AirMagnet Enterprise System 8.5
Security Target

Version 0.04

Table of Contents

1 Security Target Introduction

1.1 Security Target and TOE Identification

Security Target Title: AirMagnet Enterprise System 8.5 Security Target, ST Version: 0.04 (May 31, 2009)

TOE Identification: AirMagnet Enterprise 8.5.0-12047

Common Criteria Version: Common Criteria Version 2.3

Assurance Level: EAL2

Strength of Function: SOF-basic

1.2 Security Target Overview

AirMagnet Enterprise 8.5 is a wireless intrusion detection system. AirMagnet Enterprise Sensors provide a distributed wireless security and integrity management system that brings control over the wireless network, and provides the information and tools needed to support any number of WLANs throughout the entire network lifecycle.

AirMagnet Enterprise Sensors are positioned within the range of one or more wireless Internet networks (802.11-A, 802.11-B, or 802.11-G) throughout an enterprise. Each sensor monitors wireless network traffic and periodically reports collected traffic statistics, identifies access points and stations, performance anomalies, and security anomalies to a centralized server over a wired HTTPS connection. Authorized operators view the collected statistics of all sensors using the AirMagnet Enterprise Management Console program that accesses the centralized server over HTTPS. In the event of unusual or suspicious traffic, operators can invoke the console's Remote AirMagnet Program to view the live data being collected by any one sensor, connecting directly to the sensor over HTTPS.

1.3 Common Criteria Conformance

Common Criteria: Part 2 extended, Part 3 conformant,

Assurance Level: EAL2

1.4 Conventions

The notation, formatting, and conventions used in this ST are consistent with version 2.3 of the Common Criteria (CC). The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

The CC paradigm also allows protection profile (PP) and security target authors to create their own requirements. Such requirements are termed 'explicit requirements' and are permitted if the CC does not offer suitable requirements to meet the authors' needs. Explicit requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. In this ST, explicit requirements will be indicated with the "_EXP" following the component name.

Assumptions: TOE security environment assumptions are given names beginning with "A."-- e.g., A.ACCESS.

Threats: Threats are given names beginning with "T."-- e.g., T.COMINT.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.CRYPTOGRAPHY.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively,—e.g., O.CRYPTOGRAPHY and OE.INSTAL.

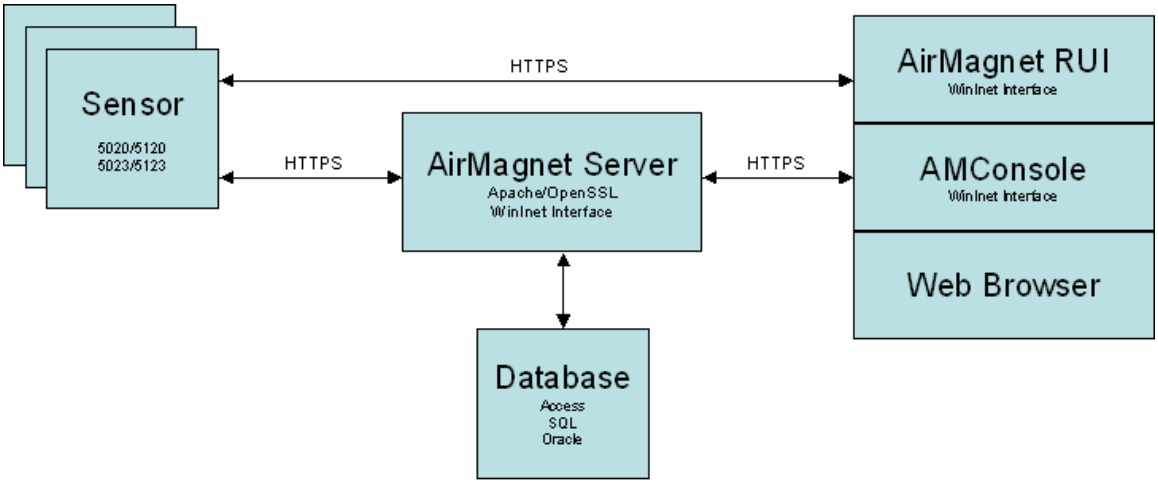
2 TOE Description

2.1 System Type

The AirMagnet Enterprise 8.5 consists of three major components— SmartEdge Sensors that provide remote monitoring and troubleshooting of 802.11 wireless networks, a centralized Enterprise Server that correlates events and integrates to other systems, and Enterprise Console that provides the user interface to the system.

