint 2000
- Checking the security level of Macro Virus in MS Word XP
- Checking the security level of Macro Virus in MS Excel XP
- Checking the security level of Macro Virus in MS PowerPoint XP
- The .ida vulnerability of MS Index Server
- Unicode web server folder traversal for IIS server
- The IIS server used spread viruses
- Infection by reading infected email (IIS 5.0)
- Running attachment by IE due to incorrect MIME header (IE 5.01)
- Running attachment by IE due to incorrect MIME header (IE 5.5)
- The transformed UPnP request (Win XP)
- MS Word field code

- The external update of MS Excel
- The Help of MS Windows XP
- Outlook Express S/MIME parsing
- Buffer overrun of Windows Help
- Authority control of Network Connection Manager(NCM)
- DoS attack using buffer overrun of SMB
- Buffer Overrun vulnerability due to Htr chunk encoding process error
- Windows Shell Buffer Overflow
- Windows SMTP vulnerability
- Outlook View Control vulnerability
- Buffer overflow of Index Server Search function
- Running codes by buffer overrun in the MS SQL Server 2000 confirmation server
- Microsoft Visual Basic for Applications code execution
- RPCSS service code execution vulnerability
- Checking the accumulated patches of Microsoft Internet Explorer
- Checking Windows Authenticode vulnerability
- Windows Troubleshooter ActiveX Control code execution vulnerability
- Windows Messenger Service remote code execution vulnerability
- Checking buffer overflow of Windows Help and Support
- Checking Exchange Server 5.5 cross site script vulnerability
- Checking cumulative security update patches of Internet Explorer (832894)
- Checking code execution due to ASN .1 vulnerability (828028)
- Checking code execution due to Microsoft Outlook vulnerability (828040)
- Checking security updates of Microsoft Windows (835732)
- Checking cumulative security updates of Microsoft RPC/DCOM (828741)
- Checking cumulative security updates of Outlook Express (837009)
- Checking executing codes due to Microsoft Jet database engine (837001)
- Checking executing remote codes due to vulnerability of Help and Support Center (840374)

258 The security warning report includes result, priority (high, medium, and low), vulnerability, and solution, and can be saved as a file and display properties by record for each report.

259 If one or more items whose level of security vulnerability is ‘critical’ and the priority that is higher than ‘medium’ exists, an alarm message is displayed on the tray of the authorized/restricted general user by V3_Alert.

260 Security Functional Requirements Mapping: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FPT_AMT.1

6.1.12 Audit Record (V3_Log)

261 Including the logs on start/termination of the audit record, V3 generates audit records of start/termination for ‘scan/repair (V3_Medic)’: the real-time system scan (monitoring), real-time Internet scan (monitoring), real-time startup program scan (monitoring), system scan, screen saver scan and V3_SelfProtect: On/Off (enable/disable) of the self protection, the result of integrity scan, and self testing. Even if the configuration is set by the authorized server/policy administrators of the policy server, and applied to V3, the audit records of start/termination for the functions mentioned above are generated and stored. V3 also generates audit records for operations (the update operation, and integrity error) of V3_SmartUpdate, and apply of the configurations set by general users (V3) or authorized server/policy administrators (APC). V3 defines this type of audit record as event log that includes date, type (normal, warning, and error), scan method (interface) name (function name), and message. These fields can be sorted, deleted, and all event logs displayed for authorized/restricted general users (V3) can be stored in the local file system as a text file. The fields in the event log are as follows:

- Event Log Type – Normal, Warning, Error
- Date
- Function Name which generates event log
- Message

262 Also, V3 generates audit records of detection and repair of viruses on the authorized/restricted general user’s system (V3), which is scan log. The scan log includes the following fields: date, infected file name, virus name, status, and scan method (interface of the scan/repair (V3_Medic) function), owner of the infected file, and accessor, and infector). The owner is a user ID who has authority of the file, and the acceessor is the name of the computer which access the file, and the infector is the name of network path/shared name in case of accessing the file via network. The infector detection function creates the information about owner, accessor, and infector, which are sorted, deleted, and saved as file. An interface to display the detailed properties of the fields by record is provided. The fields in the scan log are as follows:

- Date
- Infected File Name
- Virus Name
- Virus Repair Status
- Scan Method
- Owner
- Access
- infector

263 Authorized/restricted general users are allowed to search audit records generated and stored by V3. V3 provides separated search interfaces for event log and scan, which can be searched by date. The event log can be search with the following conditions: period, type: normal, error, warning. The scan log can searched by the following conditions for authorized/restricted general users

- Period
- Status – Repairable, Scheduled to Repair (Unrepairable), New Virus, Compressed File (Before Repair), Repair Completed, Deleted, Failed to Repair, Change Name (After Repair)

264 Security Functional Requirements Mapping: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1(1), FAU_SAR.2, FAU_SAR.3, FMT_MTD.1, FMT_SMF.1

6.1.13 Identification and Authentication for Authorized Administrator (APC_INA)

265 APC for V3 consists of policy server, policy center admin, and policy agent. When accessing to the policy server through policy center admin, the administrator is identified and authenticated. Authentication uses permutation mechanism by password. Authorized administrators login to the policy server through policy center admin by their own authorities (server administrator, policy administrator, and monitor center). If idle time keeps up for a specific time, the session of the authorized administrator is closed, and the administrator is forced to be re-identified and re-authenticated through policy center admin to re-connect to the policy server.

266 If the authentication failure count of the administrator exceeds 3, the authorized server administrator will be rejected for authentication for the specific delay time.

Administrator Account Management

267 The authorized administrators of APC are divided into the following roles: server administrator, policy administrator, and monitor center. The server administrator of the policy server is allowed to add/modify/delete administrator's account mention above through the policy center admin.

268 The password of the authorized administrator created by the following combination. If the password which an authorized server administrator adds or modifies does not conform to the following rules, the request of the server administrator is denied, and an alert window will be displayed. Each authorized administrator shall modify his own password conforming to the following rules as well. With the following password rule, the Security Target meets SOF-medium. The password rule of the policy server is as follows:

- The password must be more than 6 and less than 40 characters with combination of alphabetic characters, one or more numbers and special characters.
- Authentication Delay Time: If the authentication failure count is more than 3, the TOE will reject the user's login for at least one minute or at most 60 minutes10 seconds. (The default is one minute.)
- The following characters are available: (Total: 94)
  - a - z (26)
  - A - Z (26)
  - 0 – 9 (10)
  - Special Symbol: ~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } : " < > ? [ ] ; ' , . / (32)

269 If an administrator tries to login through the policy center admin, APC identifies and authenticates the administrator by checking ID, password, available login time, available login IP address range. If all conditions are satisfied, the security management screen will be displayed.

270 If an authorized server administrator in the security management remains idle for the specified time, the policy server terminates the session with the policy center admin. After that if the authorized administrator requests security management action via the policy center admin, the policy server will request re-authentication. Then, the authorized administrator shall login by entering his own id/password via the policy center admin for identification and authentication. The authorized administrator is able to logout from the security management screen. If authorized administrator request to logout from the security management, the policy server makes the administrator logout, and if the audit record window is opened, closes it asking whether you want to close the window or not. After logout, the session is terminated. If an administrator request security management via the policy center admin, the policy server will request re-authentication.

271 An authorized administrator provides the following security management functions by authority ((server administrator, policy administrator, monitor center):

Function \ Authorized Role	Authorized Server Administrator	Authorized Policy Manager	Authorized Monitor Staff
Virus Scan/Repair	*stop, start, determine the behavior*	*stop, start, determine the behavior*	–
Advance Scan	*stop, start*	*stop, start*	–
Spam Mail Filtering	–	–	–
Alert Mail	*stop, start*	*stop, start*	–
Alert Icon Indication	*stop, start*	*stop, start*	–
Self Scan	*stop, start, determine the behavior*	*stop, start, determine the behavior*	–
V3 Engine/Patch File Update	*stop, start, determine the behavior*	*stop, start, determine the behavior*	–
Update Integrity Scan	*stop, start*	*stop, start*	–
Viewing Update Information	*stop, start*	*stop, start*	–
V3 Configuration Security (Setting Password)	*stop, start*	*stop, start*	–
Use Items Not to Scan	*stop, start*	*stop, start*	–
Check System Restore Folder	*stop, start*	*stop, start*	–
Self-Protection	*stop, start*	*stop, start*	
APC Log Forwarding Policy Configuration	*determine the behavior*	–	–
APC Timestamp Server Configuration	*stop, start, determine the behavior*	–	–
APC Notification	*determine the behavior*	–	–
APC Integrity Scan	*determine the behavior*	*determine the behavior*	*determine the behavior*
Restart Policy Agent Policy Agent Mode Check Policy Agent Status Delete Policy Agent Check and Request Policy Agent Update Version	*determine the behavior*	*determine the behavior*	–
Policy Agent Configuration	*determine the behavior*	*determine the behavior*	–
Stop Policy Server Service Start Policy Server Service Restart Policy Server Service	*determine the behavior*	–	–
APC Update	*determine the behavior*		

272 An authorized administrator provides the following TSF data management functions for by authority ((server administrator, policy administrator, monitor center):

