AirTight Networks SpectraGuard® Enterprise, Version 7.0

Security Target

Version 1.9

November 4, 2014

Prepared By

AirTight® Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043

Revision History

Date	Version	Author	Description
06/01/2010	0.1	Hemant Chaskar	First Draft (Section 1 and FAU, FIA of Section 7)
06/07/2010	0.2	Hemant Chaskar	Incorporated comments on first draft + new sections completed through and including IDS of Section 7.
06/14/2010	0.3	Hemant Chaskar	Incorporated comments from earlier draft. All sections complete except yellow marked parts for which precise info is yet to be known.
06/22/2010	0.4	Hemant Chaskar	Incorporated 8 relevant SFRs from WLAN Access System PP
06/25/2010	0.5	Hemant Chaskar	Incorporated comments on 0.4. Made changes to mapping tables to accommodate new SFRs from WLAN Access System PP.
07/05/2010	0.6	Hemant Chaskar	Filled in acronyms and terminology
07/05/2010	0.7	Hemant Chaskar	Put in Sensor model SS-300-AT-C-50. Changed FCS_BCM_EXT assignment level from 3 to 2.
07/09/2010	0.8	Hemant Chaskar	Made changes to FCS_CKM.4 to simplify key deletion methods.
07/30/2010	0.9	Hemant Chaskar	Added CAC related text in Section 7. Reinserted RADIUS text (which was earlier removed), since we are now able to put RADIUS feature in the CC release.
08/04/2010	1.0	Hemant Chaskar	Made final revisions to CAC related text based on Nancy's input during phone call.
08/31/2010	1.1	Hemant Chaskar	Made slight change to CAC description in Section 7, to reflect the current design that LDAP is not mandatory for CAC.
09/02/2010	1.2	Hemant Chaskar	Addressed EOR comments.
09/04/2010	1.3	Hemant Chaskar	Addressed remaining EOR comments, especially in FAU_SAR.3 and FAU_SEL.1.
12/12/2011	1.4	Hemant Chaskar	Description of upgrade feature added. Changed part number from SS-300-AT to SS-300-AT-C-10. Both numbers refer to the same part, but we have been using the latter in rest of the documents. The actual device shows SS-300-AT-C-10 on label. Added few explanations to address EOR comments on test plan. FIPS information updated. Added information to address action items from IVOR meeting. Removed SS-300-AT-C-50 Sensor since it does not support FIPS only mode.
12/16/2011	1.5	Hemant Chaskar	Server FIPS information updated with certificate number. Added additional description of audit. Changed version number of JRE to be consistent with test environment.
04/25/2012	1.6	Hemant Chaskar	Addressed post team tests comments.

Date	Version	Author	Description
07/31/2014	1.7	Hemant Chaskar	Changes made for maintenance update for version 7.0.
09/23/2014	1.8	Hemant Chaskar	Made changes suggested by evaluator.
11/04/2014	1.9	Hemant Chaskar	Updated for SS-300-AT-C-75

Table of Contents

Section **Page**

Figures and Tables

Figures **Page**

Tables **Page**

1 Security Target Introduction

1.1 Security Target Reference

ST Title: AirTight Networks SpectraGuard Enterprise, Version 7.0 Security Target

ST Version: v1.8

ST Author: AirTight Networks, Inc.

ST Date: September 23, 2014

Assurance Level: EAL2 augmented with assurance component ALC_FLR.2 (EAL2+)

Protection Profile: U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007.

1.1.1 *References*

Table 1-1 provides the references used to develop this Security Target.

Table 1-1: References

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-002, Version 3.1, Revision 3	[CC]
U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007	[IDS System PP]
U.S. Government Protection Profile Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments, Version 1.1, July 25, 2007	[WLAN Access System PP]
User Guide for AirTight Networks SpectraGuard Enterprise Version 7.0	[USER]
Installation Guide for AirTight Networks SpectraGuard Enterprise Server SA-360 Version 7.0	[INSTALL1]
Installation Guide for AirTight Networks SpectraGuard Enterprise Sensor SS-300-AT-C-60 Version 7.0	[INSTALL2]

1.2 TOE Reference

TOE Identification: SpectraGuard Enterprise, Version 7.0:

- SpectraGuard Enterprise Server appliance SA-360 including software version 7.0 builds 7.0.506 and 7.0.507
- SpectraGuard Enterprise Server VMware software SE-SW-VM version 7.0 builds 7.0.506 and 7.0.507
- SpectraGuard Enterprise Sensor appliance SS-300-AT-C-60 including Sensor software version 7.0 build 7.0.506
- SpectraGuard Enterprise Sensor appliance SS-300-AT-C-75 including Sensor software version 7.0 build 7.0.507u1

TOE Vendor: AirTight Networks, Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is wireless intrusion prevention system (WIPS). It consists of SpectraGuard Enterprise Server component (also referred as “Server”), SpectraGuard Enterprise Management Console component (also referred as “Console”), and SpectraGuard Enterprise Sensor component (also referred as “Sensor”).

The Sensors scan WiFi radio channels and wired network segments, and report scan data to the Server. The Server performs analysis of the data reported by Sensors to identify and respond to unauthorized wireless activity. The Console facilitates user interaction with the TOE. The TOE ensures conformance of wireless activity to security policy, and addresses security violations such as rogue WiFi networks, unauthorized WiFi connections, WiFi network mis-configurations and wireless denial of service attacks.

The TOE operates in “overlay” fashion, i.e., Sensors are not inline the wireless connections or the wired connections. Rather, they rely on broadcast nature of the wireless medium to collect wireless scan data. They also rely on broadcast subset of traffic in the wired network to collect wire-side scan data.

The TOE performs following security functionality: auditing of security relevant events; TOE user account administration; cryptographic support of secure communications; TOE user identification and authentication; role based access to management of security functions; TOE user session security functions; trusted communication between components; and system data collection, analysis, review, availability and loss prevention.

1.3.1 *TOE Type*

The TOE is a wireless intrusion prevention system (WIPS)*,* which performs wireless intrusion detection and prevention.

1.3.2 *Hardware/Firmware/Software Required by the TOE*

The TOE consists of Server component, Console component and Sensor component.

Server

a) SpectaGuard Enterprise Server appliance SA-360:
The TOE Server application software version 7.0 (builds 7.0.506 and 7.0.507) is embedded in the SpectraGuard Enterprise Server appliance model SA-360. The appliance hardware and the Linux (Centos 6.5 kernel version 2.6.32-431) operating system installed on the appliance provide support for the intrusion detection and associated security management functions of the TOE, and are included in the TOE.

b) SpectraGuard Enterprise Server application software SE-SW-VM:
The TOE Server application software version 7.0 is also available for VMware ESX, ESXi and vSphere virtual machines versions 4.0 or above. The VMware virtual machine environment provides support for the intrusion detection and associated security management functions of the TOE, and is included in the TOE. SE-SW-VM software is provided as a OVF (Open Virtualization Format) version 1.0 file that is suitable for hosting on VMware ESX, ESXi, and vSphere virtual machines.

Console

The TOE Console version 7.0 runs as JavaScript in Internet Explorer web browser on Microsoft Windows 2000, Windows XP, or Windows 7 machine. It may be run in other web browsers such as Mozilla Firefox and Google Chrome, however the evaluated configuration is tested only on Windows 7 and hence Windows 7 is recommended. There is no need to install any software to run the Console. The Console JavaScript is received from the Server when the Server is accessed from within web browser and is removed from the browser when the web browser is closed.

Sensor

SpectraGuard Enterprise Sensor appliance models SS-300-AT-C-60 and SS-300-AT-C-75:

- The TOE Sensor application software version 7.0 build 7.0.506 is embedded in the Sensor appliance model SS-300-AT-C-60.
- The TOE Sensor application software version 7.0 build 7.0.507u1 is embedded in the Sensor appliance model SS-300-AT-C-75.

The Sensor appliance hardware and the Linux version 2.6.31 operating system installed on it provides support for the intrusion detection and associated security management functions of the TOE, and are included in the TOE.
The evaluated configuration of the TOE requires the following Operational Environment support:

- A secure IP network between Server and Sensors.
- The IP network(s) that are to be monitored for unauthorized wireless access.
- Web Browser for the management console graphical user interface (GUI): Internet Explorer (IE) 9 or higher, running on Windows 7 operating system, which in turn runs on a Intel P4 X86 or equivalent hardware platform, with processor speed of at least 1.4 GHz, at least 1 GB RAM and which supports screen resolution of 1024x768
-
- Text editor such as Microsoft Excel, Notepad, WordPad etc. to view TOE user actions audit logs.
- VMware ESX, ESXi or vSphere virtual machine version 4.0 or above (only for SE-SW-VM Server).

The following Operational Environment components are optional for the evaluated configuration of the TOE.

- A trusted DHCP server for automatic IP address assignment.
- A trusted DNS server for zero configuration installation.
- An NTP server for automatic time setting.
- An email server for the administrator to receive notifications and reports via email.
- A syslog server for administrator alert notifications.
- An SNMP server for administrator alert notifications.
- An external authentication LDAP server that supports LDAPv3 (compliant with RFCs 2251-2256, 2829-2830).
- An external authentication RADIUS server compliant with RFCs 2865 and 2866.
- A managed Wireless Local Area Network (WLAN) to be monitored. (Note: The TOE is also used to enforce no-WiFi policy in those networks that do not have managed WLAN of their own. Hence, existence of a managed WLAN is only optional for operation of the TOE). The

TOE works with all WLAN environments, which are compliant with IEEE 802.11 family of standards.

- In monitored WLAN environments, optional integration with Wireless Local Area Network (WLAN) controller is supported for Aruba controller OS version 3.3 or above, Cisco Wireless LAN Controller (WLC) version 5.2 or above, and HP ProCurve controller version 5.4 or above.
- Unmanaged (neighborhood) Wireless Local Area Networks (WLANs) to be monitored.
- A card reader attached to the computer from where the Console is accessed to facilitate client certificate based authentication using smart cards.

1.4 TOE Description

1.4.1 *Acronyms*

The following table defines product specific and CC specific acronyms used within this Security Target.

Table 1-2: Product and CC Acronyms

Acronym	Definition
AES-CBC	Advanced Encryption Standard – Cipher Block Chaining
AP	Access Point
CA	Certificate Authority
CAC	Common Access Card
CC	Common Criteria [for IT Security Evaluation]
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HMAC-SHA-1	Hash Message Authentication Code-Systematic Hashing-Algorithm-1
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IDS	Intrusion Detection System
IE	Internet Explorer
IP	Internet Protocol
IT	Information Technology
JRE	Java Runtime Environment
LBAR	Location Based Administrative Rights
LDAP	Lightweight Directory Assistance Protocol
MAC	Medium Access Control
MITS	Multifamily Information and Transactions Standard

Acronym	Definition
ND	Network Detector
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PCI	Payment Card Industry
OS	Operating System
OVF	Open Virtualization Format
PP	Protection Profile
RADIUS	Remote Authentication Dial-in User Service
RFC	Request for Comments
SFR	Security Functional Requirements
SSH	Secure Shell
SNDC	Sensor Network Detector Combo
SNMP	Simple Network Management Protocol
SOX	Sarbanes–Oxley Act
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol/Internet Protocol
TLS	Transport Security Layer
TOE	Target of Evaluation
TSF	TOE Security Functions
TSV	Tab Separated Values
UDP	User Datagram Protocol
GUI	Graphical User Interface
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller

1.4.2 *Terminology*

The following table defines product-specific and CC-specific terminology used within this Security Target.

Table 1-3: Product and CC Terminology

Terminology	Definition
Assets	Information or resources to be protected by the countermeasures of a TOE.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.

Terminology	Definition
Audit Log (Audit Trail)	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	To establish the validity of a claimed user or object.
Authentication Object	An object which contains the settings for connecting to and retrieving user data from an external authentication server.
Authorized Administrator (TOE Administrator)	The authorized users that manage the TOE or a subset of its TSF data and management functions.
Availability	Assuring information and communications services will be ready for use when expected.
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria.
Frame	A block of data sent over the link transmitting the identities of the sending and receiving stations, error-control information, and message.
Information Technology (IT) System	May range from a computer system to a computer network.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection	The process of analyzing network traffic for potential intrusions and storing attack data for security analysis.
Intrusion Detection System (IDS)	A combination of sensors, scanners, and analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Event	A record of the network traffic that violated an intrusion policy.
Intrusion Prevention	The concept of intrusion detection with the added ability to block or alter traffic that is undesirable from security perspective.
IT Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Network	Two or more machines interconnected for communications.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs
Scanner data	Data collected by the scanner functions.
Scanner functions	The active part of the scanner responsible for collecting traffic information that may be representative of vulnerabilities in and misuse of IT resources (i.e., scanner data).
Security	A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Terminology	Definition
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Signatures	Patterns of network traffic that can be used to detect attacks or exploits.
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.
WiFi	Wireless network based on IEEE 802.11 protocol family

1.4.3 *Product Description*

The Target of Evaluation (TOE) is wireless intrusion prevention system (WIPS). It consists of SpectraGuard Enterprise Server component (also referred as “Server”), SpectraGuard Enterprise Management Console component (also referred as “Console”), and SpectraGuard Enterprise Sensor component (also referred as “Sensor”).

The Sensors are geographically dispersed to provide full radio coverage of the enterprise premises to be protected against unauthorized wireless activity. These premises typically include enterprise wired local area network that may or may not have managed WiFi extension (managed WiFi access points (APs)) of its own. The Sensors are connected to the Ethernet ports of the wired local area network within the premises to provide full coverage of the local area network subnets. The Sensor application software version 7.0 is embedded in the SpectraGuard Enterprise Sensor appliance models SS-300-AT-C-60 and SS-300-AT-C-75. The Sensors can be operated with external antennas or with internal antennas. The SS-300-AT-C-60 and SS-300-AT-C-75 Sensors with software version 6.7 are FIPS 140-2 Level 2 certified (Certificate #1609). The vendor asserts that there is no change in cryptographic modules for the SS-300-AT-C-75 Sensor or from version 6.7 to version 7.0.

The Sensor appliance models SS-300-AT-C-60 and SS-300-AT-C-75 also includes following third party software to support the Sensor application:

- Linux version 2.6.31 operating system. This is basic Linux kernel and not any specific distribution such as Redhat, CentOS, etc.
- OpenSSL library 0.9.7d along with FIPS Object Module version 1.2 to perform cryptography functions

- Dropbear SSH version 0.52 to support secure remote login access to the Sensor for troubleshooting

The Server is also connected to the local area network. The Server application software version 7.0 is embedded in the SpectraGuard Enterprise Server appliance SA-360. The Server application SE-SW-VM version 7.0 can also be run on VMware ESX, ESXi and vSphere virtual machines version 4.0 and above. The Server application version 6.5 is FIPS 140-2 Level 1 certified (Certificate #1649). In the Server application version 7.0, the OpenSSL library has been upgraded to the latest release 1.0.1g with FIPS object module 2.0.5, which in the Server application version 6.5 was OpenSSL version 0.9.7d with FIPS object module 1.2. The OpenSSL version in the Server application version 7.0 is free from Heartbleed vulnerability. Vendor asserts that there is no change in cryptographic functionality of the TOE from the Server application version 6.5 to version 7.0.

The Server appliance SA-360 and the VMware software SE-SW-VM also include following third party software to support the Server application:

- Linux operating system: Centos version 6.5 with kernel version 2.6.32-431
- OpenSSL library version 1.0.1g along with FIPS Object Module version 2.0.5 to perform cryptography functions
- OpenSSH version 6.5p1 to support secure remote login access to the Server for troubleshooting
- Tomcat web server version 6.0.14
- PostgreSQL database version 9.2.1
- SNMP client: NET-SNMP version 5.5.49
- Syslog client: syslogd version 1.4.1
- Email client: libESMTP version 1.0.6
- LDAP client: OpenLDAP client version 2.4.36
- RADIUS client: FreeRADIUS C library version 1.1.6 and Java library TinyRadius version 1.0

The Console provide graphical user interface (GUI) into the TOE for management of security functions. It runs as JavaScript in Internet Explorer web browser on Microsoft Windows machine. There is no need to install any software to run the Console. The Console JavaScript is received from the Server when the Server is accessed from within web browser and is removed from the browser when the web browser is closed.