As depicted on Figure 1, standalone SmartEdge Sensors (A5020, A5120, A5023, and A5123) are deployed near clusters of access points. The sensors provide security assessment, performance monitoring, network fault detection and remote troubleshooting functions. Administrators can monitor the security measures in use on every wireless network station and access point device to insure compliance with established policies, and also automatically scan for dozens of wireless network attacks.

Figure 1. AirMagnet Enterprise



The TOE is developed by AirMagnet, Inc., 830 E. Arques Ave., Sunnyvale, CA 94085, USA.

The intelligent sensors of AirMagnet Enterprise 8.5 provide around-the-clock coverage of the entire wireless environment including all 802.11a, 802.11b, and 802.11g channels and infrastructure. Each individual sensor includes the AirWISE Analytical Engine that, in real time, monitors and analyzes the security, performance, and reliability of the wireless network.

AirMagnet Sensors audit and validate the security of every Wi-Fi device in the network, helping to insure all users employ the appropriate level of security. Supported protocols include wep, leap, peap, tkip, mic, 802.1x, ttls, tls, wpa, pptp vpn, l2tp vpn, ssh vpn, ipsec vpn.

AirMagnet Enterprise is engineered to counter wireless threats - scanning the environment for Rogue APs and War-Drivers, Spoofed MAC Addresses, and a host of Denial of Service Attacks unique to Wi-Fi. Sensors send encrypted alarms in real time in response to an attack, allowing the staff to respond before network operations are negatively impacted. AirMagnet Sensors constantly monitor and generate alarms on over 20 key indicators of network health, allowing the administrators to take a proactive approach toward the maintenance of the network.

IT Personnel is allowed to tune sensor thresholds appropriately. Additionally, AirMagnet Enterprise supports unique user levels, insuring that the users access only the level of information appropriate for their role and level of responsibility.

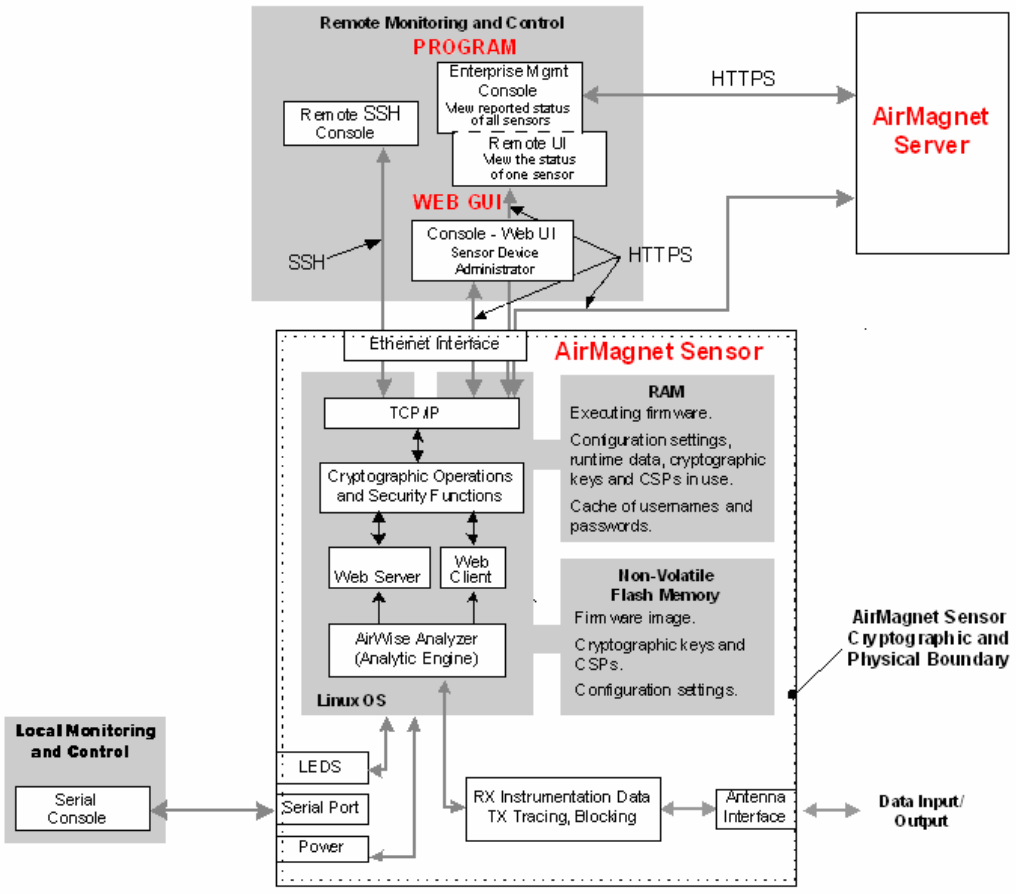
2.3 TOE Physical Boundaries

The TOE includes four Sensor models: AirMagnet SmartEdge Sensors A5020, A5120, A5023, and A5123.