Authorized Role / TSF Data	Authorized Server Administrator	Authorized Policy Manager	Authorized Monitor Staff
Home Information Data – Engine Update Date – Real Time Monitoring Status – Schedule Setting – Last Scan Activities	*[view]*	*[view]*	*[view]*
V3 Virus scheduled scan – Schedule List Data (Schedule interval, scan list)	*modify, delete, [view, add]*	*modify, delete, [view, add]*	*[view]*
V3 Configuration Security Functional Data (Configuration Password)	*modify*	*modify*	–
Warning Mail	*modify, [view]*	*modify, [view]*	–
V3 Update Configuration Data	*modify, delete, [view, add]*	*modify, delete, [view, add]*	*[view]*
Administrator Account Information	*modify, delete, [view, add]*	–	–
APC Update Configuration Data	*modify, [view]*	–	–
Authorized Administrator's Password	*modify*	*modify*	*modify*
Policy Agent Management Key Data	*modify*	–	–
Notification Configuration Data Notification Configuration	*delete, [view, add]*	–	–
Policy Agent Management Information	*[view, Save as File]*	*[view, Save as File]*	*[view]*
Hardware/Software Information	*[view]*	*[view]*	*[view]*
APC Status Summary Information	*[view]*	–	–
Backup Configuration History	*modify, delete, [view, add]*	–	–
Audit Record Stored in the Policy Server	*delete, [view, Save]*	*delete, [view, Save]*	*[view]*
Policy Server Service Status Policy Agent Policy Status	*[view]*	–	–
Policy Server Service Setting	*modify, [view]*	–	–
Policy Agent configuration policy file	*delete*	*delete*	–
Policy Agent installation program	create and delete	create and delete	–
Policy Agent patch program	register and delete	register and delete	–
CPU/Memory/Hard Disk Threshold of Notification Status Settings	*modify, [view]*	–	–

273 Security Functional Requirements Mapping: FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.6, FIA_UID.2, FMT_MTD.1, FMT_SMR.1, FMT_SMF.1, FTA_SSL.3, FTA_SSL.4

6.1.14 APC Secure Communication (APC_SecureComm)

274 V3 encrypts and attaches Hash values to protect authentication and identification data or the message for the security management, which is transmitted between Policy Server and Policy Center Admin or Policy Server and Policy Agent from unauthrized modification and exposure. Therefore, data transmitted among APC components cannot be viewed or modified. Audit data, yet, is not encrypted or Hash values are not attached. The encryption algorithm is SEED with 128bit key length, and the operation mode is the CBC operation mode. The Hash algorithm for verifying the integrity of transmitted data among the policy center admin and the policy server and the policy agent is HAS 160.

275 Security Functional Requirements Mapping: FPT_ITT.1(1), FPT_ITT.1(2)

6.1.15 APC Update (APC_Update)

276 APC stored engine/patch files of V3 received from the update server. APC carries out auto-update periodically by configuring update interval in an hour and retry count at failure. APC also sets the restrict update time to limit update during the update time considering intensive network traffic.

277 As the V3 smart update, V3 requires the license authentication of the client (APC server) before transmitting update engine/patch files from the update server. APC requests authentication by sending information such as its own product number to the update server, the update server sends back the result of the authentication to APC. After successful authentication, APC downloads engine/patch files from the update server.

278 APC uses APC_CodeSigning to verify the integrity of the update files in the same way of comparing the downloaded Hash list and Hash of the transmitted files which are codesigned. If the integrity verification succeeds, APC stored the downloaded files.

279 APC provides the update configuration interface for authorized server administrators: IP address of the update server, and update operation setting, and the urgent update function which carries out the update at the authorized server administrator's request.

280 Security Functional Requirements Mapping: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.16 APC Code Signing (APC_CodeSigning)

281 TOE is separated into V3 and APC and APC is separated into policy server, policy agent, and policy center admin. Like this, each security functions are implemented on each TOE components. The APC code signing security function is implemented as the same way of V3_CodeSigning, which means that the implementation of APC_CodeSigning is same as V3_CodeSigning but it is applied to APC. Consequently, APC_Update and APC_Integirty both use APC_CodeSigning. Because the implementation of V3_CodeSigning, authentication and integrity verification of engine/patch files from the update server are performed. The certificate and key for RSA digital signature are issued by VeriSign.

282 When creating Hash list file of engine/patch files, the HAS-160 algorithm is used to verify the integrity of transmitted data from the update server

283 Security Functional Requirements Mapping: FPT_ITI.1, FPT_TST.1

6.1.17 Time Configuration (APC_Time)

284 The policy server synchronizes the time with the NTP (Network Time Protocol) server specified by the authorized server administrator. Unless the NTP server is not in use, the policy server uses the system time where the policy server is installed. The policy agent synchronizes the time with the policy server.

285 Security Functional Requirements Mapping: FMT_MOF.1, FMT_SMF.1

6.1.18 APC Integrity Check (APC_Integrity)

286 APC performs authentication and integrity scan for the APC executable code files and data type files, TSF data file (except audit data files), by using APC_CodeSigning

287 Especially, a data type file consists of TSF data file (data type) and Hash of the original file by HAS 160 because data type files (except ASCII, and audit data files) can not be codesigned. Because an APC execution file is codesigned in the CAB file type, APC verifies the codesign.

288 In the beginning of the integrity verification, APC verifies the codesign of the file with the Hash. After that APC decompresses the cab file, and verifies it by comparing the Hash of the cab file, and original TSF data file (data type).

289 The Codesign is attached to the TSF execution code, and the codsigning verification is performed as the same way of APC_CodSigning at the integrity verification: creating the Hash of the current TSF execution code, and comparing it with the integrity of the codesign to check the integrity masquerade.

290 In addition, when modification takes places, the Hash of the configuration files are re-created and stored in the extra Hash table because the configuration files of APC, which are not downloaded from the update server, are modified in setting configuration. Therefore, APC performs integrity scan by creating the Hash of the current configuration file and comparing it with the Hash table at a integrity scan request of the authorized server/policy administrator.

291 These integrity scans for the policy server and policy center admin are requested by authorized administrators (server, policy, and monitor staff) using a menu of the policy center admin. Authorized administrators (server, policy, and monitor staff) are allowed to search audit records for the result of the integrity scan of the policy server and the policy agent. If the integrity of the configuration files are altered, authorized administrators (server, policy, and monitor staff) are able to re-create Hash of them. However, for the TSF execution codes, the deliver off-line patch shall be carried out because APC can not re-create the codesigning. In creating the Hash file, HAS-160 is used as a Hash algorithm.

292 The integrity scan of the policy agent is carried out by authorized general users or restricted general users through a menu of the policy agent. A restricted general user, however, can not use the re-create Hash function for the integrity.

293 After patching the policy agent, the integrity scan is carried out as the same way of APC because patch files of the policy agent include the codesign,

294 Security Functional Requirements Mapping: FMT_MOF.1, FMT_SMF.1, FPT_TST.1

6.1.19 Policy Agent Management Key Setting (APC_AgentKey)

295 The policy server provides the policy agent management key setting for the server administrators to prevent authorized general users from terminating, deleting, and stopping the policy agent (Restricted general users of V3 can not terminate, delete, and stop not only V3 but also the policy agent.). Because the policy agent is used for the policy server to set the configurations of V3, the policy agent prevents authorized users from terminating, deleting, and stopping the policy agent. The management key is set by the password mechanism which satisfies SOF-medium, the SOF of the Security Target..

- The password must be more than 6 and less than 40 characters with combination of alphabetic characters, one or more numbers and special characters.
- Authentication Delay Time: If the authentication failure count is more than 3, the TOE will reject the user's login for one minute.
- The following characters are available: (Total: 90)
  - a - z (26)

- ○ A - Z (26)
- ○ 0 – 9 (10)
- ○ Special Symbol: ~ ! @ # % ^ & * ( ) _ + | ` - = \ { } : < > ? [ ] ; , . / (28)

296 In protecting files by the key, the permutation mechanism is used. During the authentication delay time, termination, deletion, and stop can be done.

297 Security Functional Requirements Mapping: FMT_MTD.1, FMT_SMF.1

6.1.20 Server Task Control (APC_Service)

298 Security functions of the policy server run as service, which are started, stopped, and restarted by server administrators of the policy server. The status of each service can be queried through the policy center admin, and the service can be started, stopped, and restarted according to the status. The following describes the services of the policy server security functions:

- Policy Service: Stores the configurations of the policy server and V3in the LDAP.
- Policy Agent Service: Responses the request of the policy agent.
- Log Service: Stores logs of V3 from the policy agent in the audit data storage.
- Policy Agent Scheduler: Transmits the request of authorized server/policy administrators to the policy agent.

299 Besides, the authorized server administrators are allowed to query and set the server name of each service, server IP address, services port, time out, and whether to create file log.

300 Security Functional Requirements Mapping: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.21 Backup Configuration (APC_BackupConfig)

301 The policy server stores logs from the policy agents in the SQL database, and configurations of the policy agent and V3 in the LDAP directory. The policy server provides the backup function for the information bout DBMS and LDAP on a regular basis, and deletes unnecessary tables for DBMS. The authorized server administrators set when to back up the data by setting the scheduled interval for backup of DBMS and LDAP, and when to delete unnecessary tables from the policy server database by setting the database cleanup. At the scheduled interval, the policy server backs up DBMS and LDAP and generates the audit record of the backup. The authorized server administrators are able to add/modify/delete the scheduled interval for the backup.

302 Security Functional Requirements Mapping: FMT_MTD.1, FMT_SMF.1

6.1.22 Notification Configuration (APC_Notice)

303 Server administrators of the policy server set the notification configuration by selecting mail or notice notification through each policy center admin (all of them may be selected). Then, notification will be transmitted to the recipients designated by the administrators through email and notice at an engine update, a service failure of the policy server, or a threshold of CPU/Memory/Hard disk, or a virus infection.

304 If the notification is email, the IP address of the SMTP server, sender's email address, recipients' email addresses, and the IP address of the recipients shall be set to send notification. For the last step, the server administrator sets the virus alert settings to alert the administrator when infected with virus, and minutes and cases to notify when more than a specified times (cases) virus infection has occurred during a specified time period (minutes).