The following third party software is required to support the Console:

- Microsoft Windows 7 OS
- Internet Explorer (IE) web browser version 9 or higher
- Text editor which understands TSV (tab separated values) file format, for example, Microsoft Excel, WordPad, Notepad etc.
- Card reader software if optional certificate based authentication is used.

The Sensors scan WiFi radio channels to collect wireless activity information in their vicinity and report this information to the Server. They also scan traffic on the local area network subnets to which they are connected through the Ethernet ports and report the scanned information to the Server. The Server performs analysis of the information reported by Sensors to identify and respond to unauthorized WiFi activity. The Server notifies events related to the unauthorized WiFi activity to administrator, generates compliance reports (DoD, SOX, GLBA, PCI, HIPAA, MITS etc.), and triggers countermeasures to block (prevent) the unauthorized wireless activity.

To accomplish its function, the TOE operates in “overlay” fashion, i.e., Sensors are not inline the wireless connections or the wired connections. Rather, they rely on broadcast nature of the wireless medium to collect wireless scan data. They also rely on broadcast subset of traffic in the wired network to collect wire-side scan data.

The TOE does not provide any traffic forwarding functionality between the wired and wireless media (like the WiFi APs do) unless a separate license is applied. The optional AP functionality of the TOE is outside the scope for this evaluation.

Typical deployment architecture of the TOE is shown in Figure 1.

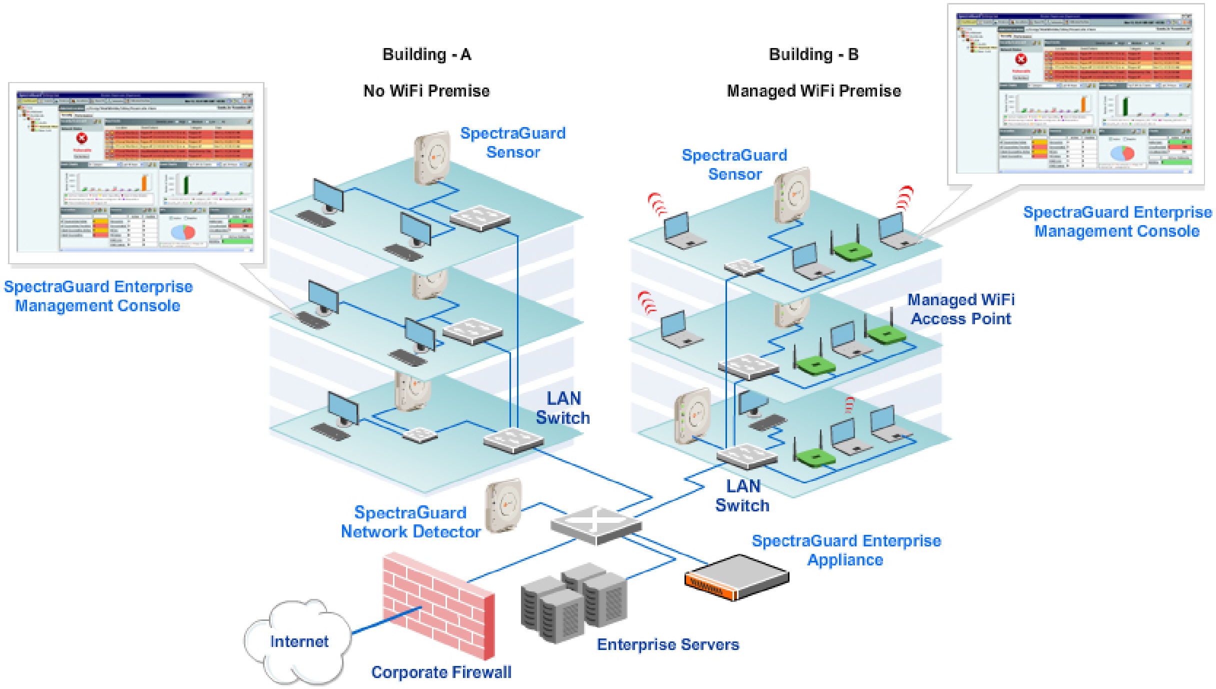
Building - A
No WiFi Premise
Building - B
Managed WiFi Premise
SpectraGuard Sensor
SpectraGuard Sensor
SpectraGuard Enterprise Management Console
SpectraGuard Enterprise Management Console
Managed WiFi Access Point
LAN Switch
LAN Switch
SpectraGuard Network Detector
SpectraGuard Enterprise Appliance
Internet
Corporate Firewall
Enterprise Servers

Figure 1: TOE Architecture and Deployment Example

In the above Figure, Network Detector is a special mode of Sensor application (software switchable mode) which has radio turned off. It then only scans traffic on the wired network.

1.4.4 *Data*

The data managed by the TOE can be categorized as:

TSF Data

- Data used to configure, manage, and operate the TOE such as user accounts
- Audit data produced by the TOE for security significant events

- Data collected by Sensors from wireless medium: The wireless scan data comprises of information gathered from headers of WiFi (IEEE 802.11) transmission frames detected by Sensors on the radio channels, such as identities (MAC addresses) of wireless devices along with their activity and configuration information (connection time, disconnection time, type of connection, security configuration, channel configuration etc.).
- Data collected by Sensors from monitored wired network segments: The wire-side scan data comprises of information gathered by Sensors from wire-side transmission frames (IEEE 802.3 Ethernet) detected on the monitored subnets such as identities (MAC addresses) of devices connected to those subnets.
- Data pertaining to Sensors which are connected to the Server
- Data pertaining to environment in which the TOE is deployed such as location hierarchy
- Data pertaining behavior of TSF such as operating policies
- Data representing output of analysis of scan data such as security events and reports

All TOE data is considered TSF Data. The TOE does not process and does not store enterprise application data that is present in the payloads of WiFi or Ethernet frames.

1.4.5 *Users*

The TOE maintains defined user roles, each with its own set of administrative privileges. When a new user account is created, it must be assigned a role. No access is allowed to the system until a user has been authenticated, and access to TSF data and functions is controlled by the TOE's interfaces only to the data and functions allowed to the authenticated user's role.

All users of the TOE have access to TSF data and management functions (within the scope of their administrative privileges) and therefore are considered administrators for the purposes of this evaluation. The terms "TOE user", "TOE administrator" and "authorized administrator" are used in this ST to refer collectively to all authorized TOE users.

The defined roles for TOE users are Superuser, Administrator, Operator and Viewer.

1.4.6 *Product Guidance*

The AirTight Network SpectraGuard Enterprise Version 7.0 documentation set includes PDF files and online help.

The following product guidance documents are provided with the TOE as PDF files on the Documentation CD included with the product.

Table 1-4: User Guidance Documents

User Guide
Installation Guides for Server and Sensor
Release Notes
Upgrade Instructions
High Availability Configuration Guide
Network Detector Configuration Guide

Product guidance is also included inline the product screens. It can be accessed as follows:

- Clicking the ? icon on top right corner opens context-sensitive help on product screens
- Clicking the “show” link on the context-sensitive help opens entire user guide

Customers with access to AirTight Networks support portal can also access product documentation online.

1.4.7 *Physical Scope of the TOE*

The TOE consists of the components described in Section 1.4.3. The physical boundary of the TOE is as follows:

- SpectraGuard Enterprise Server appliance model SA-360 including the Server software version 7.0 (builds 7.0.506 and 7.0.507) along with the appliance hardware, and the Linux OS and the third party applications included in the appliance.
- SpectraGuard Enterprise Server software SE-SW-VM version 7.0 running on VMware ESX, ESXi or vSphere virtual machine version 4.0 or above along with the hardware of the virtual machine, and the Linux operating system emulated on the virtual machine and the included third party applications.
- SpectraGuard Enterprise Management Console version 7.0 running as JavaScript in Internet Explorer (IE) web browser on Windows 7 computer.
- SpectraGuard Enterprise Sensor appliance SS-300-AT-C-60 including Sensor software version 7.0build 7.0.506 along with the appliance hardware, and the Linux OS and the third party applications included in the appliance.
- SpectraGuard Enterprise Sensor appliance SS-300-AT-C-75 including Sensor software version 7.0 build 7.0.507u1 along with the appliance hardware, and the Linux OS and the third party applications included in the appliance.

The TOE Boundary is depicted in Figure 2 (shown with yellow background). The SpectraGuard Enterprise Server depicted in the figure represents either:
a) SA-360 appliance including its hardware and software
b) SE-SW-VM server software including the virtual machine that hosts it.

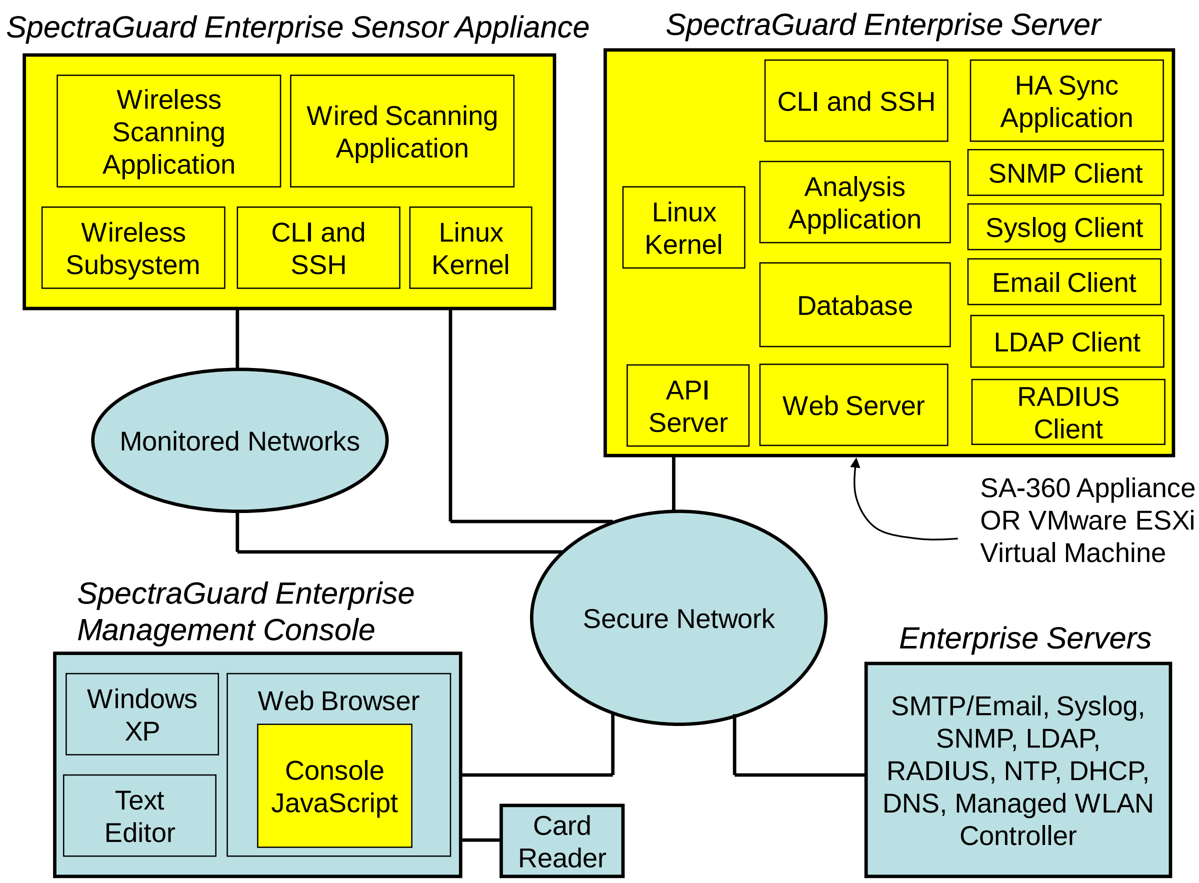

Figure 2: TOE Boundary

The Operational Environment of the TOE includes:

- The web browser used to access the management console of the TOE.
- Text editor used to view audit log.
- The secure network used for communications between the TOE components which must be protected from unauthorized access and which may be the same as or separate from the network that is monitored by the TOE.
- The network(s) that are to be monitored by the TOE.
- VMware ESX, ESXi or vSphere virtual machine version 4.0 or above to host the SE-SW-VM server software.
- An optional trusted DHCP server for automatic IP address assignment.
- An optional trusted DNS server for zero configuration installation. The term “zero configuration” refers to installation of Sensors, wherein the Sensors are automatically able to find the Server to connect to upon powered on and connected into the DHCP enabled network jack (see [INSTALL2] page 11 for details).
- An optional NTP server for automatic time setting.
- An optional email server for the administrator to receive notifications and reports via email.
- An optional syslog server for administrator alert notifications.
- An optional SNMP Server for administrator alert notifications.
- An optional external authentication LDAP server.
- An optional external authentication RADIUS server.

- An optional card reader to facilitate client certificate based authentication using smart cards
- An optional managed Wireless Local Area Network (WLAN) to be monitored by the TOE.
- In managed WLAN environments, optional WLAN controller for integration with TOE.
- Unmanaged (neighborhood) Wireless Local Area Networks (WLANs) to be monitored by the TOE (optional).

1.4.7.1 Included in the TOE:

The evaluated configuration includes the following:

- SpectraGuard Enterprise Server version 7.0 (builds 7.0.506 and 7.0.507)
- SpectraGuard Enterprise Management Console version 7.0
- SpectraGuard Enterprise Sensor version 7.0 (builds 7.0.506 and 7.0.507u1)

The Test Configuration will consist of SpectraGuard Enterprise Server appliance SA-360 including Server software version 7.0 build 7.0.506 and SpectraGuard Enterprise Sensor appliance SS-300-AT-C-60 including Sensor software version 7.0 build 7.0.506. The SpectraGuard Enterprise Management Console will be accessed using Internet Explorer (IE) version 9.0 on Windows 7 computer.

Another Test Configuration will consist of SpectraGuard Enterprise Server software SE-SW-VM version 7.0 build 7.0.507 running on VMware ESXi version 4.0 and SpectraGuard Enterprise Sensor appliance SS-300-AT-C-75 including Sensor software version 7.0 build 7.0.507u1. It suffices to test one virtual machine environment, as others are equivalent and interoperable with it. The SpectraGuard Enterprise Management Console will be accessed using Internet Explorer (IE) version 9.0 on Windows 7 computer.

The Sensor appliance SS-300-AT-C-60 includes two WiFi radio modules. Any of these radio modules can be tuned via software to monitor any WiFi channel. In the SS-300-AT-C-60 Sensor appliance, the first radio module is tuned to rotate on one subset of WiFi channels (in 2.4 GHz band) and the second radio module is tuned to rotate on the other subset of WiFi channels (in 5 GHz band).

1.4.7.2 Excluded from the TOE:

The following product components and functionality are not included in the scope of the evaluation:

- AirTight Mobile, as this feature is optional and requires a separate license.
- High Availability (HA) feature, as it is nothing but redundant Server component.
- Performance Monitoring feature which is concerned with performance monitoring rather than wireless intrusion prevention. It also requires a separate license.
- Integration with WLAN controllers (Aruba, Cisco, HP Procurve), as this feature is optional, requires third party product, and may not operate with every WLAN controller found in the operational environment. This feature requires a separate license. The integration feature is used to read the list of wireless devices managed by the WLAN controllers and automatically populate them as Authorized APs and clients in the TOE. This is done to ease the initial setup, rather than a necessity. That is, TOE is capable to perform this operation even without the WLAN controller integration (e.g., input a file with the list of MAC addresses of such devices, manually categorize devices using GUI menu, etc.). The integration may also be used to read into the TOE a list of unmanaged APs and clients detected by WLAN APs and the signal strengths of such devices. Again, this is not a

necessity, since the TOE itself is capable of detecting all wireless devices and their signal strengths by itself using the channel scanning Sensors. Importantly, the TOE does not write any information to the WLAN controllers. The read only operations are performed either over SNMP or over a JAVA API implemented by the TOE.

- Using Sensor for Wi-Fi access concurrently with or in lieu of Wireless Iintrusion Prevention System (WIPS). This feature is optional and requires a separate license.

Note: The customer must assume the risk of enabling excluded functionality that was not part of the evaluation and has not been tested and validated.

The Operational Environment components listed in Section 1.3.2 are excluded from the scope of the evaluation.