Figure 2 shows a logical block diagram of the Sensor that illustrates the physical boundaries of the Sensor as well as the Sensor interfaces.

The physical boundaries of the Enterprise Server and the Enterprise Console components match the physical boundaries of the corresponding PCs on which these components are executing.

Figure 2. AirMagnet Sensor Component Architecture



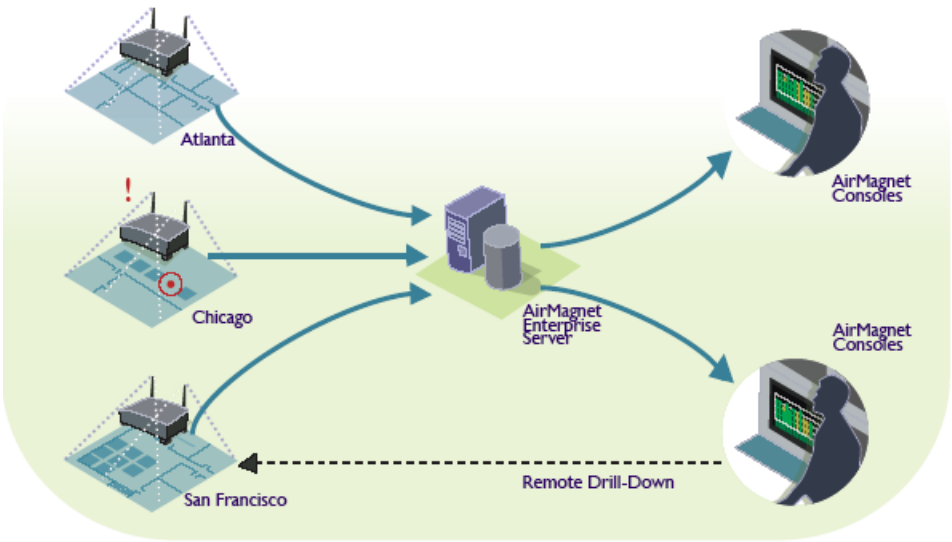
2.4 TOE Logical Boundaries

The following components are included in the logical boundary of the TOE:

- AirWise Analyzer. Analyzes wireless network traffic to detect security-relevant conditions.
- Sensor 802.11 network interface. Provides network functionality that is used to capture wireless network traffic as well as to perform wireless blocking.
- Sensor Ethernet network interface. This interface is used for TLS-secured remote communications, including remote Sensor administration.
- Web server/client. These components are used to support TLS-secured remote communications via the Ethernet interface.
- Sensor firmware update client. This component is used to facilitate secure firmware updates.
- OpenSSL Cryptographic library that provides cryptographic services for the TLS and other components.
- Sensor serial interface that includes CLI. The CLI is used for local Sensor administration.
- Enterprise Server and Enterprise Console applications.

Figure 3 illustrates the logical interconnections between the TOE components. Sensors report collected statistics to the AirMagnet Enterprise Server. Operators at the TLS-secured Enterprise Consoles view the reported data from each sensor. Remote drill-down capabilities let operators connect to any sensor to view its live data as well as initiate blocking and tracing operations.

Figure 3. TOE operation



3 TOE Security Environment

This section describes the assumptions, threats, and policies that are relevant to both the TOE and the TOE environment.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 1: Assumptions

Name	Assumption
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
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.
A.NOTRST	The TOE can only be accessed by authorized users.

3.2 Threats

The following are threats identified for the TOE and the IT System the TOE monitors.

Table 2: Threats

Threat Name	Threat Definition
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.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

Threat Name	Threat Definition
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.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
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.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each 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.
T.MISUSE.	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 3 identifies the organizational security policies applicable to this ST.

Table 3: Organizational Security Policies

Policy Name	Policy Definition
P.CRYPTOGRAPHY	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
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).

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.
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.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

Table 4: Security Objectives for the TOE

Name	TOE Security Objective
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.
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.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The TOE 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.
O.IDSENS	The TOE 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.
O.IDANLZ	The TOE must accept data from Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.

Name	TOE Security Objective
O.EXPORT	When any TOE component makes its data available to another TOE component, the TOE will ensure the confidentiality of the System data.

4.2 Security Objectives for the Environment

The TOEs operating environment must satisfy the following objectives.