305 Security Functional Requirements Mapping: FAU_APR.1, FAU_SAA.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_SMF.1

6.1.23 APC Status Summary (APC_Summary)

306 The policy server displays the current domain information of the policy server, domain configurations (name, parent server, and child server), service status (database service, LDAP service, policy agent service, policy center admin, policy agent, task scheduler service, policy service, the running status of the log manager, virus infection information, the latest update, and the latest backup information), and the summary of the policy agent registered in the policy server through the policy center admin to the server administrators. The summary information on the policy center admin is refreshed by 5 minutes.

307 Security Functional Requirements Mapping: FMT_MTD.1, FMT_SMF.1

6.1.24 Policy Agent Management (APC_Agent)

Policy Agent Installation/Patch Program Management

308 Authorized server/policy administrators are allowed to create/delete installation programs of the policy agent. The policy agent installation program is installed in the administrator's computer, and transmits security commands and configurations

from the server to the user system as a communication medium between the policy server and V3. The authorized server administrators are able to search the name of the registered policy agent installation program, the created time, and installation program description, and execution options and communication environment at a detailed request. It also can delete unused policy agent.

309 The authorized server/policy administrators are able to register patch programs of the policy agent. They are registered with a release of new patch programs by AhnLab, Inc. The policy agent updates by using the patch program registered in the policy server according to the policy agent patch interval.

Policy Agent Management

310 The policy agent management are able to display general settings, transmit the restart command, change the operating mode, display the operating status, and delete the policy agent from the managed system.

311 The authorized administrator (including monitor center) of the policy server searches the following information of the policy agent installed computer.

- Policy Agent Information – agent ID, computer name, IP address, OS type, login user, Windows group name, policy server group
- Last login user Information – user name, department, phone number, e-mail, employee-id
- Setup Program: Displays version, agent operating mode, last log in, last task, smart update version, V3 version in the policy agent installed computer, engine version/date, engine update time, real-time monitoring status, last scan time, license number, user name, organization name
- Shared Folder Information
- Hardware/Software Information of the system where the Policy Agent is installed.

312 The policy agent runs on the following modes, which are modified by the authorized server/policy administrator.

- **Passive Mode (AGENT_PASSIVE)** – When the agent program is first installed, the computer only transmits the General Information of the agent and stays in standby mode. In passive mode, the agent computer operates only when requested by the server and does not perform the scheduled tasks specified in General Agent Settings and Product Update Settings of the agent policy.
- **Active Mode (AGENT_ACTIVE)** – The agent uploads information to the policy server according to the configuration, and downloads commands and configurations from the policy server.

313 The passive mode prevents too many agent computers from accessing the server simultaneously, causing the network and server load to surge. Unless the

server/policy administrator sends the command to perform a manual scan, a manual update or software distribution. Therefore, in order to perform security-related tasks, such a virus scan an engine update, software distribution and collection of hardware/software information, or fetch agent information, the server/policy administrator must send the agent computer the corresponding commands.

314 The policy server decides whether to re-create the ID of the policy server in sending a restart command. The policy server ID, which consists of the MAC address of the network card on the policy agent computer and OS type, is unique, and helps the policy server to identify a policy agent. In communicating with the policy agent, the policy server identifies the policy agent by using the ID.

315 The status of the policy agent is confirmed by the policy center admin. The policy agent sends 'Service Available' or "Service Unavailable' as the response of the corresponding command to the policy server to display it to the authorized server/policy administrator.

316 If the authorized server/policy administrator request to delete the policy agent from the managed computers, the policy server stops the policy agent, deletes it from the list, which means that the policy server does not delete the policy agent itself but delete it only from the managed computer list.

SmartUpdate Configuration

317 The authorized server/policy administrator is allowed to search/modify the smart update configuration of V3 as the same way in the V3_SmartUpdate: update file type (engine, and patch), auto-update settings, update method, and scheduled update

Policy Agent Configuration

318 The authorized server/policy administrator can use the default policy settings at the first configuration.

319 The authorized server/policy administrator of the policy server enforces V3 to run according to configurations. Not only the authorized server/policy administrator but also monitor center are able to view the configurations of the policy agent.

320 In the configuration of the policy agent, selecting a management product, setting the policy download interval, the policy agent information upload interval, the policy agent patch interval, and the time synchronization of V3 products, and other security products by AhnLab, Inc. are available.

321 The authorized server/policy administrator is able to decide whether to display the operating settings menu (showing tray icon, pause, and delete option) of the policy agent. If the showing try icon option is enabled, the icon of the policy agent is displayed on the tray. If the operating setting menu is enabled, the authorized

general user is able to select pause or terminate option through the tray menu of the policy agent, and to select the policy agent from the Add/Remove menu of the Windows. If the Allow access when password is entered option of the pause, termination are enabled, only authorized general users entered the password set by APC_AgentKey are allowed to use the functions.

322 The policy agent enforces V3 to download engine/patch files from the policy server if the engine version of V3 is lower than one in the policy server. The authorized server/policy administrator is able to specify the settings: engine and program patch files, and update interval (Update at specific time everyday, Update when system starts, and Update repeatedly). If the update is on the restrict update time, the engine/patch files will be downloaded.

323 The policy server is able to apply the common policy agent configurations to a group of V3 installed computers.

- When applying policies to a group, the policy server modifies the configuration of the group policy, and transmits the policy to policy agents which conform to the group policy. Therefore, If the policy agents conforms to the group policy, they can be applied even though they are not located in the same group. If they are set to conform an individual group, they are out of the target.
- If the policy server applies a policy by policy agent, the policy is applied to the corresponding policy agent. If the policy agent conforms to the group policy, the policy server transmits a group policy, and if the policy agent conforms to the individual policy, the policy server transmits an individual policy.

324 Security Functional Requirements Mapping: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.25 Policy Agent V3 Configuration (APC_V3Policy)

325 The policy server communicates with the policy agent on the V3 installed computer. Before starting the communication, the policy server checks the ID of the policy agents to conform whether the policy agent is created by the policy server. After the successful identification, the policy agent transmits the commands and data from the policy server to V3. The policy server provides a security management interface of V3 through the policy center admin.

326 The policy server is able to apply the common policy agent configurations to a group of V3 installed computers. The configuration by group has the higher priority than one by an individual. The policy server is able to apply the common V3 configurations to V3 installed computers by grouping them as the same way of APC_Agent.

- When applying policies to a group, the policy server modifies the configuration of the group policy, and transmits the policy to policy agents which conform to the group

policy. Therefore, If the policy agents conforms to the group policy, they can be applied even though they are not located in the same group. If they are set to conform an individual group, they are out of the target.

- If the policy server applies a policy by policy agent, the policy is applied to the corresponding policy agent. If the policy agent conforms to the group policy, the policy server transmits a group policy, and if the policy agent conforms to the individual policy, the policy server transmits an individual policy.

327 V3 configuration interfaces of the policy server are the same as provided for authorized general users of V3. The following configurations specified by the policy server through the policy center admin are transmitted and applied to V3.

Function/Data	Related TSS of V3
Virus Scan/Repair	V3_Medic (System Scan, Scheduled Scan, Screen Saver Scan, System Real Time Scan, Internet Real Time Scan, Instant Messenger Real Time Scan, Startup Program Real Time Scan, Outlook Scan, Outlook Real Time Scan, POP3 Real Time Scan, Windows Explorer Scan, Office Protector)
Advance Scan	V3_Medic
Warning Mail	V3_WarnMail
Alert Icon Indication	V3_Alert
Self Scan	V3_SelfProtect
V3 Configuration Security (Setting Password)	V3_CM
Use Items Not to Scan	V3_Medic
Check System Restore Folder	V3_Medic

328 The authorized monitor center is able to view the configurations above. The security password string for configuration, and the disk space information of V3 are not available, and only the operating status (on/off), security target (the termination of system monitoring, and program deletion), and the status of password setting are available.

329 The policy server provides DEFAULT_GROUP to manage V3 configurations of the policy agent with consistency. When setting a new group policy and each configuration of each policy agent by modifying V3 configurations of DEFAULT_GROUP, the authorized server/policy administrator provides the security management function to apply the default via the import function.

330 Security Functional Requirements Mapping: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.1.26 APC Audit Record (APC_Log)

331 The policy server generates and stores audit records for the result of the functions in the policy agent, and policy center admin in the DBMS. The authorized administrator is able to view service events created by the policy server, virus warnings, and event logs from V3. The audit record of virus warning is identical with scan log of V3 (V3 audit records – V3_Log). Each audit record types has the following fields:

- **Service Event (Audit records generated by each services of the policy server**) – time, service name, event message
- **Policy Agent Event (Audit records generated by the policy agent)** – time, domain name, policy agent ID, IP address, computer name, user name (computer name of V3), group name, event message
- **Virus Warning (scan log of V3)** – time, domain name, policy agent ID, IP address, computer name, user name (computer name of V3), group name, virus name, diagnosis/repair status, scan method, file name, infector
- **V3 Event (event log of V3)** - time, domain name, policy agent ID, IP address, computer name, user name (computer name of V3), group name, event level (V3 audit type – normal, warning, and error), event occurred module (V3 function name), event message.

332 All audit records above provide the user who generates each audit events. For the service event, the service name is the user who generates the audit records and the policy agent ID field is the user for policy agent event, virus warning, and V3 event. The policy server allows the authorized administrator to sort all fields.

333 The authorized server administrator is allowed to be transmitted or stored audit data of V3 selectively. First, when transmitting audit data of V3 to the policy server, the administrator can specify the type (scan log, or event log) of audit data to transmit. After receiving audit data, the administrator can also specify type (scan log, or event log) of audit data to store in the DBMS.