1.4.8 *Logical Scope of the TOE*

The logical scope of the TOE are divided into two groups, one related to the administration and security of the system (Security Audit, Cryptographic Support, Identification and Authentication, Security Management, TOE Access Functions and Protection of Security Functions), and the other related to the collection and analysis of the wireless and wired network traffic (System Data Collection, System Data Analysis and System Data Review, Availability and Loss).

The TOE provides the following security functionality:

1.4.8.1 Security Audit

The TOE is able to audit the use of the administration/management functions. This function records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by TOE users once they are authenticated.

The audit data is protected by the access control mechanisms of the database and OS of the TOE components and by the TOE management Console interface. Only Superuser has access to the audit records. The Superuser can download the audit records for viewing. At the time of downloading, sorting and filtering criteria can be specified for the audit records.

The audit records are stored in the TOE for configurable number of days. Once any record becomes older than the configured lifetime, it is automatically deleted. The TOE does not place any limit on the size of the audit trail, the only limit comes from the size of the disk. When the occupied disk size approaches the capacity, the TOE generates early warning.

Security Audit relies on the Operational Environment with a properly configured text editor (such as Microsoft Excel, WordPad etc.) application to support viewing of the downloaded audit logs. It also depends on the Operational Environment to provide secure communication path between the TOE Server and management Console.

1.4.8.2 Cryptographic Support

The TOE performs cryptographic functions for:
a) Sensor-Server communication
b) Console-Server communication
c) SSH utility in Sensor and Server.

The Sensor-Server communication protocol is proprietary and uses FIPS 140-2 approved algorithms for key generation, encryption and message integrity. The Console-Server communication follows TLS version 1.0 standard and the SSH utility follows SSH version 2 standard. The TOE supports FIPS and non-FIPS operation modes.

1.4.8.3 Identification and Authentication

The TOE requires all users to provide unique identification and authentication data before any access to the system is granted. User identification and authentication is done by the TOE though username/password authentication, optionally using an external authentication server. The TOE also supports client certificate-based authentication option, such as CAC authentication. For certificate-based authentication, TOE supports optional two-factor authentication with password in addition to client certificate.

All authorized TOE users must have a user account with security attributes that control the user's access to TSF data and management functions. These security attributes include user name, password, role and location node identity for TOE users.

The TOE enforces a password policy for users who authenticate via the TOE. The TOE will also prevent a user from accessing the system after a configurable number of failed login attempts.

Identification and Authentication depends on the Operational Environment to provide an external authentication server if that feature is configured. It also depends on the Operational Environment to provide a secure communications path between the TOE and the external authentication server.

1.4.8.4 Security Management

The TOE provides a web-based (using HTTPS) management interface for all run-time TOE administration. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role.

Security Management relies on a management console in the Operational Environment with a properly configured Web Browser to support the web-based management interfaces.

1.4.8.5 TOE Access

The TOE will terminate a user's interactive session after a configurable inactivity time. Before establishing a user session, the will display an advisory warning message regarding unauthorized use of the TOE.

1.4.8.6 Protection of Security Functions

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured through strong encryption during both setup and the transition of data. The TOE Server is FIPS 140-2 Level 1 certified and the TOE Sensor is FIPS 140-2 Level 2 certified.

1.4.8.7 System Data Collection

The TOE detects WiFi threats and vulnerabilities. For this, it collects information from IEEE 802.11 protocol transmission frames detected on WiFi radio channels and IEEE 802.3 protocol traffic detected in the wired part (Ethernet) of the monitored network subnets. Sensors collect the above-mentioned data and send it to the Server.

1.4.8.8 System Data Analysis

The TOE performs various types of analyses such as signatures, anomaly, wired/wireless traffic correlation and devices configuration check, on the collected data to detect wireless threats and vulnerabilities. When threats/vulnerabilities are detected, the TOE generates alarms and (if optionally configured to do so) sends alarms by email, SNMP, syslog etc. to external servers in the operational environment.

1.4.8.9 System Data Review, Availability and Loss

TOE stores user action logs and events data in the database that is included in the TOE. User action logs can be downloaded by authorized administrator from Console as TSV (tab separated values) format file. Events are displayed in tabular form on Console. The user action logs and events are automatically deleted after administrator configured lifetime expires for them. Events are also automatically deleted when total number of events exceeds the administrator configured thresholds. When auto deletion happens, the most recent logs and events are always maintained. The TOE also proactively notifies the administrator via event if the disc occupancy reaches unsafe limits so that administrator can take appropriate action (e.g., backup) to free up the disc space. TOE also facilitates automatic periodic backup of database.

1.4.8.10 Excluded Functionality

The following product components and functionality are not included in the scope of the evaluation:

- AirTight Mobile, as this feature is optional and requires a separate license.
- High Availability (HA) feature, as it is nothing but redundant Server component.
- Performance Monitoring feature which is concerned with performance monitoring rather than wireless intrusion prevention. It also requires a separate license.
- Integration with WLAN controllers (Aruba, Cisco, HP Procurve), as this feature is optional, requires third party product, and may not operate with every WLAN controller found in the operational environment. This feature requires a separate license.
- Using Sensor for Wi-Fi access in addition to or in lieu of WIPS, as this feature is optional and requires a separate license.

Note: The customer must assume the risk of enabling excluded functionality that was not part of the evaluation and has not been tested and validated.

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2 from the Common Criteria Version 3.1 R3. This Security Target conforms to the Common Criteria Version 3.1 R3.

2.2 Protection Profile Claim

This ST claims Demonstrable Compliance to U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007. (IDS System PP).

Demonstrable Compliance in CC v3.1 R3 is defined as follows:

> **demonstrable conformance** - relation between an ST and a PP, where the ST provides a solution which solves the generic security problem in the PP
>
> The PP and the ST may contain entirely different statements that discuss different entities, use different concepts etc. Demonstrable conformance is also suitable for a TOE type where several similar PPs already exist, thus allowing the ST author to claim conformance to these PPs simultaneously, thereby saving work. [CC Part 1 p. 15]
>
> Where there is a clear subset-superset type relation between PP and ST in the case of strict conformance, the relation is less clear-cut in the case of demonstrable conformance. STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP. but can do so in any way that is equivalent or more restrictive to that described in the PP. [CC Part1 p. 92]

This ST incorporates additional SFRs from U.S. Government Protection Profile Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments, Version 1.1, July 25, 2007

Security problem definition:
The conformance rationale in the ST shall demonstrate that the security problem definition in the ST is equivalent (or more restrictive) than the security problem definition in the PP. This means that:

- all TOEs that would meet the security problem definition in the ST also meet the security problem definition in the PP;
- all operational environments that would meet the security problem definition in the PP would also meet the security problem definition in the ST.

This Security Target includes all of the threats, organizational security policies, and assumption statements described in the PP, verbatim.

This Security Target includes additional policies from the WLAN Access System PP:

- P.CRYPTOGRAPHY
- P.CRYPTOGRAPHY_VALIDATED

This Security Target includes additional threats from the WLAN Access System PP:

- T.ACCIDENTAL_CRYPTO_COMPROMISE
- T.POOR_TEST
- T.RESIDUAL_DATA
- T.TSF_COMPROMISE

Therefore, the security problem definition in this ST is equivalent to the security problem definition in the PP.

Security objectives:
The conformance rationale in the ST shall demonstrate that the security objectives in the ST is equivalent (or more restrictive) than the security objectives in the PP. This means that:

- all TOEs that would meet the security objectives for the TOE in the ST also meet the security objectives for the TOE in the PP;
- all operational environments that would meet the security objectives for the operational environment in the PP would also meet the security objectives for the operational environment in the ST.

This Security Target includes all of the TOE Security Objectives from the IDS System PP. In addition the PP Operational Environment Objectives: OE.AUDIT_PROTECTION and OE.AUDIT_SORT have been made TOE objectives: O.AUDIT_PROTECTION, O.AUDIT_SORT, since these security objectives are met by the functionality of the TOE itself. Therefore, the ST is more restrictive than the PP in the case of the TOE objectives.

This Security Target includes all of the Operational Environment Objectives of the IDS System PP with the following exceptions:

- OE.AUDIT_PROTECTION and OE.AUDIT_SORT have been made TOE Objectives as noted above.
- OE.ALARMS has been added to cover the functionality of an Email Server in the environment to send an alarm when a possible intrusion occurs. Based on the following PP requirement, the ST can define where the alarm's destination is located:

  > "IDS_RCT.1.1 The System shall send an alarm to [assignment: alarm destination] and take [assignment: appropriate actions] when an intrusion is detected. (EXT) IDS_RCT.1.1
  > Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The Analyser may optionally perform other actions when intrusions are detected; these actions should be defined in the ST. An intrusion in this requirement applies to any conclusions reached by the analyser related to past, present, and future intrusions or intrusion potential."
- OE.XAUTH has been added to cover the functionality of an external authentication service that can be invoked by the TOE to support user authentication. The PP does not define the authentication mechanism(s) required. Since the external user authentication service is invoked by the TOE, this objective is equivalent to the functionality required by the PP.
- OE.PROTECTCOMM has been added to state that the Operational Environment must provide secure communications between the TOE and the servers in the environment that support the security functionality of the TOE. This objective is the equivalent of a sub-

clause that could be added to or assumed from OE.TIME, OE.ALARMS and OE.XAUTH stating that the services provided by the Operational Environment are secure and reliable.

This Security Target also includes additional Security Objectives from the WLAN Access System PP:

- O.CRYPTOGRAPHY
- O.CRYPTOGRAPHY_VALIDATED
- O.RESIDUAL_INFORMATION
- O.CORRECT_TSF_OPERATION

The security objectives in this ST are therefore equivalent to or more restrictive than the security objective in the PP.

Security requirements:
The ST shall contain all SFRs and SARs in the PP, but may claim additional or hierarchically stronger SFRs and SARs. The completion of operations in the ST must be consistent with that in the PP; either the same completion will be used in the ST as that in the PP or one that makes the requirement more restrictive (the rules of refinement apply).

This Security Target includes all of the Security Assurance Requirements from the IDS System PP. This Security Target includes all of the Security Functional Requirement from the IDS System PP with the following modifications:

- FIA_UAU.1 has been modified into the explicitly stated requirement FIA_UAU_EXT.1 by adding the text *“either by the TSF or by an authentication service in the Operational Environment invoked by the TSF”.* This modification was necessary to provide for the use of an authentication service in the environment that is invoked by the TOE.
- The completion of the assignments in FMT_MOF.1 and FMT_SMR.1 differ from those in the PP since the TOE does not maintain the role: authorized System administrator. The assignments have been made more restrictive to include only those administrative roles that are maintained by the TOE.
- FMT_SMF.1 has been added to satisfy the dependencies of FMT_MOF.1 and FMT_MTD.1.
- Those SFRs exclusively related to authenticating or communicating TSF data with external IT products, specifically: FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.2, have been excluded from the IDS System PP and FPT_ITT.1 has been added to the IDS System PP through the precedence of PD-0097. FPT_ITT.1 has been refined to specify the specific mechanisms used by the TOE for secure internal data transfer.
- FPT_STM.1 was deleted since reliable timestamps are provided by the Operational Environment (OE.TIME).

These changes have been approved by NIAP in the PDs: PD-0151: *Acceptable Demonstrable Assurance for the IDS System PP v1.7 (BR) and PD-0152: Internal Inconsistency within the IDS System PP regarding FPT_STM.*

This Security Target also includes additional Security Functional Requirement modeled on relevant SFRs from the WLAN Access System PP:

- FCS_CKM.1
- FCS_CKM.4
- FCS_COP.1
- FCS_BCM_EXT.1
- FTA_TAB.1

- FTA_SSL.3
- FPT_TST_EXT.1

This Security Target also includes following additional Security Functional Requirements:

- FIA_SOS.1
- FIA_AFL.1

  Note: The FIA_AFL.1 included in the TOE refers to the lockout of local TOE Administrators after a configurable number of unsuccessful login attempts. This SFR has been added to reflect the security functionality of the TOE and has been taken directly from Part 2 of CC 3.1 R3.

  The version of FIA_AFL.1 that was excluded from the IDS System PP was a requirement to detect attempts to access the TOE by untrusted external IT products. The version of FIA_AFL.1 included in the WLAN Access System PP applies to remote administrator login and does not apply to the local login of the TOE.

Therefore, the security requirements in this ST are equivalent to or more restrictive than the security requirements in the PP.

2.3 Package Claim

This ST claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2*.*

3 Security Problem Definition

The following policies, threats and assumptions are identified for the TOE.

3.1 Threats

The following threats are identified for the TOE. The TOE itself has threats and the TOE is responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

This section identifies the threats applicable to the IDS System PP as specified in the Protection Profile, verbatim. Moreover, some relevant threats from the WLAN Access System PP are also included.

Table 3-1: TOE Threats

TOE Threats		
1	T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
2	T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
3	T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
4	T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System’s collection and analysis functions by halting execution of the TOE.
5	T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
6	T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
7	T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
8	T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

TOE Threats		
9	T.ACCIDENTAL_CRYPTO_COMPROMISE	A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
10	T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
11	T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
12	T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).

The following table identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

Table 3-2: IT System Threats

IT System Threats		
13	T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
14	T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
15	T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
16	T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
17	T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
18	T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
19	T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
20	T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
21	T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2 Organizational Security Policies (OSPs)

The following are the OSPs identified for the TOE. An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

This section identifies the organizational security policies applicable to the IDS System PP as specified in the IDS System Protection Profile, verbatim. Moreover, some relevant policies from the WLAN Access System PP are also included.

Table 3-3: Organizational Security Policies

Organizational Security Policies		
1	P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
2	P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
3	P.MANAGE	The TOE shall only be managed by authorized users.
4	P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
5	P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
6	P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
7	P.PROTECT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
8	P.CRYPTOGRAPHY	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
9	P.CRYPTOGRAPHY_VALIDATED	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

3.3 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE applicable to the IDS System PP as specified in the Protection Profile, verbatim.

Table 3-4: TOE Usage Assumptions

TOE Intended Usage Assumptions		
1	A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
2	A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
3	A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.

Table 3-5: TOE Physical Assumptions

TOE Physical Assumptions		
4	A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
5	A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Table 3-6: TOE Personnel Assumptions

TOE Personnel Assumptions		
6	A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
7	A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
8	A.NOTRST	The TOE can only be accessed by authorized users.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. These security objectives, categorized as IT security objectives for either the TOE or its environment are taken from the IDS System PP as specified in the Protection Profile, verbatim, with the following exceptions:

Examples:

- OE.AUDIT PROTECTION and OE.AUDIT_SORT have been made TOE objectives: O.AUDIT_PROTECTION and O.AUDIT_SORT, since these security objectives are met by the functionality of the TOE itself.
- OE.ALARMS has been added to cover the functionality of an Email Server in the environment to send an alarm when a possible intrusion occurs.
- OE.XAUTH has been added to cover the functionality of an external authentication service that can be invoked by the TOE to support user authentication.
- OE.PROTECTCOMM has been added to state that the Operational Environment must provide secure communications between the TOE and the servers in the environment that support the security functionality of the TOE.

Moreover, the following additional security objectives are taken from WLAN Access System PP, verbatim:

- O.CRYPTOGRAPHY, O.CRYPTOGRAPHY_VALIDATED, O.RESIDUAL_INFORMATION. and O.CORRECT_TSF_OPERATION.

4.1.1 *Security Objectives for the TOE*

The following are the TOE security objectives:

Table 4-1: TOE Security Objectives

TOE Security Objectives		
1	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
2	O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
3	O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
4	O. IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
5	O.RESPON	The TOE must respond appropriately to analytical conclusions.

TOE Security Objectives		
6	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
7	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
8	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
9	O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
10	O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
11	O.INTEGER	The TOE must ensure the integrity of all audit and System data.
12	O.EXPORT	When any IDS component makes its data available to other IDS components, the TOE will ensure the confidentiality of the System data.
13	O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
14	O.AUDIT_SORT	The TOE will provide the capability to sort the audit information.
15	O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.
16	O.CRYPTOGRAPHY_VALIDATED	The TOE will use NIST FIPS 140-1/2 validated crypto modules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
17	O.RESIDUAL_ INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
18	O.CORRECT_ TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.