Table 5: Security Objectives for the Environment

Name	TOE Security Objective
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.
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.
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.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps to the TOE.
OE.SELF_PROTECTION	The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.

5 IT Security Requirements

This section defines the functional requirements for the TOE that are relevant to supporting the secure operation of the TOE, as well as the assurance requirements for the TOE.

5.1 Strength of Function Claims

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism, except for cryptographic functions. For this ST, the minimum level will be SoF-basic.

In the event that a probabilistic mechanism, such as a password mechanism for user and/or administrator authentication is used, then the expectation is that for each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in a million. FIA_UAU.1 includes the probabilistic/permutational mechanism in the form of password-based authentication of users, for which specific SOF metrics are appropriate.

5.1 TOE Security Functional Requirements

This section defines the functional requirements for the TOE. The explicit requirements are indicated with the “EXP” following the component name. All other functional requirements in this ST were drawn from Part 2 of the CC.

Table 6: TOE Security Functional Requirements

Functional Component		Dependencies
FAU_GEN.1	Audit data generation	FPT_STM.1
FAU_SAR.1	Audit review	FAU_GEN.1
FAU_STG.1	Protected audit trail storage	FAU_GEN.1
FCS_BCM_EXP.1	Baseline Cryptographic Module	None
FCS_CKM.1	Cryptographic key generation	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2
FCS_CKM.4	Cryptographic key destruction	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2
FCS_COP_EXP.1	Random Number Generation	[FDP_ITC.1or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP_EXP.2(1)	Cryptographic Operation	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP_EXP.2(2)	Cryptographic Operation	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FIA_ATD.1	Administrator attribute definition	None
FIA_UAU.1	Timing of authentication	FIA_UID.1

Functional Component		Dependencies
FIA_UID.1	Timing of identification	None
FMT_MOF.1	Management of security functions behavior	FMT_SMF.1(2) FMT_SMR.1
FMT_MSA.2	Secure security attributes	ADV_SPM.1 [FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1
FMT_MTD.1(1)	Management of System and audit data	FMT_SMF.1(1) FMT_SMR.1
FMT_MTD.1(2)	Management of time data	FMT_SMF.1(2) FMT_SMR.1
FMT_SMF.1(1)	Specification of Management Functions (System and audit data)	None
FMT_SMF.1(2)	Specification of Management Functions (time data and security configuration management)	None
FMT_SMR.1	Security roles	FIA_UID.1
FPT_ITC.1	Inter-TSF confidentiality during transmission	None
FPT_ITI.1	Inter-TSF detection of modification	None
FPT_ITT.1	Basic internal TSF data transfer protection	None
FPT_RVM.1(1)	Non-bypassability of the TOE Security Policy (TSP)	None
FPT_SEP.1(1)	TSF domain separation	None
FPT_STM_EXP.1	Reliable time stamps	None
IDS_ANL_EXP.1	Analyzer analysis	None
IDS_RCT_EXP.1	Analyzer react	None
IDS_RDR_EXP.1	Restricted Data Review	None
IDS_SDC_EXP.1	System Data Collection	None
IDS_STG_EXP.1	Guarantee of System Data Availability	None

5.1.1 Security Audit (FAU)

FAU_GEN.1 Audit data generation

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 *unspecified* level of audit; and

c) [auditable events specified in table 7].

Table 7: TOE Auditable Events

Requirement	Auditable Events
FAU_GEN.1	Access to System
FIA_UAU. 1	All use of the authentication mechanism

Requirement	Auditable Events
FIA_UID.1	All use of the user identification mechanism
FMT_MOF.1	All modifications in the behavior of the functions of the TSF
FMT_SMR.1	Modifications to the group of users that are part of a role

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, [none].

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [the authorized users] with the capability to read [any audit information] 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.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the audit records in the audit trail.

5.1.2 Cryptographic support (FCS)

FCS_BCM_EXP.1 Baseline Cryptographic Module

FCS_BCM_EXP.1.1 All cryptographic modules shall comply with FIPS 140-1/2 when performing FIPS approved cryptographic functions in FIPS approved cryptographic modes of operation.

FCS_BCM_EXP.1.2 The cryptographic module implemented shall have a minimum overall rating of Level 1.

FCS_BCM_EXP.1.3 The FIPS validation testing of the TOE cryptographic module(s) shall be in conformance with FIPS 140-1, 140-2, or the most recently approved FIPS 140 standard for which NIST is accepting validation reports from Cryptographic Modules Testing laboratories.