334 The policy server records the page movement, and the modification history of the security management with the time and tasks, and asks whether to store the task history of the authorized administrator to the administrator' PC at a logout attempt of the administrator. If the administrator asks to store it, the policy center admin store the audit data file as text file to the specified location set by the administrator.

335 The policy center admin provides the following search functions of the audit data for the authorized server administrator.

- Audit data of the operation control and time for each service (policy service, policy agent service, log service, policy agent scheduler, and deliver service) of the policy server.

- Audit data of the authorized administrator's tasks, which includes the following detailed information: task time, computer name, login IP address, user ID (authorized administrator), and data (tasks).
- Audit data of the authorized administrator's task history, which includes the following detailed information: command (security management command) time by authorized administrator's ID, task type (command contents), task target (computer name of the policy agent and IP address), details, and task id.
- Audit data of the update by the policy server, which includes the following detailed information: update time, management product, update component (patch, and engine), and message.
- Audit data of the backup by the policy server, which includes the following detailed information: backup time, and backup result (backup type – classify/delete, and result).

336 Audit data (event log and scan log) generated from V3 is transmitted to the policy server via the policy agent. The authorized administrator queries and searches the transmitted audit data stored in the policy server by using an interface of the policy center admin.

337 The administrator is able to delete all or specific audit data in the query screen, which does not delete the audit data in the DBMS but in the query screen. If the administrator requests to query the audit data after deleting an audit record in the query screen, the deleted record will be displayed in the query screen because the query request retrieves the audit data from the DBMS.

338 Security Functional Requirements Mapping: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1(2), FAU_SAR.2, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

6.2 Assurance Measure

339 The assurance measures for the assurance requirements specified in this Security Target comply with the assurance requirements specified in Part 3 of the Common Criteria for the Information Protection System. [Table 5] shows the list of documents that can verify compliance with the assurance requirements.

[Table 4] Assurance Measure

Assurance component ID	Assurance Component Name	Assurance Document
ACM_AUT.1	Partial CM Automation	V3Pro 2004 and AhnLab Policy Center 3.0 Configuration Management Document V1.5
ACM_CAP.4	Authorization controls	V3Pro 2004 and AhnLab Policy Center 3.0 Configuration Management Document V1.5
ACM_SCP.2	TOE CM Coverage	V3Pro 2004 and AhnLab Policy Center 3.0 Configuration Management Document V1.5
ADO_DEL.2	Delivery procedure	V3Pro 2004 and AhnLab Policy Center 3.0 Delivery Document V1.6 AhnLab Policy Center 3.0 User Guide Part 1 V 3.0.12 AhnLab Policy Center 3.0 User Guide Part 2 V 3.0.12
ADO_IGS.1	Installation, Generation, and Start-up Procedures	V3Pro 2004 User Guide 6.0.10 AhnLab Policy Center 3.0 User Guide Part 1 V 3.0.12 AhnLab Policy Center 3.0 User Guide Part 2 V 3.0.12
ADV_FSP.2	Well-defined external interface	V3Pro 2004 and AhnLab Policy Center 3.0 Functional Specification V1.6
ADV_HLD.2	Basic design separating security function and non-security function	V3Pro 2004 and AhnLab Policy Center 3.0 High-level Design V1.6
ADV_IMP.1	Implementation of the TSF	V3Pro 2004 and AhnLab Policy Center 3.0 Implementation Representation V1.2
ADV_LLD.1	Descriptive low-level Design	V3Pro 2004 and AhnLab Policy Center 3.0 Low-level Design V1.5
ADV_RCR.1	Informal correspondence TOE security policy model	V3Pro 2004 and AhnLab Policy Center 3.0 Correspondence Analysis Report V1.1
ADV_SPM.1	Informal correspondence TOE security policy model	V3Pro 2004 and AhnLab Policy Center 3.0 Security Policy Modeling V1.2
AGD_ADM.1	User Guidance	V3Pro 2004 User Guide V6.0.10 AhnLab Policy Center 3.0 User Guide Part 1 V 3.0.12 AhnLab Policy Center 3.0 User Guide Part 2 V 3.0.12
AGD_USR.1	User Guidance	-

Assurance component ID	Assurance Component Name	Assurance Document
ALC_DVS.1	Identification of security measures	V3Pro 2004 and AhnLab Policy Center 3.0 Development Security Document V1.3
ALC_LCD.1	Developer-defined life cycle model	V3Pro 2004 and AhnLab Policy Center 3.0 Life-cycle Definition Document V1.2
ALC_TAT.1	Well-defined development tools	V3Pro 2004 and AhnLab Policy Center 3.0 Development Tool Document V1.3
ATE_COV.2	Analysis of Coverage	V3Pro 2004 and AhnLab Policy Center 3.0 Test Document V1.3
.ATE_DPT.1	Testing: low-level design	V3Pro 2004 and AhnLab Policy Center 3.0 Test Document V1.3
ATE_FUN.1	Functional testing	V3Pro 2004 and AhnLab Policy Center 3.0 Test Documentation V1.3
ATE_IND.2	Independent testing - Sample	V3Pro 2004 (6.1.2.1) AhnLab Policy Center 3.0 (3.0.11.15)
AVA_MSU.2	Evaluation of guidance	V3Pro 2004 and AhnLab Policy Center 3.0 Misuse Analysis Report V1.3
AVA_SOF.1	Strength of TOE security function evaluation	V3Pro 2004 and AhnLab Policy Center 3.0 Strength of Function Analysis Report V1.1
AVA_VLA.2	Independent vulnerability analysis	V3Pro 2004 and AhnLab Policy Center 3.0 Vulnerability Analysis Report V1.0

7. Protection Profile Claims

340 This Security Target does not claim any protection profile.

8. Rationale

8.1 Security Objectives Rationale

[Table 5] Mapping security objectives and threats/policies/assumptions

Security Environment / Security Objectives	A.NO_EVIL	A.PHYSICAL	A.SAFEITENTITY	A.CERT	A.GUARD	A.INTERNALENTITY	A.AVCONFLICT	A.TIMESTAMP	T.AUDIT_COMPROMISE	T.MASQUERADE	T.TSF_COMPROMISE	T.UNATTEND_SESS	T.UNIDENTIFIED_ACTION	T.VIRUS	T.DOWN_INTERFERENCE	T.TRANS_DESTORY	T.RESIDUAL_DATA	P.ROLES	P.AUDIT	P.MANAGEUTIL	P.ANTIHAMFULL	P.STRENGTHENOS
O.ADMIN_ROLE																		×				
O.MANAGE											×	×								×		
O.SELF_PROTECTION											×											
O.VIRUS														×							×	
O.AUDIT									×				×						×			
O.ALARM													×									
O.TSFDATA_PROTECT										×	×					×						
O.INA									×	×	×	×										
O.SECURE_UPDATE														×	×							
O.STRENGTHENOS																						×
OE.AUDIT_STORAGE									×										×			
OE.NO_EVIL	×																					
OE.PHYSICAL		×																				
OE.CERT				×																		
OE.SAFEITENTITY			×																			
OE.TIMESTAMP								×					×						×			
OE.TOE_ACCESS									×	×	×	×										
OE.GUARD					×																	
OE.INTERNALENTITY						×																
OE.AVCONFLICT							×															
OE.AUDIT_SEARCH																			×			
OE.RESIDUAL_INFO																	×					
OE.DOM_SEPARATION									×		×											
OE.NO_BYPASS									×		×											

[Table 6] Security Objectives Rationales

Threat/Policy/Assumption	Security Objective	Rationale
A.NO_EVIL	OE.NO_EVIL	Since OE.NO_EVIL ensures that the administrator who operates the TOE is reliable, It meets A.NO_EVIL.
A.PHISICAL	OE.PHISICAL	Since OE.PHISICAL ensures the policy server is installed in physically safe environment, and protected by un-authorized access, It meets A.PHISICAL.
A.SAFEITENTITY	OE.SAFEITENTITY	Since OE.SAFEITENTITY ensures the external servers interacting with the TOE for security functions and administrator's computer shall secure, it meets A.SAFEITENTITY.

A.CERT	OE.CERT	Since OE.CERT ensures that certificate being used to verify engine/patch files from the update server is issued in a secure manner and stored/managed by AhnLab, Inc. and user's IT environment (OS) which verifies the signed files with the certificate keeps up-to-date reliable authentication agency, it meets A.CERT.
A.GUARD	OE.GUARD	Since OE.GUARD ensures that the TOE is installed on the trusted network where is protected by network security devices, it meets A.GUARD.
A.INTERNALENTITY	OE.INTERNALENTITY	Since OE.INTERNALENTITY ensures that IT entities connected to the trusted network and interoperate with the TOE are run with the same security level according to the security policies of network security devices, it meets A.INTERNALENTITY.
A.AVCONFLICT	OE.AVCONFLICT	Since OE.AVCONFLICT ensures that the V3 installed system does not have any other anti-virus software and software with POP3 real-time scan (monitoring), and spam mail filtering, it meets A.AVCONFLICT.
A.TIMESTAMP	OE.TIMESTAMP	Since OE.TIMESTAMP shall provide reliable time stamps from the NTP server or the operating system, it meets A.TIMESTAMP.
T.AUDIT_COMPROMISE	O.INA	Since O.INA checks the access authority of the user by using the identification and authentication function when the user accesses audit data, it counters T.AUDIT_COMPROMISE which takes unauthorized access authority for the audit trail.
	OE.TOE_ACCESS	Since OE.TOE_ACCESS provides means to control the access to the audit data in the IT environment for the authorized general user/restricted general user, it counters T.AUDIT_COMPROMISE.
	O.AUDIT	Since O.AUDIT provides means to review audit data for the authorized user, it counters T.AUDIT_COMPROMISE which takes unauthorized access authority for the audit trail.