4.1.2 *Security Objectives for the Operational Environment*

The TOE's operating environment must satisfy the following objectives.

Table 4-2: Security Objectives for the Operational Environment

Security Objectives for the Operational Environment		
19	OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
20	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
21	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Security Objectives for the Operational Environment		
22	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
23	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
24	OE.INTROP	The TOE is interoperable with the IT System it monitors.
25	OE.ALARMS	The Operational Environment must provide email service to receive and store email notifications from the TOE.
26	OE.XAUTH *	The Operational Environment must provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.
27	OE.PROTECTCOMM	The Operational Environment must provide secure communications between the TOE and the servers in the environment that support the security functionality of the TOE.

**Note: OE.XAUTH is only applicable when the TOE is configured to use an external LDAP and/or RADIUS authentication service.*

4.2 Security Objectives Rationale

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

4.2.1 *Rationale for the IT Security Objectives*

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the IDS System PP. Table 4-3: Security Objectives and Security Environment Mapping demonstrates the mapping between the assumptions, threats, and policies to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 4-3: Security Objectives and Security Environment Mapping

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.AUDIT_SORT	O.AUDIT_PROTECTION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.RESIDUAL_ INFORMAT ION	O.CORRECT_TSF_OPERATION	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.ALARMS	OE.TIME	OE.PROTECTCOMM	OE.XAUTH
A.ACCESS																							X				
A.DYNMIC																						X	X				
A.ASCOPE																							X				
A.PROTCT																				X							
A.LOCATE																				X							
A.MANAGE																						X					
A.NOEVIL																			X	X	X						
A.NOTRST																				X	X						
T.COMINT	X						X	X			X															X	X
T.COMDIS	X						X	X				X														X	X
T.LOSSOF	X						X	X			X															X	X
T.NOHALT		X	X	X			X	X																		X	X
T.PRIVIL	X						X	X																		X	X
T.IMPCON						X	X	X											X							X	X
T.INFLUX									X															X		X	
T.FACCNT										X																	
T.SCNCFG		X																									
T.SCNMLC		X																									
T.SCNVUL		X																									
T.FALACT					X																			X		X	
T.FALREC				X																							

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.AUDIT_SORT	O.AUDIT_PROTECTION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.RESIDUAL_ INFORMAT ION	O.CORRECT_TSF_OPERATION	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.ALARMS	OE.TIME	OE.PROTECTCOMM	OE.XAUTH
T.FALASC				X																							
T.MISUSE			X																								
T.INADVE			X																								
T.MISACT			X																								
T.ACCIDENTAL_CRYPTO_COMPROMISE	X																X										
T_POOR_TEST																		X									
T_RESIDUAL_DATA																	X										
T_TSF_COMPROMISE	X																X										
P.DETECT		X	X							X															X	X	
P.ANALYZ				X																							
P.MANAGE	X					X	X	X											X		X	X				X	X
P.ACCESS	X						X	X						X										X		X	X
P.ACCACT								X		X			X												X	X	X
P.INTGTY											X																
P.PROTCT									X											X							
P.CRYPTOGRAPHY															X		X										
P.CRYPTOGRAPHY_VALIDATED															X	X											

A.ACCESS: The TOE has access to all the IT System data it needs to perform its functions.

The OE.INTROP objective ensures the TOE has the needed access.

A.DYNMIC: The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.

A.ASCOPE: The TOE is appropriately scalable to the IT System the TOE monitors.

The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT: The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The OE.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL: The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST: The TOE can only be accessed by authorized users.

The OE.PHYCAL objective provides for physical protection of the TOE against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

T.COMINT: An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

T.COMDIS: An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

T.LOSSOF: An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

T.NOHALT: An unauthorized user may attempt to compromise the continuity of the system's collection and analysis functions by halting execution of the TOE.

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze system data, which includes attempts to halt the TOE. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

T.PRIVIL: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

T.IMPCON: An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

T.INFLUX: An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

> The O.OFLOWS objective counters this threat by requiring that the TOE must handle data storage overflows. OE.ALARMS provides Operational Environment support to send warnings when the audit and/or collected system data is about to be overwritten. OE.PROTECTCOMM provides for secure communications between the TOE and the external server that provides the warnings.

T.FACCNT: Unauthorized attempts to access TOE data or security functions may go undetected.

> The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.SCNCFG: Improper security configuration settings may exist in the IT System the TOE monitors.

> The O.IDSCAN objective counters this threat by requiring a TOE, which contains a scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a scanner.

T.SCNMLC: Users could execute malicious code on an IT System that the TOE monitors which causes modification of the protected IT System data or undermines the IT System security functions.

> The O.IDSCAN objective counters this threat by requiring a TOE, which contains a scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a scanner.

T.SCNVUL: Vulnerabilities may exist in the IT System the TOE monitors.

> The O.IDSCAN objective counters this threat by requiring a TOE, which contains a scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a scanner.

T.FALACT: The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

> The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity. The OE.ALARMS objective provides Operational Environment support mechanisms for alarms to notify responsible personnel of possible intrusions. OE.PROTECTCOMM provides for secure communications between the TOE and the external servers that provide the alarm mechanisms.

T.FALREC: The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

> The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC: The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

> The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.MISUSE: Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a sensor, collect audit and sensor data.

T.INADVE: Inadvertent activity and access may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a sensor, collect audit and sensor data.

T.MISACT: Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a sensor, collect audit and sensor data.

T.ACCIDENTAL_CRYPTO_COMPROMISE: A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.

O.RESIDUAL_INFORMATION objective contributes to addressing this threat by ensuring that cryptographic material in the TOE is not accessible once it is no longer needed. The O.PROTCT objective also addresses this threat by providing TOE self-protection.

T.POOR_TEST: The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.

O.CORRECT_ TSF_OPERATION objective contributes to addressing this threat by providing assurance that the TSF continues to operate as expected in the field.

T.RESIDUAL_DATA: A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.

O.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that cryptographic material in the TOE is not accessible once it is no longer needed.

T.TSF_COMPROMISE: A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).

O.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that cryptographic material is the TOE us not accessible once it is no longer needed. The O.PROTCT objective also addresses this threat by providing TOE self-protection.

P.DETECT: Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, sensor, and scanner data. OE.TIME supports the data collection by providing reliable timestamps for the collected audit, sensor, and scanner data. OE.PROTECTCOMM provides for secure communications between the TOE and the external time server.

P.ANALYZ: Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

The O.IDANLZ objective requires analytical processes are applied to data collected from sensors and scanners.

P.MANAGE: The TOE shall only be managed by authorized users.

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrators follow all provided documentation and maintain the security policy. The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

P.ACCESS: All data collected and produced by the TOE shall only be used for authorized purposes.

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this policy by providing TOE self-protection. O.AUDIT_PROTECTION provides for the protection of the audit data from unauthorized deletion and modification. OE.ALARMS provides Operational Environment support to send warnings when the audit and/or collected system data is about to be overwritten. OE.PROTECTCOMM provides for secure communications between the TOE and the external server that provides the warnings and between the TOE and the external authentication server.

P.ACCACT: Users of the TOE shall be accountable for their actions within the IDS.

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH and OE.XAUTH objectives support this policy by ensuring each user is uniquely identified and authenticated. OE.TIME supports the generation of audit data by providing reliable timestamps. OE.PROTECTCOMM provides for secure communications between the TOE and the external time server and between the TOE and the external authentication server. O.AUDIT_SORT supports the interpretation of the audit records by sorting the data.

P.INTGTY: Data collected and produced by the TOE shall be protected from modification.

The O.INTEGR objective ensures the protection of data from modification.

P.PROTCT: The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

The O.OFLOWS objective implements this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

P.CRYPTOGRAPHY: The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

The O.CRYPTOGRAPHY and O.RESIDUAL_INFORMATION objectives implement this policy by requiring the TOE to implement NIST FIPS 140-1/2 validated cryptographic services to provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE.

P.CRYPTOGRAPHY_VALIDATED: Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

The O.CRYPTOGRAPHY and O.CRYPTOGRAPHY_VALIDATED objectives implement this policy by requiring the TOE to implement NIST FIPS 140-1/2 validated cryptographic services to provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE.

4.2.2 *Rationale for the Security Objectives for the Environment*

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, interoperability requirements on the TOE and for external components that support the TOE objectives. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

5 Extended Components Definition

All of the components defined below have been taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 (IDS System PP), verbatim, except for FIA_UAU_EXT.1 and FPT_TST_EXT.1, which have been modeled on SFRs from Part 2 of the CC Version 3.1 R3 and FCS_BCS_EXT.1, which has been taken from the U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments, Version 1.1, July 25, 2007 (WLAN Access System PP).

The extended components are denoted by adding "_EXT" in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FCS_BCM_EXT.1	Baseline Cryptographic Module
2	FIA_UAU_EXT.1	Timing of authentication
3	FPT_TST_EXT.1	TSF Self Testing
4	IDS_SDC_EXT.1	System Data Collection
5	IDS_ANL_EXT.1	Analyser analysis
6	IDS_RCT_EXT.1	Analyser react
7	IDS_RDR_EXT.1	Restricted Data Review
8	IDS_STG_EXT.1	Guarantee of System Data Availability
9	IDS_STG_EXT.2	Prevention of System data loss

5.1 FCS_BCM_EXT.1 Baseline Cryptographic Module

5.1.1 *Class FCS: Cryptographic support*

See Section 10 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.2 *Family: Baseline Cryptographic Module (FCS_BCM)*

5.1.3 *Family Behavior*

This family defines the standards for the cryptographic modules used by the TSF.

5.1.4 *Management*

The following actions could be considered for the management functions in FMT:

- None

5.1.5 *Audit*

There are no auditable events foreseen.

5.1.6 *Definition*

FCS_BCM_EXT.1 Baseline Cryptographic Module

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_BCM_EXT.1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_EXT.1.2 All cryptographic modules implemented in the TOE

[selection:

Entirely in hardware shall have a minimum overall rating of FIPS PUB 140-2, [assignment: Level],

Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, [assignment: Level] and also meet FIPS PUB 140-2, [assignment: Level] for the following: [assignment: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; Design Assurance; other].

As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, [assignment: Level] for the following: [assignment: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; Design Assurance; other]]

5.1.7 *Rationale*

FCS_BCM_EXT.1 is taken from the U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments, Version 1.1, July 25, 2007. This extended requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.

5.2 FIA_UAU_EXT.1 Timing of authentication

5.2.1 *Class FIA: Identification and authentication*

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.2.2 *Family: User authentication (FIA_UAU)*

5.2.3 *Family Behavior*

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

5.2.4 *Management*

The following actions could be considered for the management functions in FMT:

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

5.2.5 *Audit*

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism
- Basic: All use of the authentication mechanism

5.2.6 *Definition*

FIA_UAU_EXT.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.1.1 The TSF shall allow ***[assignment: list of TSF mediated actions]*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU_EXT.1.2 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

5.2.7 *Rationale*

FIA_UAU_EXT.1 is modeled closely on the standard component FIA_UAU.1: Timing of authentication. FIA_UAU_EXT.1 needed to be defined as an extended component because the functionality of the standard component was extended by adding the text “either by the TSF or by an authentication service in the Operational Environment invoked by the TSF”.

5.3 FPT_TST_EXT.1 TSF Self Testing

5.3.1 *Class FPT: Protection of the TSF*

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.3.2 *Family: TSF self test (FPT_TST)*

5.3.3 *Family Behavior*

See Section 15.14 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.3.4 *Management*

The following actions could be considered for the management functions in FMT:

- management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions;
- management of the time interval if appropriate.

5.3.5 *Audit*

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Execution of the TSF self tests and the results of the tests.

5.3.6 *Definition*

FPT_TST_EXT.1 TSF Self Testing

Hierarchical to: No other components

Dependencies: FCS_COP.1

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests ***[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]*** to demonstrate the correct operation of ***[selection: [assignment: parts of TSF], the TSF].***

FPT _TST_EXT.1.2 The TSF shall run a suite of self-tests tests ***[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]*** to verify the integrity of ***[selection: [assignment: parts of TSF], the TSF].***

FPT _TST_EXT.1.3 Upon detection of a test failure, the cryptographic module shall ***[assignment: actions taken on error condition].***

5.3.7 *Rationale*

FPT_TST _EXT.1 is modeled closely on the standard component FPT_TST.1: TSF Testing. FPT_TST_EXT.1 needed to be defined as an extended component because the standard component does not specify the actions taken on an error condition and all self tests for the TOE are done automatically in FIPS mode. Authorized users can perform an on-demand self test by rebooting the module.

5.4 IDS_SDC_EXT.1 System Data Collection

5.4.1 *Class IDS: Intrusion Detection System*

5.4.2 *Family: System Data Collection (IDS_SDC)*

5.4.3 *Family Behavior*

This family defines the requirements for the TSF to be able to collect information from targeted IT System resources.

5.4.4 *Management*

The following actions could be considered for the management functions in FMT:

- the management (addition, removal, or modification) of specific IDS information that will be obtained from targeted IT System resource(s);
- the management (addition, removal, or modification) of specific targeted IT System resources.

5.4.5 *Audit*

There are no auditable events foreseen.

5.4.6 *Definition*

IDS_SDC_EXT.1 System Data Collection

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC_EXT.1.1 The TSF shall be able to collect the following information from the targeted IT System resource(s): ***[selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities];*** and ***[assignment: other specifically defined events].***

IDS_SDC_EXT.1.2 At a minimum, the TSF shall collect and record the following information

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the Details column of Table 5-2: System Events.

Table 5-2: System Events

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	None
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address
IDS_SDC.1	Start-up and shutdown of audit functions	None
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked, passwords, account policy, parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known, vulnerability

5.4.7 *Rationale*

IDS_SDC_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_SDC_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically System data collection.

5.5 IDS_ANL_EXT.1 Analyser analysis

5.5.1 *Class IDS: Intrusion Detection System*

5.5.2 *Family: Analyser analysis (IDS_ANL)*

5.5.3 *Family Behavior*

This family defines the requirements for the TSF to be able to analyze the IDS data that has been gathered from targeted IT System resources.

5.5.4 *Management*

The following actions could be considered for the management functions in FMT:

- the management (addition, removal, or modification) of specific IDS information that will be obtained from targeted IT System resource(s).

5.5.5 *Audit*

There are no auditable events foreseen.

5.5.6 *Definition*

IDS_ANL_EXT.1 Analyser analysis

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1

IDS_ANL_EXT.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) ***[selection: statistical, signature, integrity]; and***

b) ***[assignment: other analytical functions].***

IDS_ANL_EXT.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and
b) ***[assignment: other security relevant information]***

5.5.7 *Rationale*

IDS_ANL_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_ANL_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the analysis function.

5.6 IDS_RCT_EXT.1 Analyser react

5.6.1 *Class IDS: Intrusion Detection System*

5.6.2 *Family: Analyser react (IDS_RCT)*

5.6.3 *Family Behavior*

This family defines the requirements for the TSF to be able to send an alarm and react when an intrusion is detected.

5.6.4 *Management*

The following actions could be considered for the management functions in FMT:

- the management (addition, removal, or modification) of actions

5.6.5 *Audit*

There are no auditable events foreseen.

5.6.6 *Definition*

IDS_RCT_EXT.1 Analyser react

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1

IDS_RCT_EXT.1.1 The TSF shall send an alarm to ***[assignment: alarm destination]*** and take ***[assignment: appropriate actions]*** when an intrusion is detected.

5.6.7 *Rationale*

IDS_RCT_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_RCT_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the alarm and reaction function.

5.7 IDS_RDR_EXT.1 Restricted Data Review

5.7.1 *Class IDS: Intrusion Detection System*

5.7.2 *Family: Security data review (IDS_RDR)*

5.7.3 *Family Behavior*

This family defines the requirements for data tools that should be available to authorized users to assist in the review of system data.

5.7.4 *Management*

There are no management activities foreseen.

5.7.5 *Audit*

There are no auditable events foreseen.

5.7.6 *Definition*

IDS_RDR_EXT.1 Restricted Data Review

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1

IDS_RDR_EXT.1.1 The TSF shall provide ***[assignment: authorised users]*** with the capability to read ***[assignment: list of system data]*** from the system data.

IDS_RDR_EXT.1.2 The TSF shall provide the system data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3 The TSF shall prohibit all users read access to the system data, except those users that have been granted explicit read-access.