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [listed in Table 8: Cryptographic Operation] and specified cryptographic key sizes [listed in Table 8: Cryptographic Operation] that meet the following: [standards listed in Table 8: Cryptographic Operation].

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a [cryptographic key zeroization method] that meets the following: [

c) The Key Zeroization Requirements in FIPS PUB 140-1/2 Key Management Security Levels 1;

d) Zeroization of all private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters shall be immediate and complete.]

FCS_COP_EXP.1 Random Number Generation

FCS_COP_EXP.1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved cryptomodule running in a FIPS-approved mode.

FCS_COP_EXP.2(1) Cryptographic Operation

FCS_COP_EXP.2.1(1) A cryptomodule shall perform encryption and decryption using the FIPS-140-1/2 Approved *AES* algorithm and operating in [ECB mode, CBC mode] and supporting FIPS approved key sizes of [128 bits, 256 bits].

FCS_COP_EXP.2(2) Cryptographic Operation

FCS_COP_EXP.2.1(2) A cryptomodule shall perform encryption and decryption using the FIPS-140-1/2 Approved *Triple DES* algorithm and operating in [CBC mode] and supporting FIPS approved key sizes of [168 bits].

Table 8: Cryptographic Operation

Cryptographic operations	Cryptographic algorithm	Key sizes (bits)	Standards
Data authentication and verification.	SHA-1 HMAC SHA-1	 128	FIPS PUB 180-2 FIPS PUB 198
Encryption/decryption of the traffic	AES–ECB AES–CBC	128 256	FIPS PUB 197
Encryption/decryption of the traffic	Triple DES-CBC	168	FIPS PUB 46-3
Public key encryption/decryption and signature generation/verification	RSA	2048	FIPS PUB 186-2
Random data generation	RNG	112	ANSI X9.31

5.1.3 Identification and authentication (FIA)

FIA_ATD.1 User attribute definition

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

a) User identity;
b) Authentication data;
c) Authorizations
].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [secure TLS connection establishment, user identification] on behalf of the user to be performed before the user is authenticated.

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

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [secure TLS connection] on behalf of the user to be performed before the user is identified.

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

5.1.4 Security management (FMT)

FMT_MOF.1 Management of audit security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behaviour of* the functions of [System data collection, analysis and reaction] to [administrators].

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MTD.1(1) Management of System and audit data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, clear* the [System and audit data] **and shall restrict the ability to modify, delete System data** to [the authorized users].

FMT_MTD.1(2) Management of time data

FMT_MTD.1.1(2) The TSF shall restrict the ability to *[set]* the [time and date used to form the time stamps in FPT_STM_EXP.1] to [the administrator or authorized IT entity].

FMT_SMF.1(1) Specification of Management Functions (System and audit data)

FMT_SMF.1.1(1) The TSF shall be capable of performing the following security management functions: [query, clear System and audit data and modify, delete System data].

FMT_SMF.1(2) Specification of Management Functions (time data and security configuration management)

FMT_SMF.1.1(2) The TSF shall be capable of performing the following security management functions: [set time and date used to form the time stamps in FPT_STM_EXP.1 and security configuration management].

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [administrator, user].

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

5.1.5 Protection of the TSF (FPT)

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [a TLS integrity error].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [retransmission in case of a protocol error, or session termination in case of malicious tampering] if modifications are detected.

FPT_ITT.1 Basic internal TSF data transfer protection

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

FPT_RVM.1(1) Non-bypassability of the TOE Security Policy (TSP)

FPT_RVM.1.1(1) The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1(1) TSF domain separation

FPT_SEP.1.1(1) The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2(1) The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM_EXP.1 Reliable time stamps

FPT_STM_EXP.1.1 The TSF shall be able to provide reliable time stamps**, synchronized via an external time source,** for its own use.

5.1.6 IDS component requirements (IDS)

IDS_ANL_EXP.1 Analyzer analysis

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

a) *statistical*; *signature* and

b) [none].

IDS_ANL_EXP.1.2 The System 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) [none].

IDS_RCT_EXP.1 Analyzer react

IDS_RCT_EXP.1.1 The System shall send an alarm to [the Enterprise Server] and [attempt to deactivate a potentially insecure wireless device] when such device is detected.

IDS_RDR_EXP.1 Restricted Data Review

IDS_RDR_EXP.1.1 The System shall provide [authorized users] with the capability to read [all wireless activity data] from the System data.

IDS_RDR_EXP.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

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

IDS_SDC_EXP.1 System Data Collection

IDS_SDC_EXP.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) [SSID, MAC address, status (active/down), first and last seen time, ACL status (known device/rogue/ neighbor/monitored), channel, security status]; and

b) [no other information].