	OE.AUDIT_STORAGE	Since OE.AUDIT_STORAGE provides means to store audit data in a secure manner, it counters T.AUDIT_COMPROMISE which prevents audit data from losing, modifying, and recording.
	OE.DOM_SEPARATION	Since OE.DOM_SEPARATION controls and maintains the separated areas for executing of the TOE, general processes are not able to access the audit data. Thereby, it lightens T.AUDIT_COMPROMISE.
	OE.NO_BYPASS	Since OE.NO_BYPASS does not allow violation of the audit data, bypassing the TSF, it counters T.AUDIT_COMPROMISE.
T.MASQUERADE	OE.TOE_ACCESS	OE.TOE_ACCESS is necessary step to control the logical access of general users (V3) to the TOE. OS identifies and authenticates the users to counter T.MASQUERADE.
	O.INA	O.INA counters T.MASQUERADE, guaranteeing that the TOE identifies and authenticates the administrator with uniqueness.
	O.TSFDATA_PROTECT	O.TSFDATA_PROTECT counters T.MASQUERADE by providing means to protect the TSF data, identification and authentication data.
T.TSF_COMPROMISE	O.SELF_PROTECTION	Since O.SELF_PROTECTION protects TSF and TSF resources by preventing the user/process from accessing TSF data via TSFI irrelevantly, it counters T.TSF_COMPROMISE.
	O.MANAGE	Since O.MANAGE limits the access of the user/process by specifying the user with the authority to query/modify/delete TSF data and TSF functions, it counters T.TSF_COMPROMISE.
	O.INA	Since O.INA identifies and authenticates the administrator as a preliminary step for preventing unauthorized access to TSF data, it counters T.TSF_COMPROMISE.
	O.TSFDATA_PROTECT	Since O.TSFDATA_PROTECT protects TSF data transmitted between separated TOEs from unauthorized disclosure, modification, and deletion, it counters T.TSF_COMPROMISE.

	OE.TOE_ACCESS	Since OE.TOE_ACCESS provides the TSF data access control for the authorized general user/restricted general user of V3 in the IT environment, it counters T.TSF_COMPROMISE.
	OE.DOM_SEPARATION	Since OE.DOM_SEPARATION controls and maintains the separated areas for executing of the TOE, general processes are not able to access TSF data. Thereby, it lightens T.TSF_COMPROMISE.
	OE.NO_BYPASS	Since OE.NO_BYPASS does not allow violation of TSF data, bypassing the TSF, it counters T.TSF_COMPROMISE.
T.UNATTEND_SESS	OE.TOE_ACCESS	Since OE.TOE_ACCESS controls the logical access of the TOE by the IT environment, it counters T.UNATTEND_SESS.
	O.MANAGE	Since O.MANAGE prevents unauthorized user access during the idle session of the authorized administrator by carrying out session termination in a secure manner via the policy center admin, it counters T.UNATTEND_SESS.
	O.INA	Since O.INA maintains the session information of the authorized administrator using identification and authentication, and terminates the session between the policy server and the policy center admin after the idle time, it counters T.UNATTEND_SESS.
T.UNIDENTIFIED_ACTIONS	O.AUDIT	Since O.AUDIT provides means to review audit data for the authorized user via the policy center admin, it counters T.UNIDENTIFIED_ACTIONS.
	O.ALARM	Since O.ALARM provides means to send a warning message at a security violation to the general user and the authorized administrator, it counters T.UNIDENTIFIED_ACTIONS.
	OE.SAFEITENTITY	OE.SAFEITENTITY counters T.UNIDENTIFIED_ACTIONS, which the general user and authorized administrator are not identify the potential security violation case by providing the correct audit data.
T.VIRUS	O.VIRUS	Since O.VIRUS provides means to prevent viruses from flowing into the user computer, it counters to T.VIRUS.

	O.SECURE_UPDATE	O.SECURE_UPDATE receives engine/patch files from the update server periodically to keep the latest version of engine/patch files which are necessary to prevent the inflow of the malicious codes. Also, the update is conducted after verifying the integrity (modification/disguise) of the transmitted engine/patch files. Since these processes prevent new viruses, it counters T.VIRUS.
T.DOWN_INTERFERENCE	O.SECURE_UPDATE	Since O.SECURE_UPDATE verifies the identity of the sender and the integrity of the received engine/patch files from the update server, files created by the threat agent can not be applied to V3. Thereby, it counters T.DOWN_INTERFERENCE.
T.TRANS_DESTORY	O.TSFDATA_PROTECT	Since O.TSFDATA_PROTECT protects TSF data transmitted between the policy server and the policy center admin, and the policy server and policy agent from unauthorized disclosure, modification, and deletion, it counters T.TRANS_DESTORY.
T.RESIDUAL_DATA	OE.RESIDUAL_INFO	When TOE release the memory, and re-allocate it to the user/process, since OE_RESIDUAL_INFO removes the remaining information of the memory, it counters T.RESIDUAL_DATA.
P.ROLES	O.ADMIN_ROLE	Since O.ADMIN_ROLE supports the security management role, and limits certain behaviors for the role, it meets P.ROLES
P.AUDIT	O.AUIDT	Since O.AUIDT has the TOE to record and maintain the security audit data, it meets P.AUDIT.
	OE.AUDIT_STORAGE	Since OE.AUDIT_STORAGE ensure the secure storage of the audit data in IT environment of the TOE, it meets P.AUDIT.
	OE.TIMESTAMP	Since OE.TIMESTAMP ensure the time reliability of the audit data, which is necessary to trace the responsibility to the security related behavior using audit data, it meets P.AUDIT.
	OE.AUDIT_SEARCH	Since OE.AUDIT_SEARCH provides the audit data search function in IT environment (DBMS), it meets P.AUDIT.

P.MANAGEUTIL	O.MANAGE	Since O.MANAGE provides all management functions and means to support the authorized general user (V3) or the administrator (APC) in a secure manner, it meets P.MANAGEUTIL.
P.ANTIHAMFULL	O.VIRUS	Since O.VIRUS blocks the default harmful programs defined by AhnLab, Inc., and provides spam filtering, it meets P.ANTIHAMFULL.
P.STRENGTHENOS	O.STRENGTHENOS	Since O.STRENGTHENOS provides means to check the operating system and supporting applications which are necessary to operate the TOE are installed and running properly, and review the vulnerability reinforcement of them, it meets P.STRENGTHENOS.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security functional requirements

[Table 7] Mapping security objectives for the IT Environment and security requirements

Security Objectives for IT Environment / Security Requirement	OE.AUDIT_STORAGE	OE.TIMESTAMP	OE.TOE_ACCESS	OE.AUDIT_SEARCH
FAU_SAR.3				X
FAU_STG.1	X			
FIA_UAU.2			X	
FIA_UAU.6			X	
FIA_UID.2			X	
FPT_STM.1		X		
FTA_SSL.1			X	

[Table 8] Security Requirements Rationale for the IT Environment

Objective	Requirement	Rationale
OE.AUDIT_STORAGE	FAU_STG.1	Since FAU_STG.1 has OS to protect audit data files from the unauthorized deletion, it meets OE.AUDIT_STORAGE.
OE.TIMESTAMP	FPT_STM.1	Since FPT_STM.1 has IT environment to provide the time stamp for the TOE in a secure manner, it meets OE.TIMESTAMP.
OE.TOE_ACCESS	FIA_UID.2 FIA_UAU.2 FIA_UAU.6	To access the TOE, the user is identified by the TOE. Thereby, FIA_UID.2 meets OE.TOE_ACCESS.

	FTA_SSL.1	To access the TOE, the user is authenticated by the TOE. Thereby, FIA_UAU.2 meets OE.TOE_ACCESS. After the locking of the user session, re-authentication is carried out by the TOE. Thereby FIA_UAU.6 meets OE.TOE_ACCESS. After the idle time, the session is locked. Thereby FTA_SSL.1 meets OE.TOE_ACCESS.
OE.AUDIT_SEARCH	FAU_SAR.3	IT environment provides the search of the audit data in the policy server. Thereby, FAU_SAR.3 meets OE.AUDIT_SEARCH.