5.7.7 *Rationale*

IDS_RDR_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_RDR_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the restricted data review function.

5.8 IDS_STG_EXT.1 Guarantee of System Data Availability

5.8.1 *Class IDS: Intrusion Detection System*

5.8.2 *Family: System data storage (IDS_STG)*

5.8.3 *Family Behavior*

This family defines the requirements for the TSF to be able to secure system data.

5.8.4 *Management*

There are no management activities foreseen.

5.8.5 *Audit*

There are no auditable events foreseen.

5.8.6 *Definition*

IDS_STG_EXT.1 Guarantee of System Data Availability

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1

IDS_STG_EXT.1.1 The TSF shall protect the stored system data from unauthorized deletion.

IDS_STG_EXT.1.2 The TSF shall protect the stored system data from modification.

IDS_STG_EXT.1.3 The TSF shall ensure that ***[assignment: metric for saving system data]*** system data will be maintained when the following condition occurs: ***[selection: system data storage exhaustion, failure, attack].***

5.8.7 *Rationale*

IDS_STG_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_STG_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the guarantee of System data availability.

5.9 IDS_STG_EXT.2 Prevention of System data loss

5.9.1 *Class IDS: Intrusion Detection System*

5.9.2 *Family: System data storage (IDS_STG)*

5.9.3 *Family Behavior*

This family defines the requirements for the TSF to be able to secure system data.

5.9.4 *Management*

The following actions could be considered for the management functions in FMT:

- the maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure

5.9.5 *Audit*

There are no auditable events foreseen.

5.9.6 *Definition*

IDS_STG_EXT.2 Prevention of System data loss (EXT)

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1

IDS_STG_EXT.2.1 The TSF shall ***[selection: 'ignore system data', 'prevent system data, except those taken by the authorised user with special rights', 'overwrite the oldest stored system data ']*** and send an alarm if the storage capacity has been reached.

5.9.7 *Rationale*

IDS_STG_EXT.2 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_STG_EXT.2 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the prevention of system data loss.

6 Security Requirements

6.1 Security Functional Requirements

Conventions
The following conventions have been applied in this document:

- **Security Functional Requirements** – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., ***[assignment]).***
  - **Selection**: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., ***[selection]***).
  - **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.

Note: Operations already performed in the corresponding Protection Profile are not identified in this Security Target.

- **Application notes** provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

- **Explicitly stated Security Functional Requirements** (i.e., those not found in Part 2 of the CC) are identified "_EXT" in the component name.

The TOE security functional requirements are listed in Table 6-1. All SFRs based on requirements defined in Part 2 of the Common Criteria or the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007, are included. Additional SFRs are also included based on certain SFRs from U.S. Government Protection Profile Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments, Version 1.1, July 25, 2007.

Table 6-1: TOE Security Functional Components

No.	Component	Component Name
1	FAU_GEN.1	Audit data generation
2	FAU_SAR.1	Audit review
3	FAU_SAR.2	Restricted audit review
4	FAU_SAR.3	Selectable audit review

No.	Component	Component Name
5	FAU_SEL.1	Selective audit
6	FAU_STG.2	Guarantees of data availability
7	FAU_STG.4	Prevention of audit data loss
8	FCS_BCM_EXT.1	Baseline Cryptographic Module
9	FCS_CKM.1	Cryptographic key generation
10	FCS_CKM.4	Cryptographic key destruction
11	FCS_COP.1	Cryptographic operation
12	FIA_AFL.1	Authentication failure handling
13	FIA_ATD.1	User attribute definition
14	FIA_SOS.1	Verification of secrets
15	FIA_UAU_EXT.1	Timing of authentication
16	FIA_UID.1	Timing of identification
17	FMT_MOF.1	Management of security functions behavior
18	FMT_MTD.1	Management of TSF data
19	FMT_SMF.1	Specification of Management Functions
20	FMT_SMR.1	Security roles
21	FPT_ITT.1	Basic internal TSF data transfer protection
22	FPT_TST_EXT.1	Self testing
23	FTA_SSL.3	TSF-initiated termination
24	FTA_TAB.1	Default TOE access banners
25	IDS_SDC_EXT.1	System Data Collection
26	IDS_ANL_EXT.1	Analyzer analysis
27	IDS_RCT_EXT.1	Analyzer react
28	IDS_RDR_EXT.1	Restricted Data Review
29	IDS_STG_EXT.1	Guarantee of System Data Availability
30	IDS_STG_EXT.2	Prevention of System data loss

6.1.1 *Class FAU: Security Audit*

6.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the ***[***

- ***basic level of audit for SFRs included in the IDS PP***
- ***not specified level of audit for SFRs not included in the IDS PP]*** and

c) Access to the System and access to the TOE and system data

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 identity, 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 PP/ST, the additional information specified in the Details column of Table 6-2: Auditable Events.

Table 6-2: Auditable Events

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object ID, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FAU_STG.2	None	
FAU_STG.4	Actions taken due to the audit storage failure	
FCS_BCM_EXT.1	None	
FCS_CKM.1	None	
FCS_CKM.4	None	
FCS_COP.1	None	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal).	User identity
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_UAU_EXT.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions	User identity
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_ITT.1	None	
FPT_TST_EXT.1	None	
FTA_SSL.3	Termination of session.	User identity
FTA_TAB.1	None	
IDS_SDC_EXT.1	None	
IDS_ANL_EXT.1	None	
IDS_RCT_EXT.1	None	

Component	Event	Details
IDS_RDR_EXT.1	None	
IDS_STG_EXT.1	None	
IDS_STG_EXT.1	None	

6.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[users with Superuser role and users with access privilege to location node]*** with the capability to read ***[user action logs and system health events, respectively,]*** from the audit records.

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

6.1.1.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

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

6.1.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event.

6.1.1.5 FAU_SEL.1 Selective audit

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type

b) ***[none other]***

6.1.1.6 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to detect unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that ***[the most recent]*** audit records will be maintained when the following conditions occur: ***[audit storage exhaustion]***.

6.1.1.7 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall ***[overwrite the oldest stored audit records]*** and send an alarm if the audit trail storage is full.

6.1.2 *Class FCS: Cryptographic Support*

6.1.2.1 FCS_BCM_EXT.1 Baseline Cryptographic Module

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_BCM_EXT.1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_EXT.1.2 All cryptographic modules implemented in the TOE

[

Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 2 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; and Design Assurance.

]

6.1.2.2 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- ***as provided in TLS version 1.0,***
- ***as provided in SSH version 2, and***
- ***as provided in proprietary Sensor-Server communication protocol listed in Column 1 of Table 6-3***

] and specified cryptographic key sizes [

- ***as provided in TLS version 1.0,***
- ***as provided in SSH version 2, and***
- ***as provided in proprietary Sensor-Server communication protocol listed in Column 2 of Table 6-3***

] that meet the following: ***[***

- ***RFC 2246 for TLS 1.0,***
- ***RFCs 4252 and 4253 for SSH version 2, and***
- ***FIPS 140-2 approved key generation algorithms for proprietary protocol***

].

Table 6-3: Cryptographic Keys

Key Generation Algorithm	Key Size	Cryptographic Operations	Standards
Manual key entry	128 bits (master key)	Mutual authentication between Sensor and Server.	FIPS 140-2 approved
Random generation	128 bits (session key)	Session key is randomly generated by the Server and transported to Sensor AES-CBC encrypted with master key.	FIPS 140-2 approved
HMAC-SHA-1 using session key as secret	128 bits (encryption key) and 160 bits (authentication key)	Message encryption (AES-CBC) and authentication (HMAC-SHA-1) between Sensor and Server.	FIPS 140-2 approved

6.1.2.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[key deletion (key file deletion for persistent keys and key memory freeing for ephemeral keys)]*** that meets the following: **[*FIPS 140-2 key deletion standards].***

6.1.2.4 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform ***[***

- ***cryptographic operations for communications between the Server and the Console as provided in TLS version 1.0,***
- ***cryptographic operations to support remote CLI access and to perform secure file copy as provided in SSH version 2, and***
- ***cryptographic operations as provided in proprietary Sensor-Server communication protocol listed in Column 3 of Table 6-3***

] in accordance with a specified cryptographic algorithm ***[***

- ***as provided in TLS version 1.0,***
- ***as provided in SSH version 2, and***
- ***HMAC-SHA-1 and AES-CBC in proprietary Sensor-Server communication protocol***

] and cryptographic key sizes ***[***

- ***as provided in TLS version 1.0,***

- ***as provided in SSH version 2, and***
- ***as provided in proprietary Sensor-Server communication protocol listed in Column 2 of Table 6-3***

] that meet the following: ***[***

- ***RFC 2246 for TLS 1.0,***
- ***RFCs 4252 and 4253 for SSH version 2, and***
- ***FIPS 140-2 approved algorithms for proprietary protocol***

].

6.1.3 *Class FIA: Identification and Authentication*

6.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***[an administrator configurable positive integer within (the range of 3 through 10)]*** unsuccessful authentication attempts occur related to ***[unsuccessful logins in the administrator configurable time period (range of 5 through 30 minutes)].***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[surpassed]***, the TSF shall ***[prevent the user from accessing the system for the administrator defined time period for the user's role (range of 5 through 30 minutes)].***

Application Note: The FIA_AFL.1 included in the TOE refers to the lockout of local TOE Administrators after a configurable number of unsuccessful login attempts. This SFR has been added to reflect the security functionality of the TOE and has been taken directly from Part 2 of CC 3.1 R3.
The version of FIA_AFL.1 that was excluded from the IDS System PP was a requirement to detect attempts to access the TOE by untrusted external IT products.
The version of FIA_AFL.1 included in the WLAN Access System PP applies to remote administrator login and does not apply to the local login of the TOE.

6.1.3.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity (User name);
b) Authentication data (Password);
c) Authorizations (Role and Location of privilege) ; and
d) ***[***

   - ***Email address***
   - ***Session timeout setting***
   - ***LDAP authentication option***
   - ***RADIUS authentication option***
   - ***Password expiry setting***

   ].

6.1.3.3 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet

[The following password policy:

- ***Number of Minimum characters required (numeric value 4 through 15) (default: 6)***
- ***Numeric characters required? (yes/no) (default: No)***
- ***Special characters required? (yes/no) (default: No)***

]

6.1.3.4 FIA_UAU_EXT.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.1.1 The TSF shall allow ***[selecting between certificate based authentication or username/password based authentication, when either one is allowed]*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU_EXT.1.2 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user

6.1.3.5 FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow ***[selecting between certificate based authentication or username/password based authentication, when either one is allowed]*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 *Class FMT: Security Management*

6.1.4.1 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

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the System data collection, analysis and reaction to authorized System administrators.

6.1.4.2 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[operations as specified in Table 6-4]*** the ***[TSF data as specified in Table 6-4]*** to ***[user security role as specified in Table 6-4].***

Table 6-4: Management of TSF data

Operation	TSF Data	TOE User Roles			
		Superuser	Administrator	Operator	Viewer
User account management					
Set or modify identification and authentication option (uname/password only, certificate only, two-factor or either)	User Accounts	Yes	No	No	No
Add and delete users	User Accounts	Yes	No	No	No
View and modify properties of any user (User Management screens)	User Accounts	Yes	No	No	No
Define password strength, account lockout policy, maximum concurrent sessions for all users	User Accounts	Yes	No	No	No
View and modify User Preferences (email, password, session timeout)	User Accounts	Yes (self only)	Yes (self only)	Yes (self only)	Yes (self only)

User actions audit					
Download user actions audit log	Audit Data	Yes	No	No	No
Modify user actions audit lifetime	Audit Data	Yes	No	No	No
TOE behavior					
Modify TOE behavior (all settings under Configuration tab other than User Management, Logs, Login configuration)	TOE Behavior	Yes	Yes	No	No
Events, devices, and locations					
View generated events	Events	Yes	Yes	Yes	Yes
Modify and delete generated events	Events	Yes	Yes	Yes	No
View devices	Devices	Yes	Yes	Yes	Yes
Add, delete, and modify devices (APs, Clients, Sensors)	Devices	Yes	Yes	Yes	No
View locations	Locations	Yes	Yes	Yes	Yes
Add, delete, and modify locations	Locations	Yes	Yes	Yes	No
Calibrate location tracking	Locations	Yes	Yes	Yes	No
Reports					
Add, delete, modify Shared Report	Reports	Yes (all)	Yes (only self created)	Yes (only self created)	No
Generate Shared Report	Reports	Yes	Yes	Yes	Yes
Schedule Shared Report	Reports	Yes	Yes	Yes	No
Add, delete, modify, generate, schedule My Report	Reports	Yes (only self created)	Yes (only self created)	Yes (only self created)	No
Software Upgrade					
Upgrade TOE	TOE Software	Yes	No	No	No

Note: Access to TOE behavior, events, devices, locations, and reports is also restricted by location privilege of the user (see Sections 7.1.3.1 and 7.1.6.4).

6.1.4.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

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

- ***Set or modify user identification and authentication option***
  - ***Add, delete, modify, and manage users***
  - ***Download audit records***

- ***Modify TOE behavior***
- ***View, modify and delete events***
- ***View, modify and delete devices***
- ***View, modify and delete locations***
- ***Add, delete, modify, generate and schedule reports***
- ***Facilitate upgrading the TOE software***

].

Application Note: FMT_SMF.1 is not included in the IDS System PP; however, it needed to be included to satisfy the dependencies of the SFRs FMT_MOF.1 and FMT_MTD.1.

6.1.4.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles ***[***

- ***Superuser***
- ***Administrator***
- ***Operator***
- ***Viewer***

].

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

6.1.5 *Class FPT: Protection of the TSF*

6.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT.1.1 **Refinement:** The TSF shall protect TSF data from ***[disclosure, modification]*** when it is transmitted between:

- **Server and Sensors via vendor proprietary communication protocol**
- **Server and the Console via HTTPS/TLS version 1.0**

Application Note: The communications between TOE components are FIPS compliant.

Application Note: FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.2, have been excluded from the IDS System PP and FPT_ITT.1 has been added to the IDS System PP through the precedence of PD-0097.

6.1.5.2 FPT_TST_EXT.1 TSF Self Testing

Hierarchical to: No other components

Dependencies: FCS_COP.1

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests ***[during start-up, at the conditions [on generation of new public/private key pair and request for generation of new random number]]*** to demonstrate the correct operation of ***[the cryptographic module portion of the TSF].***

FPT _TST_EXT.1.2 The TSF shall run a suite of self-tests ***[during start-up]*** to verify the integrity of ***[the cryptographic module portion of the TSF].***

FPT _TST_EXT.1.3 Upon detection of a test failure, the cryptographic module shall ***[enter error state]***.

6.1.6 *Class FTA: TOE Access*

6.1.6.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after an ***[administrator configured timeout period of session inactivity].***

6.1.6.2 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.1.7 *Class IDS: IDS Component Requirements*

6.1.7.1 IDS_SDC_EXT.1 System Data Collection

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC_EXT.1.1 The TSF shall be able to collect the following information from the targeted IT System resource(s): ***[network traffic];*** and ***[none].***

IDS_SDC_EXT.1.2 At a minimum, the TSF shall collect and record the following information

c) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
d) The additional information specified in the Details column of Table 5-2: System Events.

Table 6-5: System Events

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

6.1.7.2 IDS_ANL_EXT.1 Analyser analysis

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1 System Data Collection

Dependencies: IDS_SDC_EXP.1

IDS_ANL_EXT.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) ***[statistical, signature]; and***
b) ***[auto-classification of devices, wireless policy check].***

IDS_ANL_EXT.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and
b) ***[Location tracking information]***

6.1.7.3 IDS_RCT_EXT.1 Analyser react (EXT)

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1 System Data Collection

IDS_RCT_EXT.1.1 The TSF shall send an alarm to ***[administrator]*** and take ***[automatic prevention action]*** when an intrusion is detected.

6.1.7.4 IDS_RDR_EXT.1 Restricted Data Review (EXT)

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1 System Data Collection

IDS_RDR_EXT.1.1 The TSF shall provide ***[authorized users with location privilege]*** with the capability to read ***[events, devices, location information, reports, forensics, local policies]*** from the system data.