IDS_SDC_EXP.1.2 At minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity; and

b) [no other information].

IDS_STG_EXP.1 Guarantee of Sensor Data Availability

IDS_STG_EXP.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

IDS_ STG.1.3 The System shall ensure that [the latest, up to the maximum storage capacity] System data will be maintained when the following conditions occur: *System data storage exhaustion*.

5.2 Security Requirements for the IT Environment

Table 9: Security Requirements for the IT Environment

Functional Component		Dependencies
FPT_RVM.1(2)	Non-bypassability of the TOE Security Policy (TSP)	None
FPT_SEP.1(2)	TSF domain separation	None
FPT_STM.1	Reliable time stamps	None

5.2.1 Protection of the TSF (FPT)

FPT_RVM.1(2) Non-bypassability of the TOE Security Policy (TSP)

FPT_RVM.1.1(2) The ~~TSF~~ **TOE IT environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the ~~TSC~~ **IT environmental scope of control** is allowed to proceed.

FPT_SEP.1(2) TSF domain separation

FPT_SEP.1.1(2) The ~~TSF~~ **TOE IT environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2) The ~~TSF~~ **TOE IT environment** shall enforce separation between the security domains of subjects in the ~~TSC~~ **IT environmental scope of control**.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The ~~TSF~~ **TOE IT environment** shall be able to provide reliable time stamps for **the TOE and** its own use.

5.3 Assurance Requirements

This chapter defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 assurance requirements.

5.3.1 Assurance components

Table 10: TOE Security Assurance Requirements

Assurance Class	Assurance Component	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

6 TOE Summary Specification

This section addresses IT security functions and the corresponding assurance measures.

6.1 TOE Security Functions

The security functions implemented by the TOE are presented in the following table:

Table 11: TOE Security Functions

Security Function Name
Security Audit
Identification and Authentication
Security Management
Protection of the TSF
IDS Function
Cryptographic Support

6.1.1 Security Audit

The Security Audit function enables generation of audit records of the following auditable events (FAU_GEN.1):

1. Startup and shutdown of the audit functions
2. Access to System
3. All use of the authentication mechanism
4. All use of the user identification mechanism
5. All modifications in the behavior of the functions of the TSF
6. Modifications to the group of users that are part of a role

The audit logs include the following data:

1. Date and time of the event
2. Type of event
3. Subject identity
4. The outcome (success or failure) of the event

AirMagnet Server and AirMagnet Sensors allow successfully authenticated users to assume Administrator role and User role with the capability to read any audit information from the audit records. The users can use the GUI to access the audit information. The GUI also provides the audit records in a manner suitable for the user to interpret the information (FAU_SAR.1). The audit trail is protected as follows: the audit data is stored on a FIPS 140-2 certified module while on the Sensor or Server. The Sensor and Server prevent any audit data access by unauthorized operators. Therefore, stored audit records are protected from unauthorized deletions and modifications (FAU_STG.1).

6.1.2 Identification and Authentication

TOE provides centralized user management. Each user account includes the following security attributes:

1. User identity;
2. Authentication data (i.e. strong password)
3. Authorizations (Administrator, User) (FIA_ATD.1).

The Sensor and Server components only allow secure TLS connection for a login attempt on behalf of the user before the user is authenticated using correct user name and password. These components require each user to be successfully authenticated before allowing other mediated actions on behalf of that user (FIA_UAU.1). TOE components only allow secure TLS connection for a login attempt on behalf of the user before the user is identified by supplying the user name. These components require each user to be successfully identified before allowing any other mediated actions on behalf of that user (FIA_UID.1).

6.1.3. Security Management

The Security Management function restricts the ability to modify the behavior of the functions of System data collection, analysis and reaction to authorized System administrators. The TOE provides users successfully authenticated to assume Administrator role with the capability to modify the behavior of the functions of System data collection, analysis and reaction. These users can use the GUI to perform such modifications. The TOE architecture ensures that other users cannot modify the behavior of the functions of System data collection, analysis and reaction (FMT_MOF.1). The TOE design restricts the ability to query and clear the System and audit data, and the ability to modify and delete the System data to the authorized TOE users, and restricts the ability to set the time and date used for the time stamps to TOE administrators or an authorized NTP server. TOE does not allow users or administrators to add System or audit data (FMT_MTD.1(1) and FMT_MTD.1.(2)). The TOE is capable of performing a query and clearing of System and audit data as well as performing a modification and deletion of System Data, setting time and date used to form the time stamps in FPT_STM_EXP.1, and security configuration management using the local and remote interfaces (FMT_SMF.1(1) and FMT_SMF.1(2)). The TOE maintains the administrator role and the user role in a centralized user management database (FMT_SMR.1). The TOE ensures that security attributes related to cryptographic objects (e.g. cryptographic keys) are protected (FMT_MSA.2).