8.2.2 Security Requirements Rationale for TOE

[Table 9] Mapping Security Requirements and TOE Security Objectives

Security Requirement \ Security Objectives	O.ADMIN_ROLE	O.MANAGE	O.SELF_PROTECTION	O.VIRUS	O.AUDIT	O.ALARM	O.TSFDATA_PROTECT	O.INA	O.SECURE_UPDATE	O.STRENGTHENOS
FAU_ARP.1						×				
FAU_GEN.1					×					
FAU_GEN.2					×					
FAU_SAA.1						×				
FAU_SAR.1(1)					×					
FAU_SAR.1(2)					×					
FAU_SAR.2					×					
FAU_SAR.3					×					
FAU_STG.4					×					
FAV_ACT.1(Ext.)			×	×						
FAV_ALR.1(Ext.)			×	×						
FAV_SCN.1(Ext.)			×	×						
FAV_SPM.1(Ext.)			×	×						
FIA_AFL.1								×		
FIA_SOS.1								×		
FIA_UAU.2								×		
FIA_UAU.6								×		
FIA_UID.2								×		
FMT_MOF.1		×								
FMT_MTD.1		×								
FMT_MTD.2		×								
FMT_SMF.1		×								
FMT_SMR.1	×									
FPT_AMT.1										×
FPT_ITI.1									×	
FPT_ITT.1(1)							×			
FPT_ITT.1(2)							×			
FPT_TST.1			×							
FTA_SSL.3		×						×		
FTA_SSL.4(Ext.)		×						×		

[Table 10] Security Requirements Rationale for TOE

Objective	Requirement	Rationale
O.ADMIN_ROLE	FMT_SMR.1	Since FMT_SMR.1 ensures the security management roles of the TOE, it meets O.ADMIN_ROLE.
O.MANAGE	FMT_MOF.1 FMT_MTD.1 FMT_MTD.2 FMT_SMF.1 FTA_SSL.3 FTA_SSL.4 (extension)	Since FMT_MOF.1 defines security management functions of the TOE according to the authorized role, it meets O.MANAGE. Since FMT_MTD.1 defines the management of TSF data for the authorized general user/restricted general user, authorized server/policy administrator/monitor center, it meets O.MANAGE. Since FMT_MTD.2 allows to the authorized general user or authorized server administrator to the threshold of the disk space, and resources (hard disk, memory, and CPU), it meets O.MANAGE. Since FMT_SMF.1 defines the TOE management functions for the TOE management means defined in FMT_MOF.1, FMT_MTD.1, and FMT_MTD.2, it meets O.MANAGE. Since FTA_SSL.3 provides the secure security management by terminating the security management session in the idle time, it meets O.MANAGE. Since FTA_SSL4 (extension) defines a function which terminates the administrator's session in a secure manner for the authorized administrator, it meets O.MANAGE.
O.SELF_PROTECTION	FPT_TST.1 FAV_ACT.1 (extension) FAV_ALR.1 (extension) FAV_SCN.1 (extension)	Since FPT_TST.1, FAV_ACT.1, FAV_ALR.1, and FAV_SCN.1 protect TSF and TSF resources from unauthorized modification by using self scan/repair, and integrity scan, it meets O.SELF_PROTECTION.
O.VIRUS	FAV_ACT.1 (extension) FAV_ALR.1 (extension) FAV_SCN.1 (extension) FAV_SPM.1 (extension)	Since FAV_ACT.1 ensures that there are actions of the TOE for the detection of viruses, it meets O.VIRUS. Since FAV_ALR.1 ensures the function which alerts the user to the detection of the virus, it meets O.VIRUS. Since FVA_SCN.1 allows the TOE to detect viruses, it meets O.VIRUS. Since FAV_SPM.1 prevents spam mails according to the configuration set by the authorized user or authorized administrator using spam mail filtering function, it meets O.VIRUS.

Objective	Requirement	Rationale
O.AUDIT	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1(1)-(2) FAU_SAR.2 FAU_SAR.3 FAU_STG.4	Since FAU_GEN.1 and FAU_GEN.2 ensure defining audit events, and generating audit records, it meets O.AUDIT. Since FAU_SAR.1(1), FAU_SAR.2, and FAU_SAR.3 ensure reviewing audit data for the authorized general user/restricted general user, it meets O.AUDIT. Since FAU_SAR.1(), FAU_SAR.2 ensure reviewing audit data for the authorized administrator, it meets O.AUDIT. Since FAU_STG.4 is required to ensure actions for the prevention of audit data loss if the audit trail is full, it meets O.AUDIT.
O.ALARM	FAU_ARP.1 FAU_SAA.1	Since FAU_APR.1 defines the alarm for the general user or authorized administrator in case of the potential security threat defined in FAU_SAA.1, it meets O.ALARM. Since FAU_SAA.1 defines the potential security violation event by analyzing audited events, it meets O.ALARM.
O.TSFDATA_PROTECT	FPT_ITT.1(1)-(2)	Since FPT_ITT.1(1)-(2) defines the requirements to prevent disclosure and detect modification for the TSF data communication among the policy server, policy center admin, and policy agent, which is the basic internal TSF data transfer protection, it meets O.TSFDATA_PROTECT.
O.INA	FIA_AFL.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.6 FIA_SOS.1 FTA_SSL.3 FTA_SSL.4 (extension)	Since FIA_AFL.1 defines the limit of failed the authentication attempts, the response action in case that the failed attempts reaches or excesses the limit, it meets O.INA. Since FIA_SOS.1 provides a mechanism to verify that the secrets meet the defined limit, it meets O.INA Since FIA_UAU.2 ensures the successful authentication of the administrator, it meets O.INA. Since FIA_UAU.6 requires the administrator to be re-authenticated when the session is terminated in the idle time, it meets O.INA. Since FIA_UID.2 ensures the successful identification of the administrator, it meets O.INA. Since FTA_SSL.3 re-authenticates the administrator in

Objective	Requirement	Rationale
		case the session is terminated by exceeding the idle time, it meets O.INA. Since FTA_SSL.4 (extension) ensures the termination of the session at a request of the authorized administrator, it meets O.INA.
O.SECURE_UPDATE	FPT_ITI.1	Since FPT_ITI.1 verifies the integrity of the files and authenticates the distributor when receiving engine/patch files from the update server, it meets O.SECURE_UPDATE.
O.STRENGTHENOS	FPT_AMT.1	Since FPT_AMT.1 defines means to report the vulnerabilities of the operating system and application which are necessary to run the TOE to the administrator, it meets O.STRENGTHENOS.

8.2.3 Assurance Requirements Rationale

341 EAL4 allows a developer to gain maximum assurance from the security engineering based on the solid Commercial Development methodology. The solid Commercial Development methodology does not require substantial specialized knoledge, skill, or other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs. The TOE that meets the requirements defined in this Security Target is developed by the development engineering thereby the TOE may be assured by the EAL4. Since the extension components (FAV_ACT.1, FAV_ALR.1, FAV_SCN.1, FTA_SSL.4, and FAV_SPM.1) are also defined in the similar level of the components in CC part 2, the EAL4 assurance package requirements are sufficient to evaluate the corresponding functions and extra assurance components are not necessary. Since the TOE security environment in this Security Target has resistance for the threat agent who possessed a low level of knowledge base on AVA_VLA.2, it is sufficient to meet the assurance requirements of the EAL4.

8.3 TOE Summary Specification Rationale

8.3.1 TOE Security Functions Rationale

[Table 11] Mapping TOE Security Requirements and TOE Summary Specification

Security Requirement / Summury Spec.	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1(1)	FAU_SAR.1(2)	FAU_SAR.2	FAU_SAR.3	FAU_STG.4	FAV_ACT.1	FAV_ALR.1	FAV_SCN.1	FAV_SPM.1	FIA_AFL.1	FIA_SOS.1	FIA_UAU.2	FIA_UAU.6	FIA_UID.2	FMT_MOF.1	FMT_MTD.1	FMT_MTD.2	FMT_SMF.1	FMT_SMR.1	FPT_AMT.1	FPT_ITI.1	FPT_ITT.1(1)	FPT_ITT.1(2)	FPT_TST.1	FTA_SSL.3	FTA_SSL.4
V3_SmartUpdate																			×	×		×								
V3_CodeSigning																									×			×		
V3_CM																			×	×		×								
V3_Medic										×	×	×							×	×		×						×		
V3_SelfProtect																			×			×						×		
V3_WarnMail											×								×	×		×								
V3_SpamFilter													×						×	×		×								
V3_FileBackup										×										×		×								
V3_Alert	×			×							×								×			×								
V3_Disk									×										×		×	×								
V3_Report																			×	×		×		×						
V3_Log		×	×		×		×	×												×		×								
APC_INA														×	×	×	×	×		×		×	×						×	×
APC_SecureComm																										×	×			
APC_Update																			×	×		×								
APC_CodeSigning																									×			×		
APC_Time																			×			×								
APC_Integrity																			×			×						×		
APC_AgentKey																				×		×								
APC_Service																			×	×		×								
APC_BackupConfig																				×		×								
APC_Notice	×			×															×	×	×	×								
APC_Summary																				×		×								
APC_Agent																			×	×		×								
APC_V3Policy																			×	×		×								
APC_Log		×	×			×	×												×	×		×								

[Table 12] TOE Summary Specification Rationale

Security Function	TOE Summary Spec.	Rationale
FAU_ARP.1	V3_Alert APC_Notice	Since V3_Alert sends a warning message at a security violation event like viruses, it meets FAU_ARP.1 Since APC_Notice alarm the security violation by using email and notice, it meets FAU_ARP.1.
FAU_GEN.1	V3_Log APC_Log	Since V3_Log and APC_Log provides the audit record generation function at an event related to the security in the TOE, it meets FAU_GEN.1.
FAU_GEN.2	V3_Log APC_Log	Since V3_Log and APC_Log include the information of the user (process, and IT entity) who causes audit records in the audit records, it meets FAU_GEN.2.
FAU_SAA.1	V3_Alert APC_Notice	Since V3_Alert sends a message at a security violation event such as update success/failure and well-known vulnerability, it meets FAU_SAA.1. Since APC_Notice alarm update, server start/failure, and excess of the resource's threshold by using email and notice, it meets FAU_SAA.1.
FAU_SAR.1(1)	V3_Log	Since V3_log allows users to query V3 audit data generated