IDS_RDR_EXT.1.2 The TSF shall provide the system data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3 The TSF shall prohibit all users read access to the system data, except those users that have been granted explicit read-access.

6.1.7.5 IDS_STG_EXT.1 Guarantee of System Data Availability

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1

IDS_STG_EXT.1.1 The TSF shall protect the stored system data from unauthorized deletion.

IDS_STG_EXT.1.2 The TSF shall protect the stored system data from modification.

IDS_STG_EXT.1.3 The TSF shall ensure that ***[most recent]*** system data will be maintained when the following condition occurs: ***[system data storage exhaustion].***

6.1.7.6 IDS_STG_EXT.2 Prevention of System data loss

Hierarchical to: No other components

Dependencies: IDS_SDC_EXP.1 System Data Collection

IDS_STG_EXT.2.1 The TSF shall ***[overwrite the oldest stored system data]*** and send an alarm if the storage capacity has been reached.

6.2 Security Assurance Requirements for the TOE

This Section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL *2* augmented with ALC_FLR.2*.* None of the assurance components are refined. Table 6-6 summarizes the components.

Table 6-6: EAL2+ Assurance Components

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Architectural Design with Domain Separation and non-bypassability
	ADV_FSP.2	Security enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance documents	AGD_OPE.1	Operational User guidance

Assurance Class	Assurance Components	
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw Reporting Procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability Analysis

6.2.1 *Class ADV: Development*

6.2.1.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1 4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.2 ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.1.3 ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.2 *Class AGD: Guidance documents*

6.2.2.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.11D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies

Developer action elements:

AGD_PRE.11D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.3 *Class ALC: Life-cycle support*

6.2.3.1 ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.21D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.23C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.2 ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.3 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.4 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C	The flaw remediation procedures shall describe a means by which the developer receives from TOE users' reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6C	The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.2.7C	The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8C	The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4 *Class ATE: Tests*

6.2.4.1 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.2 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:
ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.3 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:
ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:
ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:
ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall execute a sample
ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.5 *Class AVA: Vulnerability assessment*

6.2.5.1 AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:
AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:
AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.12.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.3 Security Requirements Rationale

6.3.1 *Dependencies Satisfied*

Table 6-7 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 6-7: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	Environment *
2	FAU_SAR.1	Audit review	FAU_GEN.1	1
3	FAU_SAR.2	Restricted audit review	FAU_SAR.1	2
4	FAU_SAR.3	Selectable audit review	FAU_SAR.1	2
5	FAU_SEL.1	Selective audit	FAU_GEN.1	1
			FMT_MTD.1	18
6	FAU_STG.2	Guarantees of data availability	FAU_GEN.1	1
7	FAU_STG.4	Prevention of audit data loss	FAU_STG.1	6 (H)
8	FCS_BCM_EXT.1	Baseline Cryptographic Module	None	N/A
9	FCS_CKM.1	Cryptographic key generation	FCS_CKM.2 or FCS_COP.1	11
			FCS_CKM.4	10
10	FCS_CKM.4	Cryptographic key destruction	FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1	9
11	FCS_COP.1	Cryptographic operation	FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1	9
			FCS_CKM.4	10
12	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	15
13	FIA_ATD.1	User attribute definition	None	N/A
14	FIA_SOS.1	Verification of secrets	None	N/A
15	FIA_UAU_EXT.1	Timing of authentication	FIA_UID.1	16
16	FIA_UID.1	Timing of identification	None	N/A
17	FMT_MOF.1	Management of security functions behavior	FMT_SMF.1	19
			FMT_SMR.1	20
18	FMT_MTD.1	Management of TSF data	FMT_SMF.1	19
19	FMT_SMF.1	Specification of Management Functions	None	N/A
20	FMT_SMR.1	Security roles	FIA_UID.1	15
21	FPT_ITT.1	Basic internal TSF data transfer protection	None	N/A
22	FPT_TST_EXT.1	Self testing	FCS_COP.1	11
23	FTA_SSL.3	TSF-initiated termination	None	N/A

Item	SFR ID	SFR Title	Dependencies	Item Reference
24	FTA_TAB.1	Default TOE access banners	None	N/A
25	IDS_SDC_EXT.1	System Data Collection	FPT_STM.1	Environment *
26	IDS_ANL_EXT.1	Analyzer analysis	IDS_SDC_EXT.1	26
27	IDS_RCT_EXT.1	Analyzer react	IDS_SDC_EXT.1	26
28	IDS_RDR_EXT.1	Restricted Data Review	IDS_SDC_EXT.1	26
29	IDS_STG_EXT.1	Guarantee of System Data Availability	IDS_SDC_EXT.1	26
30	IDS_STG_EXT.2	Prevention of System data loss	IDS_SDC_EXT.1	26

* Reliable time is satisfied by the external time server in the Operational Environment (OE.TIME)

6.3.2 *Functional Requirements*

The following table traces each SFR back to the security objectives for the TOE.

Table 6-8: Requirements vs. Objectives Mapping

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.AUDIT_PROTECTION	O.AUDIT_SORT	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.RESIDUAL_INFORMATION	O.CORRECT_TSF_OPERATION
FAU_GEN.1										X								
FAU_SAR.1						X												
FAU_SAR.2							X	X										
FAU_SAR.3						X								X				
FAU_SEL.1						X				X								
FAU_STG.2	X						X	X	X		X		X					
FAU_STG.4									X	X			X					
FCS_BCM_EXT.1															X	X		
FCS_CKM.1															X	X		
FCS_CKM.4															X	X	X	
FCS_COP.1															X	X		
FIA_AFL.1								X										
FIA_ATD.1								X										
FIA_SOS.1								X										
FIA_UAU_EXT.1							X	X										
FIA_UID.1							X	X										
FMT_MOF.1	X						X	X										
FMT_MTD.1	X						X	X			X							
FMT_SMF.1	X						X	X			X							
FMT_SMR.1								X										
FPT_ITT.1											X	X						

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.AUDIT_PROTECTION	O.AUDIT_SORT	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.RESIDUAL_INFORMATION	O.CORRECT_TSF_OPERATION
FPT_TST_EXT.1																		X
FTA_SSL.3								X										
FTA_TAB.1							X											
IDS_SDC_EXT.1		X	X															
IDS_ANL_EXT.1				X														
IDS_RCT_EXT.1					X													
IDS_RDR_EXT.1						X	X	X										
IDS_STG_EXT.1	X						X	X	X		X							
IDS_STG_EXT.2									X									
ADV_ARC.1	X					X		X		X	X							

The following discussion provides detailed evidence of coverage for each security objective:

O.PROTCT: The TOE must protect itself from unauthorized modifications and access to its functions and data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. The TOE is required to provide the ability to restrict modifying the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data [FMT_SMF.1, FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.IDSCAN: The scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

A TOE containing a scanner is required to collect and store static configuration information from an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC_EXT.1].

O.IDSENS: The sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

A TOE containing a sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity by the assets of an IT System. These events must be defined in the ST [IDS_SDC_EXT.1].

O.IDANLZ: The analyzer must accept data from IDS sensors or IDS scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

> The analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL_EXT.1].

O.RESPON: The TOE must respond appropriately to analytical conclusions.

> The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT_EXT.1].

O.EADMIN: The TOE must include a set of functions that allow effective management of its functions and data.

> The TOE must provide the ability to review and manage the audit trail of the system [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The TOE must provide the ability for authorized administrators to view all system data collected and produced [IDS_RDR_EXT.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data.

> The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the review of system data to those granted with explicit read-access [IDS_RDR_EXT.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion [IDS_STG_EXT.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU_EXT.1]. The TOE is required to provide the ability to restrict modifying the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data [FMT_SMF.1, FMT_MTD.1]. The TOE is required to present a warning banner when a user attempts to login to the TOE [FTA_TAB.1].

O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

> The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the review of system data to those granted with explicit read-access [IDS_RDR_EXT.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU_EXT.1]. The TOE is required to provide the ability to restrict modifying the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data

[FMT_SMF.1, FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1]. [FIA_AFL.1] ensures that the TOE can protect itself and its users from brute force attacks on their authentication credentials. [FTA_SSL.3] ensures that inactive user and administrative sessions are dropped. The TOE enforces a password policy for users authenticated by the TOE [FIA_SOS.1]

O.OFLOWS: The TOE must appropriately handle potential audit and system data storage overflows.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event its audit trail is full [FAU_STG.4]. The TOE is required to protect the system data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. The TOE must prevent the loss of audit data in the event its audit trail is full [IDS_STG_EXT.2].

O.AUDITS: The TOE must record audit records for data accesses and use of the system functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event that its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1].

O.INTEGR: The TOE must ensure the integrity of all audit and system data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion [IDS_STG_EXT.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data [FMT_SMF.1, FMT_MTD.1]. The TOE must protect the collected data from modification and ensure its integrity when the data is transmitted to another part of the TOE [FPT_ITT.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1].

O.EXPORT: When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the system data.

The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another TOE component [FPT_ITT.1].

O.AUDIT_PROTECTION: The TOE must provide the capability to protect audit information.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must also prevent the loss of audit data in the event that its audit trail is full [FAU_STG.4].

O.AUDIT _SORT: The TOE must provide the capability to sort the audit information.

The TOE is required to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event [FAU_SAR.3].

O.CRYPTOGRAPHY: The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.

TOE must provide baseline cryptographic services using FIPS PUB 140-2 compliant modules implemented in software [FCS_BCM_EXT.1]. The TOE must address the generation of cryptographic keys [FCS_CKM.1] and destruction of cryptographic keys [FCS_CKM.4]. The TOE must perform data encryption and decryption, cryptographic data integrity protection, cryptographic authentication, and random number generation [FCS_COP.1].

O.CRYPTOGRAPHY_VALIDATED: The TOE will use NIST FIPS 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.

TOE must provide baseline cryptographic services using FIPS PUB 140-2 compliant modules implemented in software [FCS_BCM_EXT.1]. The TOE must address the generation of cryptographic keys [FCS_CKM.1] and destruction of cryptographic keys [FCS_CKM.4]. The TOE must perform data encryption and decryption, cryptographic data integrity protection, cryptographic authentication, and random number generation [FCS_COP.1].

O.RESIDUAL_ INFORMATION: The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.

TOE must properly destroy cryptographic keys when they are no longer needed for cryptographic operations [FCS_CKM.4].

O.CORRECT_ TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.

TOE must perform self tests to ensure integrity and proper operation of cryptographic modules [FPT_TST_EXT.1].

6.3.3 *Assurance Rationale*

EAL 2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL *2*, the TOE will have incurred a search for obvious flaws to support its introduction to the non-hostile environment.

7 TOE Summary Specification

7.1 IT Security Functions

Section 7 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.8 Logical Scope of the TOE. The following sub-sections describe how the TOE meets each SFR listed in Section 5.9.7.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Function	Security Functions	SFRs
Security Audit	AU-1 Audit Generation	FAU_GEN.1
	AU-2 Audit Review	FAU_SAR.1 FAU_SAR2 FAU_SAR3
	AU-3 Selective Audit Review	FAU_SEL.1
	AU-4 Audit Data Availability	FAU_STG.2 FAU_STG.4
User Identification and Authentication	IA-1 Authentication and Identification	FIA_UAU_EXT.1 FIA_UID.1
	IA-2 User Security Attributes	FIA_ATD.1 FIA_AFL.1 FIA_SOS.1
Security Management	SM-1 Management Functions and User Roles	FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1
Protection of Security Functions	PT-1 Internal Data Transfer Protection	FPT_ITT.1
	PT-2 Self Tests	FTP_TST_EXT.1
TOE Access	TA-1 Session Termination	FTA_SSL.3
	TA-2 Access Banner	FTA_TAB.1
IDS Component Requirements	IDS-1 System Data Collection	IDS_SDC_EXT.1
	IDS-2 Analyser Analysis	IDS_ANL_EXT.1
	IDS-3 Analyser React	IDS_RCT_EXT.1
	IDS-4 Restricted Data Review	IDS_RDR_EXT.1

Security Function	Security Functions	SFRs
	IDS-5 System Data Availability	IDS_STG_EXT.1 and IDS_STG_EXT.2
Cryptographic Support	CS-1 Cryptographic Keys and Operations	FCS_BCM_EXT.1 FCS_CKM.1 FCS_CKM.4 FCS_COP.1

7.1.1 *Security Audit Functions*

7.1.1.1 AU-1: Audit Generation

(FAU_GEN.1)

FAU_GEN.1 describes the auditing capabilities of the TOE. The TOE collects audit data and provides interface for authorized administrators to review the generated audit records. The following events are audited by the TOE:

a) Start-up and shutdown of the audit functions
b) Access to the system
c) Access to the TOE and system data
d) Viewing of the audit records
e) Unsuccessful attempts to view the audit records
f) All modification to the audit configuration that occurs during collection
g) Actions taken due to an audit storage failure
h) All identification and authentication attempts, including the user identity and location (IP address of host) from where authentication was attempted
i) All modification to the behavior of the TSF such as modifications to event generation and notification, modifications to operating policies, modifications to location tracking parameters, and modifications to reports.
j) All modifications to TSF data values such as event data, monitored device data, and location hierarchy data.
k) Creation, deletion, and modification of user accounts
l) System health audit events

The Server logs read-only auditing information for user activity in the audit log, which can be downloaded as TSV file from the Configuration menu in the Console (available only to Superuser role) and viewed using text editor. Downloading the audit file is the only way to review the user activity audit, i.e., there isn’t a GUI interface to directly read the audit log. When the Superuser downloads the audit file, an audit entry for the downloading activity is generated and stored in the audit log.

The TOE webserver directly checks GUI user action audit information into the TOE database. So, as long as the database server is running, audit recording is operational. Database server automatically starts when TOE powers up/booted up. When TOE starts up, administrator can ensure that the database server is running using “get status" CLI command. Thereafter, database server can be stopped and started on demand from the CLI using “set dbserver” command. Audit record is created for each such user action of stopping and starting the database server (and hence starting and stopping of audit). Note aside that if database server stops, the TOE in fact does not allow any user action on the TOE GUI.

The Server also logs system health audit events, which can be viewed in the Events menu of the Console.

The Sensor, having no administrative GUI, does not record information to the audit log. The Sensor only has command line interface (CLI) for basic installation and troubleshooting functions. The Sensor cannot operate without being first connected to the Server.

The following fields are recorded for each user action audit event in the audit log table:

- **Date and time**: The date and time that the audit record was generated.
- **User**: The login name of the user whose action triggered the audit event, along with the role of the user and the IP address of the host from where the user obtained access to the system.
- **Module**: The interface from where the user action was performed such as server GUI or server CLI.
- **Type**: The type of audit event. The possible types are: System Access, Devices, Events, Reports, Location Tree, Local Settings, Global Settings, Start/Stop Functions and Others.
- **Status**: The status indicates whether the particular record pertains to success or failure of the action.
- **Message**: The message describing action performed.

The following fields are recorded for each system health audit event in the audit log table:

- **Date and time**: The date and time that the audit record was generated.
- **Subsystem:** The object that the event pertains to.
- **Message**: The message describing the event.
- **Severity:** Severity level of the event.
- **Location**: Location of event.

AU-1: Audit Generation optionally relies on the Operational Environment to supply reliable timestamps for the audit records. (OE.TIME). AU-1 optionally relies on syslog server, email server or SNMP server in the Operational Environment if external logging is configured in the TOE. AU-1 also optionally relies on the Operational Environment to provide secure communications between the TOE and external syslog/email/SNMP servers. (OE.PROTECTCOMM).

7.1.1.2 AU-2: Audit Review

(FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

FAU_SAR.* describes audit review capabilities of the TOE. The TOE makes user action audit data available for download as TSV file. The authorized administrator can download the audit data file and view the downloaded file using a text editor. Examples of text editors which can be used to view the downloaded audit file are Microsoft Excel, WordPad, notepad etc. In the downloaded audit file, one audit record is presented per row and each row is divided into different columns such as date and time, module, host address, role, login name, type, status and message for ease of interpretation of audit data.

At the time of downloading the user action audit file from the TOE, the superuser can optionally specify a sorting criterion. The sorting criterion specifies the column in the TSV file on which the audit records should be sorted in the downloaded file. If no specific sorting parameter is selected, the audit records in the TSV file are sorted on date and time column by default.