6.1.4. Protection of the TSF

All data transmitted from TOE components to remote trusted IT products, such as Web UI clients, is protected from unauthorized disclosure during transmission using TLS (FPT_ITC.1). All modifications of data during transmission between the TOE components and remote trusted IT products trigger TLS integrity error and are therefore detected. The use of TLS ensures the integrity of all data transmitted between the TOE components and remote trusted IT products. Underlying TCP/IP layers also help to ensure integrity of such data and provide necessary retransmission mechanisms (FPT_ITI.1). The TOE utilizes TLS protocol to protect the TSF data that is transmitted between separate parts of the TOE from disclosure and modification (FPT_ITT.1.1).

The TSF ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. TOE maintains centralized user database and requires successful operator authentication. In particular, Sensor Wireless traffic port is only used to monitor wireless network traffic and to launch an active response to network security issues. This port is not used for any other communications or tasks. The Sensor Ethernet port can only be accessed by authorized operators. Such access is protected by TLS. After successful

authentication, an operator assumes the administrator role or the user role. The role determines the set of actions that can be performed by the operator. The Serial port of the Sensor is used for setup and administration. Only an authorized operator that has physical access to the Sensor and knows the Sensor Shared secret is able to access the Sensor command prompt via the Serial port (FPT_RVM.1).

The TSF maintains a security domain for its own execution that protects it from interference and tampering by non-trusted subjects. In particular, AirMagnet SmartEdge Sensors and AirMagnet Enterprise Server are multi-chip standalone products utilizing FIPS 140-2 cryptographic modules. All Sensor and Server services are executed on the Sensor or Server hardware, and access to the Sensors and Server is physically and logically protected. The TOE implements user session separation and separate handling of the monitored wireless devices (FPT_SEP.1).

The Sensor maintains internal clock that is able to provide reliable time stamps for Sensor's use. The clock is synchronized with the Server clock upon startup of the Sensor and periodically thereafter. The Server clock is periodically synchronized with the official atomic clock (FPT_STM_EXP.1).

6.1.5 IDS Function

TOE performs statistical and signature analysis on all wireless traffic data received. The results are compared to pre-defined patterns to identify security-relevant network conditions.

The following information is recorded within each analytical result:

1. Date and time of the result
2. Type of result
3. Identification of data source (IDS_ANL_EXP.1)

The Sensor sends an alarm to the Enterprise Server and attempts to deactivate a potentially insecure wireless device when an insecure condition is detected. A corresponding log entry is made. (IDS_RCT_EXP.1).

The TOE is able to collect the following events from the targeted wireless devices:

1. SSID
2. MAC address
3. Status (active/down)
4. First and last seen time
5. ACL status (known device/rogue/ neighbor/monitored)
6. Channel
7. Security status

TOE also collects the following information:

1. Date and time of the event
2. Type of event
3. Subject identity (IDS_SDC_EXP.1).

The TOE provides the authorized users with the capability to read all wireless activity data using the GUI. TOE architecture does not permit any access to System data by unauthorized users.

The TOE provides users successfully authenticated to assume the administrator role or the user role with the capability to read the System data. The authorized users can use the GUI Interface to access the System data which is presented in a manner suitable for the user to interpret the information (IDS_RDR_EXP.1).

TOE protects the stored TOE data from unauthorized deletion and modification. In particular, only authorized users successfully authenticated to assume the administrator role or the user role are able to delete the stored TOE data. The TOE data is stored on a FIPS 140-2 Level 2 certified module while on the Sensor or Server. The Sensor and Server prevent any TOE data modification or deletion by unauthorized operators. The TOE design ensures that the latest, up to the maximum storage capacity TOE data is maintained when TOE data storage is exhausted (IDS_STG_EXP.1).