Security Function	TOE Summary Spec.	Rationale
		from the his own system, it meets FAU_SAR.1(1).
FAU_SAR.1(2)	APC_Log	Since APC_Log allows the authorized administrator to query the audit records of V3 and APC, it meets FAU_SAR.1(2).
FAU_SAR.2	V3_Log APC_Log	V3_Log and APC_Log allow only the authorized administrator (APC) to view audit records of V3. In case of the authorized general user/restricted general user, viewing audit records through the interface provided by V3 is allowed. Thereby, it meets FAU_SAR.2. In addition, using the interface provided by APC to view audit records of APC is available. Thereby it meets FAU_SAR.2.
FAU_SAR.3	V3_Log	Since V3_Log provides the selectable audit review function for the authorized general user/restricted general user, it meets FAU_SAR.3.
FAU_STG.4	V3_Disk	Since V3_Disk provides the prevention of audit data loss function which overwrites the oldest stored audit records if the audit trail is full by specifying the disk space to store audit records of V3, it meets FAU_STG.4.
FAV_ACT.1	V3_Medic V3_FileBackup	Since V3_Medic provides repair actions when the virus is detected on the V3 system and V3 files, it meets FAV_ACT.1. Since V3_FileBackup provides backup actions for the infected files, it meets FAV_ACT.1.
FAV_ALR.1	V3_Medic V3_WarnMail V3_Alert	Since V3_Medic alarm the general user when a virus is detected on the V3 system and V3 files, it meets FAV_ALR.1 Since V3_WarnMail sends a warning mail for the virus infected mail, it meets FAV_ALR.1. Since V3_Alert displays a virus detection message, and alarm the user with the sound when detecting a virus, it meets FAV_ALR.1.
FAV_SCN.1	V3_Medic	Since V3_Medic provides the self scan function, which scans the V3 system, and V3 files, it meets FAV_SCN.1
FAV_SPM.1	V3_SpamFilter	Since V3_SpamFilter scans spam mails on the V3 system according to spam filtering rules set by the authorized general user or authorized server/policy administrator, it meets FAV_SPM.1.
FIA_SOS.1	APC_INA	Since APC_INA provides the password mechanism for the administrator's identification and authentication, and the password meets the allowable rules of FIA_SOS.1, it meets FIA_SOS.1.
FIA_AFL.1 FIA_UAU.2 FIA_UID.2	APC_INA	Since APC_INA carries out the administrator's identification and authentication for the security management, it meets FIA_AFL.1, FIA_UAU.2, and FIA_UID.2. And then, APC_INA defines the authentication failure limit, and the authentication delay function is carried out if the

Security Function	TOE Summary Spec.	Rationale
		authentication failure reaches or surpluses the limt. Thereby, it meets FIA_AFL.1, FIA_UAU.2, FIA_UID.2.
FIA_UAU.6 FTA_SSL.3 FTA_SSL.4 (extension)	APC_INA	Since APC_INA terminates the administrator's session and requests re-authentication if the idle time keeps up for a specific time on the administrator's session after logging in to the policy server via the policy center admin, it meets FIA_UAU.6, FTA_SSL.3, and FTA_SSL.4 (extension). In addition, if the authorized administrator request to log out from the server, APC_INA terminates the session and requests re-authentication. Thereby it meets FIA_UAU.6, FTA_SSL.3, and FTA_SSL.4 (extension).
FMT_MOF.1	V3_SmartUpdate V3_CM V3_Medic V3_SelfProtect V3_WarnMail V3_SpamFilter V3_Alert V3_Disk V3_Report APC_Update APC_Time APC_Integrity APC_Service APC_Notice APC_Agent APC_V3Policy APC_Log	V3_SmartUpdate, V3_CM, V3_Medic, V3_SelfProtect, V3_WarnMail, V3_SpamFilter, V3_Alert, V3_Disk, V3_Report, APC_Update, APC_Time, APC_Integrity, APC_Service, APC_Notice, APC_Agent, APC_V3Policy and APC_Log allows the authorized general user/restricted general user (V3) or the authorized administrator (APC) to start/stop or determine the behavior of the security function, it meets FMT_MOF.1.
FMT_MTD.1	V3_SmartUpdate V3_CM V3_Medic V3_WarnMail V3_SpamFilter V3_FileBackup V3_Report V3_Log APC_INA APC_Update APC_AgentKey APC_Service APC_BackupConfig APC_Notice APC_Summary APC_Agent APC_V3Policy APC_Log	Since V3_SmartUpdate, V3_CM, V3_Medic, V3_WarnMail, V3_SpamFilter, V3_FileBackup, V3_Report, V3_Log, APC_INA, APC_Update, APC_AgentKey, APC_Service, APC_BackupConfig, APC_Notice, APC_Summary, APC_Agent, APC_V3Policy, and APC_Log provides the management function for the following security attributes: rule/list, audit data, and password, it meets FMT_MTD.1. Since APC_Agent, APC_INA, and APC_Log allows the monitor staff of policy server to query the configuration of the policy agent and V3, and audit data, it meets FMT_MTD.1.
FMT_MTD.2	V3_Disk	Since V3_Disk provides the management function of the

Security Function	TOE Summary Spec.	Rationale
	APC_Notice	threshold of the audit data storage, it meets FMT_MTD.2. Since APC_Notice notify when the policy server's resource reaches the threshold, it meets FMT_MTD.2.
FMT_SMF.1	V3_SmartUpdate V3_CM V3_Medic V3_SelfProtect V3_WarnMail V3_SpamFilter V3_FileBackup V3_Alert V3_Disk V3_Report V3_Log APC_INA APC_Update APC_Time APC_Integrity APC_AgentKey APC_Service APC_BackupConfig APC_Notice APC_Summary APC_Agent APC_V3Policy APC_Log	V3_SmartUpdate, V3_CM, V3_Medic, V3_SelfProtect, V3_WarnMail, V3_SpamFilter, V3_FileBackup, V3_Alert, V3_Disk, V3_Report, V3_Log, APC_INA, APC_Update, APC_Time, APC_Integrity, APC_AgentKey, APC_BackupConfig, APC_Notice, APC_Summary, APC_Agent, and APC_V3Policy provides the management function of the security function behavior, security function data, and TSF data threshold. V3 provides easy configuration and default configuration (resetting). The policy server provides the policy agent installation program management function for the authorized server administrator.
FMT_SMR.1	APC_INA	Since APC_INA performs identification and authentication according to the role (server administrator/policy administrator/monitor center) of each administrator, it meets FMT_SMR.1.
FPT_AMT.1	V3_Report	Since V3_Report scans vulnerabilities of the operating system where V3 is installed, and allows the authorized general user/restricted general user to view the result, it meets FPT_AMT.1.
FPT_ITI.1	V3_CodeSigning APC_CodeSigning	Since V3_CodSigning and APC_CodeSinging provides means to prevent the modification and masquerade during the update from the update server, and CodeSigining is implemented on V3 and APC individually, it meets FPT_ITI.1,
FPT_ITT.1(1)	APC_SecureComm	Since APC_SecureComm provides secrecy and integrity through the policy center admin, and the policy server, it meets FPT_ITT.1(1).
FPT_ITT.1(2)	APC_SecureComm	Since APC_SecureComm provides secrecy and integrity when transmitting the configurations defined in the policy server to the policy agent, it meets FPT_ITT.1(2).
FPT_TST.1	V3_CodeSigning	Since V3_CodeSigning, V3_Medic, V3_SelfProtect,

Security Function	TOE Summary Spec.	Rationale
	V3_Medic V3_SelfProtect APC_CodeSigning APC_Integrity	APC_CodeSigning, and APC_Integrity provides self-scan and integrity for TSF data and executable code in the V3 and the policy server, it meets FPT_TST.1.
FTA_SSL.3	APC_INA	If the authorized administrator keeps the session between the policy server and the policy center admin for the specified time of user inactivity after logging in, APC_INA terminates the session. Thereby it meets FTA_SSL.3.
FTA_SSL.4	APC_INA	Since APC_INA provides the session termination function between the policy server and the policy center admin in case of the authorized administrator's logout request, it meets FTA_SSL.4.

8.3.2 TOE Assurance Measures Rationale

[Table 13] Mapping Assurance Components and Assurance Measures

Assurance Components \ Assurance Measures	형상관리문서	배포문서	기능명세서	기본설계서	상세설계서	구현검증명세서	보안정책모델서	일치성분석서	사용설명서	개발보안문서	생명주기지원서	개발도구문서	시험서	오용분석서	기능강도분석서	취약성분석서
ACM_AUT.1	×															
ACM_CAP.4	×															
ACM_SCP.2	×															
ADO_DEL.2		×							×							
ADO_IGS.1									×							
ADV_FSP.2			×													
ADV_HLD.2				×												
ADV_IMP.1						×										
ADV_LLD.1					×											
ADV_RCR.1								×								
ADV_SPM.1							×									
AGD_ADM.1									×							
AGD_USR.1(*)																
ALC_DVS.1										×						
ALC_LCD.1											×					
ALC_TAT.1												×				
ATE_COV.2													×			
ATE_DPT.1													×			
ATE_FUN.1													×			
ATE_IND.2													×			
AVA_MSU.2									×					×		
AVA_SOF.1															×	
AVA_VLA.2																×

[Table 14] Assurance Requirements Rationale

Assurance Measure	Requirement	Rationale
V3Pro 2004 and AhnLab Policy Center 3.0 Configuration Management Document V1.5	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2 provides the configuration management documentation to ensure that the TOE provides the control of denying unauthorized modification, and the relevant use of configuration management system's functionality.
V3Pro 2004 and AhnLab Policy Center 3.0 Delivery Document V1.5, AhnLab Policy Center 3.0 User Guide 3.0.12	ADO_DEL.2	ADO_DEL.2 provides the delivery document to ensure that facilities and procedures that can deliver and control the TOE without any change.
V3Pro 2004 User Guide 6.0.10 AhnLab Policy Center 3.0 User Guide 3.0.12	ADO_IGS.1 AGD_ADM.1 AVA_MSU.2	To assure that the TOE is installed, generated and started in a safe manner that the developer intended, the installation guide document is provided AGD_ADM.1 provides the administrator guidance documents for people who are responsible to configure, maintain, and manage the TOE in a secure manner to