When the downloaded audit file is opened using a text editor in the environment, the additional searching and sorting features of the text editor can also be availed.

The system health audit data (system health events) can be viewed in the Events → System menu of the Console in tabular form. This view allows audit records to be sorted based on event ID, severity level, date and time, event category, and event message. It also allows searching on various fields in the audit records such as even ID, severity level, date and time, event status, text string in event message etc.

The user action audit data is available for download to only Superuser. The system health audit events can be viewed by all authorized users who have privilege at a location where the system health event is tagged. The system health events can also be optionally sent to administrator via email. They can also be optionally sent as SNMP traps or syslog events.

AU-2: Audit Review relies on the Operational Environment to supply text editor to view the downloaded audit file and the OS for access control to the downloaded file. AU-2 relies on the Operational Environment to supply properly configured Web Browser to host the Console. AU-2 optionally relies on syslog server, email server or SNMP server in the Operational Environment if external logging is configured in the TOE. AU-2 also optionally relies on the Operational Environment to provide secure communications between the TOE and external syslog/email/SNMP servers.

7.1.1.3 AU-3: Selective Audit Review

(FAU_SEL.1)

FAU_SEL.1 describes selective audit review capabilities of the TOE. The system health events in the TOE can be included or excluded in the audit log based upon type of event. For this, the administrator chooses Configuration -> Events → Configuration → System menu option. In this menu option, all system health events are listed under Sensor and Server tabs. For any of these events, the administrator can check/uncheck in the Display column to enable/disable generation of that specific event.

At the time of downloading the user action audit file from the TOE, the superuser can optionally specify a single type of audit logs which he wants to download. When the type selection is made, the audit logs pertaining to only that type are included in the downloaded TSV file. The type can be any one of: System Access, Devices, Events, Reports, Location Tree, Local Settings, Global Settings, Start/Stop Functions, Others. If no type selection is made, the audit logs pertaining to all types are downloaded by default.

AU-3: Selective Audit Review relies on the Operational Environment to supply properly configured Web Browser for accessing the Console.

7.1.1.4 AU-4: Audit Data Availability

(FAU_STG.2, FAU_STG.4)

FAU_STG.* describes guarantees on availability of audit data. The TOE stores audit records in database. Authorized administrator can cause user action audit records to be deleted only through configuration of lifetime for which audit records are to be stored. Other than that, authorized administrator has read only (download only) access to user action audit records. TOE ensures that the most recent user action audit records that have not yet exceeded their lifetime will be maintained in case of audit storage exhaustion.

The size of user action audit trail is limited by configurable lifetime. Once the lifetime of audit record expires, the corresponding audit record is deleted. The limitation on audit storage capacity comes from the occupancy of the hard disk. If the hard disk occupancy crosses safe limits, an alarm is generated for the administrator to act on it and ensure that the disk storage does not reach full capacity.

Authorized administrator can cause system health events to be deleted via right click -> Delete option. The administrator needs to have at least Operator role access at a location for event deletion to succeed. When the authorized administrator performs any action on the event (delete, acknowledge etc.), such action is recorded in the user action audit log.

The size of system health events trail is limited by auto deletion settings which specify maximum number of system events to be stored and maximum lifetime for which event will be stored. When the total number of system events exceed the maximum number setting, oldest system events are deleted even if their lifetimes may not expired. This ensures that most recent audit events are still maintained. Whenever auto-deletion is performed, event is generated summarizing the auto-deletion action.

The TOE also provides automatic periodic database backup feature which ensures that the past system data can be retrieved whenever desired.

AU-4: Audit Data Availability relies on Operational Environment to supply properly configured Web Browser for accessing the Console. AU-4 optionally relies on external servers to securely store backed up database. It also optionally relies on the Operational Environment to provide secure communication path between the TOE and the external backup servers.

7.1.2 *User Identification and Authentication Functions*

7.1.2.1 IA-1: Timing of Authentication and Identification

(FIA_UAU_EXT.1, FIA_UID.1)

FIA_UAU_EXT.1 and FIA_UID.1 describe allowing certain actions on behalf of the user to be performed before user is authenticated, but requires user to authenticate for performing any actions on the TOE. The TOE pops up login screen for on the management console when unauthenticated user attempts to access the TOE. In case where either of the certificate based authentication or the username/password based authentication is allowed, the user can select between the two options without having to authenticate or identify himself.

Each individual must be successfully identified and authenticated before access is allowed to the TOE. For this, the user accesses the TOE Console over HTTPS over the network. Superuser is required to set one of the following options for user identification and authentication. The option set by the Superuser applies to all users. The Superuser can also modify this setting during operation. In the following description, client certificate-based authentication is representatively referred to as CAC authentication, though any type of client certificate can be used consistent with the certificate authority configured in the TOE. The options are:

1) Username/password only: In this option, user identification and authentication are performed natively by the TOE via username and password. The TSF uses the security attributes of the user account described in Section 7.1.2.2, which are stored in the TOE. When identification and authentication data is entered, the TOE attempts to identify the applicable user account from the provided identity and if a match is found, the password provided is compared against that stored with the user account information. If a user account cannot be associated with the provided identity or the provided password does not match that stored with the user account information, identification and authentication will fail. No actions are allowed, other than entry of identification and authentication data, until successful identification and authentication.

Optionally, the TOE can be configured to use an external LDAP authentication service for identification and authentication of one or more users. That is, if the user password is not natively configured in the TOE, the TSF accesses the external LDAP authentication service as configured. Any LDAP aware directory server which supports LDAPv3 (RFCs 2251-2256, 2829-2830) can be used in "Simple Authentication" configuration. For LDAP authentication, an LDAP authentication object must be created to provide user authentication services by specifying the following:

- settings for the connection to the LDAP server
- LDAP directory context
- search criteria used to retrieve user data from the LDAP server
- authentication data for access to the LDAP server
- default role and location privilege that will be assigned to LDAP authenticated user, if such information is not present in LDAP

Optionally, the TOE can be configured to use an external RADIUS authentication service (RFCs 2865, 2866) for identification and authentication of one or more users. That is, if the user password is not natively configured in the TOE, the TSF accesses the RADIUS authentication service as configured. RADIUS authentication can be simple password based or challenge-response based or both (as configured at the RADIUS server) for a given user (with a given username). Authorization is based on vendor-specific attributes configured at the RADIUS server for a user or defaults configured in the Server. A RADIUS authentication object must be created to provide user authentication services by specifying the following:

- settings for connection to the RADIUS server
- default values for vendor specific attributes to be used if not available from RADIUS server for a user: CLI access allowed/disallowed, Console access allowed/disallowed, role and location privilege.

2) CAC only: In this option, user identification and authentication are performed using CAC. The user has to insert CAC in smart card reader attached to the computer from where TOE Console is accessed. If CAC authentication succeeds, the TSF obtains the user identity from

CAC. The TSF then retrieves the user attributes (user role and location privilege) either natively from the TOE or from the external LDAP service. If CAC authentication fails or information on user is not available natively in the TOE as well as in the external LDAP authentication service, no actions are allowed other than re-authentication attempt. When this option is set, the Superuser has to configure appropriate CA certificate in the TOE. The client certificate based authentication is performed by the web server in the TOE using standard TLS version 1.0 procedure.

3) Two-factor authentication: In this option, both CAC and password are required for user identification and authentication. The user has to insert CAC in smart card reader attached to the computer from where TOE Console is accessed. If CAC authentication succeeds, the TSF obtains the user identity from CAC and prompts the user for password. The TSF validates the password entered by the user against the password stored either natively in the TOE, in the external LDAP server or in the external RADIUS server. If the password matches, user role and location privilege information are also retrieved. If CAC authentication fails or if user entered password is not verified, no actions are allowed other than re-authentication attempt. When this option is set, the Superuser has to configure appropriate CA certificate in the TOE. The client certificate based authentication is performed by the web server in the TOE using standard TLS version 1.0 procedure.

4) Either CAC or username/password: In this option, user identification and authentication is permitted either using CAC only option or using username/password option. This option is provided for sake of backward compatibility in those deployments which may not have fully migrated to CAC.

Note: LDAP server and RADIUS server require TCP/IP access from the TOE to the authentication server.

IA1: User Identification and Authentication optionally relies on the Operational Environment to provide an external authentication service if LDAP/RADIUS authentication is configured or if client certificate is required for user identification and authentication. (OE.XAUTH). In that case, IA-2 also relies on the Operational Environment to provide secure communications between the TOE and the authentication server. (OE.PROTECTCOMM).

7.1.2.2 IA-2: User Security Attributes

(FIA_ATD.1, FIA_AFL.1, FIA_SOS.1)

User account information contains the following security attributes:

- **User identity (User name)**
- **Password (applicable only for authentication options which use password)**
- **Role**
- **Location of privilege**
- **Email address**
- **Session timeout setting**
- **LDAP authentication option**
- **RADIUS authentication option**
- **Password expiry setting (applicable only for native authentication in TOE using username/password)**

These attributes are configured in the TOE when Superuser creates a new account. In case of authentication options that use external LDAP/RADIUS service, user account is created in the TOE upon first successful login by the user, based on information obtained from LDAP/RADIUS. The LDAP may also provide role, location of privilege and email address attributes for the user account and RADIUS may provide role and location privilege attributes. RADIUS does not provide email attribute. If any of these attributes are not obtained from LDAP/RADIUS, the TOE assigns Superuser configured default values to these attributes.

Attributes of other users stored in the TOE are modifiable only by the Superuser. In case, email attribute is received from LDAP, Superuser cannot modify it for other users.

Any user can modify his own password (stored in TOE for the case of native username/password authentication option), email address (if not provided by LDAP) and session timeout setting.

There are three more settings, namely “password policy” (applicable only for native authentication using username/password), “account locking” (applicable only for native/LDAP/RADIUS authentication using username/password or two-factor authentication) and “concurrent login sessions”, which are accessible only to Superuser. The password policy specifies minimum required strength for the password in terms of number of minimum characters required (configurable value 4 through 15) (default: 6), whether presence of at least one numeric character is required (Yes/No)(default: No) and whether at least one special character is required (Yes/No)(default: No). There is only one password policy allowed and it applies to all users (of all roles). Change of password policy does not affect currently present passwords.

The “account locking” specifies temporary account lockout behavior after repeated authentication failures. There can be different account lockout setting for each role. The Superuser can specify for each role the temporary account lockout duration (configurable value 5 minutes through 30 Minutes, default: 15 Minutes) and the number of failed attempts (configurable value 3 attempts to 10 attempts, default: 3 attempts) in a time period (configurable value 5 minutes through 30 minutes, default: 10 Minutes) which trigger the lockout.

The “concurrent login sessions” specified maximum number of login sessions user can establish with Console. This maximum number is same for all users of all roles.

IA-2: User Security Attributes relies on the Operational Environment to supply properly configured Web Browser for accessing the Console.

7.1.3 *Security Management Functions*

7.1.3.1 SM-1: Management Functions and User Roles

(FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1)

The TOE requires user authentication before any actions (other than entry of identification and authentication data and password reset) can be performed through the TOE interfaces. All users of the TOE have access to TSF data and management functions and therefore are considered administrators for the purposes of this evaluation. The terms “TOE user”, “TOE administrator" and "authorized administrator" are used in this ST to refer collectively to all authorized TOE users.

There are four roles defined for users: Superuser, Administrator, Operator and Viewer. There can be only one role (from the above list) for any TOE user. There can be one or more users of any given role. Access to TSF data and management functions is restricted by a user's assigned role as specified in FMT_MTD.1 (see Section 6.1.4.2 FMT_MTD.1 Management of TSF data).

Access to TSF data and management functions can also be restricted by location privilege assigned to the user. With LBAR, user has read and write access to TSF data (as appropriate with role as described in see Section 6.1.4.2 FMT_MTD.1 Management of TSF data) only at location assigned to user and all its child locations in the network location tree. Superuser role is always assigned to root of the tree. Users with other roles can be assigned to root or any other locations.

Administration policies are classified into two types: Global and Local. Global policies are applicable to entire system. With LBAR, only Superuser or Administrator with right at root location can modify Global policies. Local polices are customizable for locations. User can change Local policies for the location assigned to the user (and its child locations) consistent with the user role. Whether certain policy is Global or Local is indicated on the policy configuration menu.

The TOE also provides CLI (Command Line Interface) on the Sensor and the Server. Refer to Chapter 5 of [INSTALL2] and Chapter 5 of [INSTALL1] for full list of commands that are available on the Sensor CLI and the Server CLI. The CLI can be remotely accessed over the network using SSH or can be locally accessed over the serial cable. The CLI natively supports only single user with username "config". Server CLI can support additional users, but only by way of external RADIUS authentication.

Note: The CLI is used only for initial installation and offline maintenance. It is not used during normal operation of the TOE.

TOE facilitates upgrading the Sensor and Server software when required. Any update to proprietary or third party software within the Sensor and the Server is provided via the TOE upgrade process. TOE upgrade is a software upgrade process. Instructions for upgrading the TOE to the new software image are provided to customers in email. Customers can securely download the software upgrade bundle from the AirTight customer support portal (http://www.airtightnetworks.com/home/support.html). To be able to download the software from the AirTight customer support portal, the customers need to have account in the AirTight customer support portal. The customers can then log into the account with valid credentials to download the upgrade software. They can then themselves upgrade the software in the field to the desired version (see [USER], page 91, Section "Upgrade Server" for details on how to upgrade the Server software; Sensors can be upgraded after Server using right click option on the Sensor listing in the GUI). The upgrade bundle includes digital signature, which is verified before the software upgrade is performed on the TOE. AirTight also provides assisted upgrade to customers who wish so. In the assisted upgrade, AirTight support person gets into web meeting/desktop sharing with the customer and executes the above upgrade process along with the customer.

(Note: It should be understood that upgrading the Server software can put the TOE outside of the evaluated configuration, depending upon the version of the upgraded software).

SM-1: Management Functions and User Roles depend on the Operational Environment for administrative Console with a properly configured Web Browser to support the TOE's management interfaces.

7.1.4 *Protection of Security Functions*

7.1.4.1 PT-1: Internal Data Transfer Protection

(FPT_ITT.1)

The communications between the TOE components can be configured for Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6) packet-switched internetworks.

The following types of communications can occur between TOE components:

- Scan data transmission from Sensor(s) to Server
- Commands transmission from Server to Sensor(s)
- Notifications from Console to Server for data requests, selections etc.
- Responses to triggers from Server to Console

The TSF ensures that data transmitted between separate parts of the TOE are protected from disclosure and modification via cryptographic techniques.

The communication protocol between the Server and the Sensor(s) is vendor proprietary. It supports shared key based mutual authentication at the time of establishment of the communication session and thereafter supports per message HMAC-SHA-1 authentication with 160-bit authentication key and per message AES encryption with 128-bit encryption key. The authentication and encryption keys are rotated periodically. The mutual authentication, session key generation, message authentication and message encryption procedures and implementations used in the Sensor-Server communication protocol are FIPS compliant.

The communication protocol between the Server and the Console is HTTPS/TLS version 1.0. It supports certificate based Server authentication at the time of establishment of communication session and thereafter supports per-message authentication and per-message encryption. The cryptographic procedures and implementations used in the Console-Server communication are FIPS compliant (when Server is operated in FIPS mode).

Note: The SS-300-AT-C-60 Sensor appliance including software version 6.7 is FIPS 140-2, Level 2 certified. The Vendor affirms that there is no change in operation of cryptographic modules from Sensor software version 6.7 to 7.0.

PT-1: Internal Data Transfer Protection relies on the Operational Environment to provide secure communication path between the TOE components.

7.1.4.2 PT-2: Self Testing

(FPT_TST_EXT.1)

The TOE supports FIPS mode of operation. In the FIPS mode, it runs several self tests to ensure integrity and correct operation of cryptographic modules. At boot time, software integrity check is done using MD5 checksum. If it passes, the TOE performs known answer tests (KAT) for the following cryptographic modules: AES, TDES, RSA, PRNG (pseudo random generator), HMAC-SHA-1, SHA-1 and SHA-256, and performs pair wise consistency test and sign/verify for DSA. Thereafter, during operation it performs following self tests: pair wise consistency test for DSA and RSA (upon generation of new key pair) and self test for PRNG (upon every request for new random number generation). If any of the above tests fails, TOE goes to Error State and stops functioning. These self testing procedures are compliant with FIPS 140-2. Authorized administrators can perform start-up self tests on demand by rebooting the Sensor/Server.