Assurance Measure	Requirement	Rationale
		maximize the security. AVA_MSU.2 has the guidance documentation to be complete, clear, internally consistent, and to include the Misuse Analysis in the user guidance documents to ensure that the secure procedures have been addressed during the operation.
V3Pro 2004 and AhnLab Policy Center 3.0 Functional Specification V1.6	ADV_FSP.2	ADV_FSP.2 provides the functional specification document to describe user interfaces, their operations, TSF operations, and the TOE security functional requirements.
V3Pro 2004 and AhnLab Policy Center 3.0 High-level Design V1.6	ADV_HLD.2	ADV_HLD.2 provides the high level design to describe main components (subsystem) of the TSF and the relations between the subsystem and the functions it provides, and ensure that the TOE provides a proper structure to implement the TSF requirements.
V3Pro 2004 and AhnLab Policy Center 3.0 Security Policy Modeling V1.2	ADV_SPM.1	ADV_SPM.1 provides the TOE security policy model to ensure that TSP described in the Security Target is clear, and consistent.
V3Pro 2004 and AhnLab Policy Center 3.0 Implementation Representation V1.2	ADV_IMP.1	ADV_IMP.1 provides the implementation representation to ensure the analysis by understanding the operations of the TSF in detail.
V3Pro 2004 and AhnLab Policy Center 3.0 Low-level Design V1.5	ADV_LLD.1	ADV_LLD.1 provides the low level design to ensure that the TOE describes internal operations of the TSF and interactions and dependency between modules and the TSF sub-system is accurate and effective.
V3Pro 2004 and AhnLab Policy Center 3.0 Correspondence Analysis Report V1.1	ADV_RCR.1	ADV_RCR.1 provides the correspondence analysis to ensure correspondence among various expressions of the TSF (TOE summary specification, function specification, high-level design, low-level design, and implementation representation).
V3Pro 2004 and AhnLab Policy Center 3.0 Development Security Document V1.3	ALC_DVS.1	ALC_DVS.1 provides the development security documentation to protect the TOE with physical resources, procedures, human resources, and other security users in the development environment.
V3Pro 2004 and AhnLab Policy Center 3.0 V3Pro 2004 and AhnLab Policy Center 3.0 Life-cycle Definition Document V1.2	ALC_LCD.1	ALC_LCD.1 provides the life-cycle definition documentation to control the life-cycle by using procedures, tools, and techniques which are used to develop and maintain the TOE.
V3Pro 2004 and AhnLab Policy Center 3.0 Development Tool Document V1.3	ALC_TAT.1	ALC_TAT.1 provides the development tool documentation to ensure that the TOE is developed safely by describing tools used in development, analysis, and implementation.
V3Pro 2004 and AhnLab	ATE_COV.2	ATE_COV.2 provides test documents to prove the TOE is

Assurance Measure	Requirement	Rationale
Policy Center 3.0 Test Documentation V1.3	ATE_DPT.1 ATE_FUN.1 ATE_IND.2	tested with the systematic procedures according to the functional specification. ATE_DPT.1 provides test documents to ensure that TSF subsystems are implemented correctly. ATE_FUN.1 provides test documents to ensure that all security functions run as specified. ATE_IND.2 describes testing tools in the test documents for the evaluator to conduct the independent testing.
V3Pro 2004 and AhnLab Policy Center 3.0 Strength of Function Analysis Report V1.1	AVA_SOF.1	AVA_SOF.1 provides the strength of TOE security functions analysis to determine the strength of the security behavior by quantitative or statistical result for the security behaviors of the lower security mechanism and effort to deal with the result.
V3Pro 2004 and AhnLab Policy Center 3.0 Misuse Analysis Report V1.3	AVA_MSU.2	AVA_MSU.2 provides the misuse analysis to ensure that the guidance documents does not have misleading, unreasonable or conflicting, and secure procedures for all mode of operation have been addressed.
V3Pro 2004 and AhnLab Policy Center 3.0 Vulnerability Analysis Report V1.0	AVA_VLA.2	AVA_VLA.2 identifies security vulnerabilities of the TOE and provides a vulnerability analysis report to ensure that these vulnerabilities will not be intentionally misused.

342 As the administrator who carries out the security roles defined in FMT_SMR.1, the authorized general user/restricted user and authorized administrator carry out the management of security functions and TSF data via FMT_MOF.1 and FMT_MTD.1 by role. Since the TOE does not have the general user, user guidance document (AGD_USR.1) will be not provided.

8.4 Rationale for Functional Requirements SOF (Strength of Function)

343 This Security Target conforms to SOF-medium according to Common Criteria for the information protection system. The session lock function for the security management, policy agent management key setting, and identification and authentication for administrators are implemented by the same password mechanism used probabilistic/permutation mechanism which meets SOF-medium by SOF security function analysis with CEM V2.3 Annex A. Consequently, the TOE is resistant to the threat agent who possessed a low level of knowledge, resource, and motivation.

8.5 Dependencies Rationale

[Table 15] Dependencies Rationale

Section	Component	Dependency	Rationale
TOE Functional Requirements	FAU_ARP.1	FAU_SAA.1	FAU_ARP.1 analyzes the potential violations defined in FAU_SSA.1 to perform security alarms – selected.
	FAU_GEN.1	FPT_STM.1	Since the TOE is not able to provide the reliable time stamps, it is selected from the IT environment security requirement.
	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Selected – This Security Target selects FIA_UID.2 having more hierarchical relationship to FAU_GEN.1 instead of selecting FIA_UID.1.
	FAU_SAA.1	FAU_GEN.1	FAU_SAA.1 generates audit records to analyze the potential violation. – Selected
	FAU_SAR.1(1) FAU_SAR.1(2)	FAU_GEN.1	Selected
	FAU_SAR.2	FAU_SAR.1	Selected
	FAU_SAR.3	FAU_SAR.1	Selected
	FAU_STG.4	FAU_STG.1	Since the TOE is not able to provide the prevention of audit data loss function, it is selected from the IT environment.
	FAV_ACT.1(extension)	FAV_SCN.1, FMT_SMR.1, FAV_ALR.1	Selected – This component defines responses conducted by the TOE when the virus is detected. Since the SFRs (FDP_ACF, and FDP_IFC) defined in CC part 2 handle the access or flow of the user data, they are irrelevant to define actions for the anti-virus product. The dependent component is selected since only users with security roles (FMT_SMR.1) must conduct the virus scan to meet the security requirement. Since the virus repair actions of FAV_ALR.1 is conducted by the user (FMT_SMR.1) after the virus warning, it is dependent on the component.

Section	Component	Dependency	Rationale
	FAV_ALR.1(extension)	FAV_SCN.1, FMT_SMR.1	Selected – This component defines how to alarm users when a virus is detected. Since the SFRs (FDP_ACF, and FDP_IFC) defined in CC part 2 handle the access or flow of the user data, they are irrelevant to define alarm methods for the anti-virus product. In addition, since the component describes the virus prevention function with FAV_ACT.1 and FAV_SCN.1, it is selected. The dependency components are selected since the users with the security roles (FMT_SMR.1) must scan (FAV_SCN.1) to meet the security requirement.
	FAV_SCN.1(extension)	FMT_SMR.1	Selected – This component defines scans to be conducted by the TOE to detect a virus. Since the SFRs (FDP_ACF, and FDP_IFC) defined in CC part 2 handle the access or flow of the user data, they are irrelevant to define actions for the anti-virus product. The dependency components are selected since the users with the security roles (FMT_SMR.1) must scan to meet the security requirement.
	FAV_SPM.1 (extension)	FMT_MTD.1	Selected – This component defines policies to be conducted by the TOE to block spam mail. Since the SFRs (FDP_ACF, and FDP_IFC) defined in CC part 2 handle the access or flow of the user data, they are irrelevant to define actions for blocking spam mail. The dependency components are selected since configuration of the spam rules (FMT_MTD.1) is necessary to apply them to the spam mail block policies.
	FIA_AFL.1	FIA_UAU.1	Selected (hierarchical to FIA_UAU.2)
	FIA_UAU.2	FIA_UID.1	Selected (hierarchical to FIA_UID.2)
	FIA_UAU.6	No dependencies.	–
	FIA_UID.2	No dependencies.	–
	FIA_SOS.1	No dependencies.	–
	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	Selected
	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	Selected
	FMT_MTD.2	FMT_MTD.1, FMT.SMR.1	Selected
	FMT_SMF.1	No dependencies.	–

Section	Component	Dependency	Rationale
	FMT_SMR.1	FIA_UID.2	Selected
	FPT_AMT.1	No dependencies.	-
	FPT_ITI.1	No dependencies.	-
	FPT_ITT.1(1) FPT_ITT.1(2)	No dependencies.	-
	FPT_TST.1	FPT_AMT.1	Selected
	FTA_SSL.3	No dependencies.	-
	FTA_SSL.4(extension)	No dependencies.	- This component defines policies to be conducted by the TOE to terminate the session at a request of the administrator. Since the SFR (FPT_SSL.3) defined in CC part 2 handles the session termination after a specified period of user inactivity, it is added to terminate the session at a request of the administrator.
IT Environment Requirements	FAU_SAR.3	FAU_SAR.1	Selected
	FAU_STG.1	FAU_GEN.1	Selected
	FIA_UAU.2	FIA_UID.1	Selected (hierarchical to FIA_UID.2)
	FIA_UAU.6	No dependencies.	-
	FIA_UID.2	No dependencies.	-
	FPT_STM.1	No dependencies.	-
	FTA_SSL.1	FIA_UAU.1	Selected (hierarchical to FIA_UAU.2)