7.1.5 *TOE Access*

7.1.5.1 TA-1: Session Termination

(FTA_SSL.3)

Session timeout setting specifies the period of inactivity after which existing session of user with the TOE console is to be automatically terminated. Superuser specifies session timeout for the user at the time of creating user account. User can later modify his own session timeout setting from User Preferences menu. Superuser can modify session timeout setting for any user. Session timeout can be between 10 min and 120 min or it can be set to never expire even in the wake of inactivity.

7.1.5.2 TA-2: Access banner

(FTA_TAB.1)

Superuser can configure a custom message to be displayed on the login screen of the console from the Login Configuration Screen. This message will then be displayed on the login screen when any user attempts to access the Console and before the user enters authentication credentials. The Superuser can create the login message to warn the user of unauthorized access.

7.1.6 *IDS Functions*

7.1.6.1 IDS-1: System Data Collection

(IDS_SDC_EXT.1)

The TOE detects WiFi threats and vulnerabilities in the monitored IP network subnets and in the optional managed WLAN. The detection is based on information (source and destination MAC addresses and other information encoded in protocol header fields) collected by Sensors from IEEE 802.11 protocol wireless transmission frames detected on radio channels and/or

IEEE 802.3 protocol traffic detected by Sensors in the wired part (Ethernet) of the monitored network subnets. Following threats and vulnerabilities are detected:

- Rogue WiFi APs connected to the local area network
- Mis-configuration of the managed WiFi APs
- Misbehaving WiFi clients, e.g., managed WiFi clients which connect to neighborhood WiFi networks, banned WiFi clients etc.
- Ad hoc connections involving managed WiFi clients
- Wireless honeypots (man-in-the-middle attacks) which attract managed WiFi clients
- WiFi Denial of Service (DoS) attacks on the managed WLAN
- WiFi MAC address spoofing
- WiFi encryption cracking
- WiFi reconnaissance

A complete list of threats and vulnerabilities detected by the TOE can be seen in the Console under the Configuration -> Events -> Configuration → Security menu. Each line item in the list there has “click for more information” button (the “i” button) which provides detailed description of the specific threat/vulnerability.

For the detected threats/vulnerabilities, the TOE generates security events that are displayed under Events → Security menu. The security event has associated with it event ID, event severity level (low, medium, high), read status (unread, read, acknowledged), activity status (live, expired, instantaneous), contribution to vulnerability status flag, event category (rogue AP, mis-configured AP, misbehaving clients, prevention, DOS, ad hoc network, man-in-the-middle, MAC spoofing, reconnaissance, cracking), time and date of the event (start and stop times), identities of devices participating in the event (MAC addresses), location tracking information of devices participating in the event (floor map view and distance from sensor view), event description, and recommended action to mitigate the detected threat/vulnerability. Some events also have sub-events that describe how events evolve from start time to stop time.

Administrator can select security events to be generated (by checking in Display column in Configuration -> Events → Configuration → Security menu). The same menu also facilitates additional configurations such as selection of email notification, selection of SNMP and syslog notification (Notify column), selection of whether event contributes to vulnerability status of network and assignment of severity level to event (low, medium, high).

The administrator can configure radio channels to be monitored by Sensors for detection of wireless transmission frames in Sensor templates (Channel Settings tab) under Configuration -> Device Configuration menu. When the Sensor is operated in Network Detector (ND) or Sensor Network Detector Combo (SNDC) configuration, administrator can also configure wired networks to be monitored for detection of Ethernet traffic (see Network Detector configuration guide).

IDS-1: System Data Collection relies on the Operational Environment to provide secure communication path between the TOE components. IDS-1 relies on Operational Environment for administrative Console with a properly configured Web Browser to support the TOE’s management interfaces.

7.1.6.2 IDS-2: Analyser Analysis

(IDS_ANL_EXT.1)

IDS_ANL_EXT.1 describes types of analysis performed on the IDS data. The TOE performs following types of analyses on the data collected by Sensors: signature analysis, statistical analysis, auto-classification of wireless devices, and wireless policy check.

Signature analysis is used to detect presence of MAC spoofing devices. Signatures for banned MAC addresses (for banned APs and clients), vulnerable SSIDs, hotspot SSIDs etc. are configurable by administrator under Configuration -> WIPS menu. Signatures to detect well-known attack tools are pre-included in the analyzer logic.

Statistical analysis is used to detect anomalies in wireless traffic to detect DoS attacks. Thresholds for statistical analysis can be modified by the administrator in Advanced Settings link of Configuration -> Events → Configuration menu.

The TOE performs auto-classification of wireless devices (WiFi access points (APs) and clients) into authorized, rogue and external categories. The authorized APs and clients list can be imported by the administrator (if optional managed WLAN is to be monitored) either from Configuration -> WIPS → Import Devices menu or by moving them from Uncategorized folder to Categorized folder in Devices listing tab. The TOE performs wired/wireless traffic correlation to identify wireless access points that are connected to the monitored network. The APs which are found inappropriately connected to the monitored network (e.g., those that are connected to no-WiFi network, which are not in the authorized AP list but are still connected to the monitored network etc.) are identified as rogue APs. The APs which are found unconnected to the monitored network are identified as external APs. The TOE thus automatically classifies APs other than authorized APs into rogue and external categories. The AP auto-classification for rogue and external APs can be enabled from the Configuration -> WIPS menu. This menu also facilitates configuring client classification policy whereby the TOE automatically classifies WiFi clients into authorized, rogue and external categories. Classifying devices into appropriate categories then facilitates identifying wireless connections which represent security violation (e.g., rogue AP, authorized client connecting to external AP, external client connecting to authorized AP etc.) versus those which represent benign neighborhood activity (e.g., external client connecting to external AP).

The TOE also facilitates configuration of wireless security policy for different locations (Configuration -> WIPS -> Authorized WLAN Policy). For example, the policy can be no-WiFi policy for particular location(s). Optionally, if managed WiFi is available for particular location(s), then desirable security settings (wireless authentication, encryption, protocol, SSID to network mapping etc.) for the managed (authorized) WiFi APs can be configured via SSID templates. TOE monitors for violation of wireless security policies. For example, if a managed WiFi AP is found to use encryption different from what is specified in policy, it is marked mis-configured AP and appropriate event and prevention action are triggered.

7.1.6.3 IDS-3: Analyser React

(IDS_RCT_EXT.1)

The TOE generates events (alarms) for detected vulnerabilities/threats. The events are displayed on the Console for administrator review. The displayed events contain various information fields as described in Section 7.1.6.1. Optionally, the events can also be sent via email including information on location node where event is raised, time and date, severity level of event, summary, description, recommended action and list of participating devices). Events can also be optionally sent as SNMP traps or as syslog events (see [USER] pages 116-117 for additional details on syslog and SNMP).

If the event is configured to affect status of vulnerability status icon on the Console, the vulnerability status icon for the location node turns red (vulnerable) at a location where the event is generated. The vulnerability status of particular location is displayed on dashboard for that location as well as vulnerability statuses of all locations are displayed in the location tree to provide overall view of network security status.

The TOE also automatically initiates over the air blocking (prevention) of wireless activity related to threat/vulnerability, if the intrusion prevention policy is enabled for that threat/vulnerability. In the intrusion prevention policy, the administrator can select threats/vulnerabilities for which automatic prevention is desired at a particular location (Configuration -> WIPS → Intrusion Prevention). Prevention can also be manually triggered on devices that are involved in the vulnerability/threat. This is done by right clicking on the device entry and selecting “Move to Quarantine” option. Over the air prevention operates by sending periodic DEAUTHENTICATE messages from the Sensor to the AP and/or Client engaged in undesirable wireless connection. The Sensor time-shares between prevention and scanning when prevention is active. The effectiveness of prevention depends on factors such as signal strength from the Sensor that can be detected by the AP and/or the Client that is under prevention, number of simultaneous channels the Sensor is preventing on, re-connection behavior of Client, etc. The effectiveness of prevention can be measured in terms of packet loss inflicted on the connection by the prevention. If automatic or manual quarantine fails for some reason (e.g., insufficient signal strength, overloaded Sensor etc.), event is generated to let administrator know about it. The TOE supports configurable level of over the air prevention (block, disrupt, interrupt, degrade). The prevention level indicates desirable effect of prevention on the wireless activity related to threat/vulnerability (e.g., in terms of inflicted packet loss). The TOE also supports configuration of channels on which prevention is to be supported (Channels to Defend setting in Sensor template).

The TOE can track physical location of devices involved in the security event by performing received signal strength based distance estimation by Sensors (“Current Location” and “Event Time Location” buttons in events). Estimated location is displayed as a region on the floor map and also provided as estimated distance from individual Sensors which see the device. If three or more Sensors can see the device, the distance estimation results into triangulation to display a more compact estimated location region on the floor map. With less than three Sensors, the estimated location region on the floor map is less compact, for example, more like annular ring with one sensor and more like elongated patch with two sensors.

IDS-3: Analyser React relies on Operational Environment for administrative Console with a properly configured Web Browser to support the TOE’s management interfaces. IDS-3 optionally relies on syslog server, email server or SNMP server in the Operational Environment if external logging is configured in the TOE. IDS-3 also optionally relies on the Operational Environment to provide secure communications between the TOE and external syslog/email/SNMP servers. (OE.PROTECTCOMM).

7.1.6.4 IDS-4: Restricted Data Review

(IDS_RDR_EXT.1)

The TOE presents system data on the Console. The data is organized into different tabs and screens. System data such as devices identities (APs, clients, sensors) and events is presented in tabular form with ability to see additional details for any row. The columns to be shown in the table are configurable. The summary information is also presented in the form of graphs and pie charts as appropriate. Forensic information on threats/vulnerabilities is presented in human readable, easy to interpret form under Forensics tab. The TOE data can also be presented in the form of reports. Certain frequently used reports such as risk/vulnerability assessment reports, regulatory/standards compliance reports (DoD, SOX, GLBA, PCI, HIPAA, MITS etc.), device inventory reports are preconfigured for the user. The TOE also facilitates users to create new reports with customized contents and look. The user can store newly created report under Reports -> Custom -> Custom Reports, in which case it can be generated by any user with privilege at the location, or the user can store newly created report under Reports -> Custom -> My Reports tab in which case it can only be generated by the user who has created it.

Note: The use of Forensics tab requires additional license in addition to the basic license.

Moreover, the data is also organized according to location context. The location tree is displayed on the Console and the data that is presented corresponds to the location node currently selected by the user. All user roles have read access to data. However, the user privilege to read TOE data is location specific, i.e., a user can read data corresponding to only those location nodes where the user has privilege.

IDS-4: Restricted Data Review relies on Operational Environment for administrative Console with a properly configured Web Browser to support the TOE’s management interfaces.

7.1.6.5 IDS-5: System Data Availability

(IDS_STG_EXT.1, IDS_STG_EXT.2)

The TOE data can be deleted and/or modified only by authorized users. The users need to properly authenticate before they can do any data deletion/modification. Moreover, the user needs to have high enough role as well as needs to have privilege at a location where data deletion/modification is attempted.

The system data is maintained in a database. The size of database is limited by available disc space. The SA-360 appliance has 500 GB of disc space. If the disc occupancy reaches unsafe limits, the TOE generates system health audit event, so that the administrator can take appropriate actions to free up disc space.

The TOE also provides various auto deletion configurations to limit the size of devices and events data. This ensures availability of the most recent/most relevant data, while controlling the disc occupancy. Whenever auto-deletion is performed, an event is generated summarizing the auto-deletion action. The TOE also provides automatic periodic database backup feature which ensures that the past system data can be retrieved when desired.

IDS-5: System Data Availability optionally relies on external servers to securely store backed up database. It also optionally relies on the Operational Environment to provide secure communication path between the TOE and the external backup servers.

7.1.7 *Cryptographic Support*

7.1.7.1 CS-1: Cryptographic keys and operations

(FCS_BCM_EXT.1, FCS_CKM.1, FCS_CKM.4, FCS_COP.1)

The TOE performs cryptographic functions for: a) Sensor-Server communication, b) Console-Server communication, c) SSH utility in Sensor and Server.

The Sensor-Server communication protocol is vendor proprietary. It runs over UDP. It is called as "SpectraTalk" protocol and IANA (Internet Assigned Number Authority) has assigned UDP and TCP port numbers 3851 to SpectraTalk protocol. SpectraTalk uses 128 bit manually entered master key for mutual authentication between Sensor and Server at the time of session establishment. The mutual authentication is performed by challenge/response procedure in which each side sends challenge text to the other side and the other side sends response, which is AES-CBC encrypted (with master key) version of the challenge text. Once authentication is complete, the Server randomly generates 128 bit session key and transports it to the Sensor using AES-CBC encryption with master key. The Sensor and Server then generate message authentication keys (160 bits) and message encryption keys (128 key) by using HMAC-SHA-1 on predetermined texts and using session key as secret. The message authentication key is used for HMAC-SHA-1 message integrity protection and the message encryption key is used for AES-CBC message encryption between Sensor and Server. In each of the Sensor and Server, there is one pair of authentication/encryption key for outbound messages and one pair of authentication/encryption key for inbound messages. The master key is same for all Sensors, while all other keys described above are different for different Sensors. The above described key generation, message integrity and message encryption algorithms are all FIPS 140-2 approved.

Console-Server communication occurs over HTTPS using TLS version 1.0. It supports digital signatures, encryption and authentication as described in the TLS version 1.0 standard (RFC 2246). The Sensor and the Server also include SSH version 2 utility to support remote CLI access and to perform secure file copy (SCP). The SSH utility supports digital signatures, encryption and authentication as described in the SSH version 2 standard (RFC 4252 and RFC 4253).

Table 7-2: Cryptographic Key Generation and Deletion

Cryptographic Component	Key Type	When Generated	When Deleted	How Deleted
SSH version 2	RSA and DSA key pair	First ever boot time, first boot time after entry/exit from FIPS mode or factory reset	Factory reset, entry/exit from FIPS mode	The file containing key is deleted

Cryptographic Component	Key Type	When Generated	When Deleted	How Deleted
	Ephemeral key (session key)	Initiation of SSH session	Termination of SSH session	The memory block in volatile memory containing key is freed
	Message encryption and authentication keys	Rotated periodically during established SSH session	Rotated periodically during established SSH session	The memory block in volatile memory containing key is freed
TLS 1.0	RSA key pair	First ever boot time, first boot time after entry/exit from FIPS mode or factory reset or import of new Server certificate	Factory reset, entry/exit from FIPS mode, import of new Server certificate	The file containing key is deleted
	Diffie Hellman key pair	Initiation of TLS session	Termination of TLS session	The memory block in volatile memory containing key is freed
	Message encryption and authentication keys	Rotated periodically during established TLS session	Rotated periodically during established TLS session	The memory block in volatile memory containing key is freed
Sensor-Server Communication Protocol	Master key	Manually entered	Factory reset, entry/exit from FIPS mode, entry of new key	The file containing key is deleted
	Session key	Initiation of Sensor-Server session	Sensor disconnection from Server	The memory block in volatile memory containing key is freed
	Message encryption and authentication keys	Rotated periodically during established Sensor-Server session	Rotated periodically during established Sensor-Server session	The memory block in volatile memory containing key is freed

The TOE supports FIPS mode of operation. Sensor is FIPS 140-2, Level 2 certified (certificate number 1609) and the Server is FIPS 140-2, Level 1 certified (certificate number 1649).

Note: The SS-300-AT-C-60 Sensor appliance including software version 6.7 is FIPS 140-2, Level 2 certified (certificate number 1609). The Vendor affirms that there is no change in operation of cryptographic modules from Sensor software version 6.7 to 7.0.

Note: The Server application version 6.5 is FIPS 140-2, Level 1 certified (certificate number 1649).In the Server application version 7.0, the OpenSSL library has been upgraded to the *latest release 1.0.1g with FIPS object module 2.0.5, which in the Server application version 6.5 was OpenSSL version 0.9.7d with FIPS object module 1.2. The OpenSSL version in the Server application version 7.0 is free from Heartbleed vulnerability. Vendor asserts that there is no change in cryptographic functionality of the TOE from the Server application version 6.5 to version 7.0.*