6.1.6 Cryptographic Support

AirMagnet Sensors and Enterprise Server comply with FIPS 140-2 when performing FIPS approved cryptographic functions in the FIPS approved mode of operation. The cryptographic modules that are used have an overall rating of Level 2 and Level 1 correspondingly. The FIPS validation testing of the cryptographic modules used by Sensors and the Server is in conformance with FIPS 140-2 (FCS_BCM_EXP.1). AirMagnet Enterprise Server and Sensors generate cryptographic keys in accordance with a specified cryptographic key generation algorithms and specified cryptographic key sizes listed in Table 8: Cryptographic Operation (FCS_CKM.1). The TOE destroys cryptographic keys in accordance with the cryptographic key zeroization method that meets the key zeroization requirements in FIPS PUB 140-2 Key Management Security Level 1. Zeroization of all private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters is immediate and complete (FCS_CKM.4). The TOE performs all cryptographic random number generation using a FIPS-approved Random Number Generator (ANSI X9.31) implemented in a FIPS-approved Sensor or Server cryptomodule running in a FIPS-approved mode (FCS_COP_EXP.1). The TOE performs encryption and decryption using the FIPS 140-2 Approved Triple DES and AES algorithms, operating in a FIPS 140-2 mode and supporting FIPS approved key sizes as listed in Table 8: Cryptographic Operation (FCS_COP_EXP.2(1) and FCS_COP_EXP.2(2)).

6.2 TOE Security Functions Rationale

The following table provides the mapping between security functions and security functional requirements.

Table 12: Mapping between security functions and security functional requirements

	Security Audit	Identification and Authentication	Cryptographic Support	Protection of the TSF	Security Management	IDS Function
FAU_GEN.1	X					

	Security Audit	Identification and Authentication	Cryptographic Support	Protection of the TSF	Security Management	IDS Function
FAU_SAR.1	X					
FAU_STG.1	X					
FCS_BCM_EXP.1			X			
FCS_CKM.1			X			
FCS_CKM.4			X			
FCS_COP_EXP.1			X			
FCS_COP_EXP.2(1)			X			
FCS_COP_EXP.2(2)			X			
FIA_ATD.1		X				
FIA_UAU.1		X				
FIA_UID.1		X				
FMT_MOF.1					X	
FMT_MSA.2					X	
FMT_MTD.1(1)					X	
FMT_MTD.1(2)					X	
FMT_SMF.1(1)					X	
FMT_SMF.1(2)					X	
FMT_SMR.1					X	
FPT_ITC.1				X		
FPT_ITI.1				X		
FPT_ITT.1				X		
FPT_RVM.1(1)				X		
FPT_SEP.1(1)				X		
FPT_STM_EXP.1				X	X	
IDS_ANL_EXP.1						X
IDS_RCT_EXP.1						X
IDS_RDR_EXP.1						X
IDS_SDC_EXP.1						X
IDS_STG_EXP.1						X

6.3 Assurance Measures

The assurance measures addressed in this section apply to the EAL 2 requirements and are presented in the following table.

Table 13: Assurance Measures

Assurance Compoment	Assurance measure
ACM_CAP.2 Configuration items	AirMagnet Design Assurance procedures
ADO_DEL.1 Delivery procedures	AirMagnet Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures	AirMagnet Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification	AirMagnet Functional Specification
ADV_HLD.1 Descriptive high-level design	AirMagnet High-Level Design Specification
ADV_RCR.1 Informal correspondence demonstration	AirMagnet Informal Correspondence Demonstration
AGD_ADM.1 Administrator guidance	AirMagnet 8.5 Enterprise User Guide
AGD_USR.1 User guidance	AirMagnet 8.5 Enterprise User Guide
ATE_COV.1 Evidence of coverage	AirMagnet Evidence of Coverage
ATE_FUN.1 Functional testing	AirMagnet Functional Testing Plan
ATE_IND.2 Independent testing – sample	AirMagnet Functional Testing Plan
AVA_SOF.1 Strength of TOE security function evaluation	AirMagnet SOF Analysis
AVA_VLA.1 Developer vulnerability analysis	AirMagnet Vulnerability Analysis

7. Protection Profile claims

This Security Target does not correspond to any Protection Profile.

8. 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.

8.1 Rationale for Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. Table 14 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 14: Security Environment vs. Objectives

	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.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME_STAMPS	OE.SELF_PROTECTION
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
T.COMDIS	X						X	X				X									X
T.LOSSOF	X						X	X			X										X
T.NOHALT		X	X	X			X	X													
T.PRIVIL	X						X	X													X
T.IMPCON						X	X	X							X						
T.INFLUX									X												
T.FACCNT										X											
T.SCNCFG		X																			
T.SCNMLC		X																			
T.SCNVUL		X																			
T.FALACT					X																
T.FALREC				X																	
T.FALASC				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.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME_STAMPS	OE.SELF_PROTECTION
T.MISUSE			X							X											
T.INADVE			X							X											
T.MISACT			X							X											
P.DETECT		X	X							X											
P.ANALYZ				X																	
P.MANAGE	X					X	X	X							X		X	X			X
P.ACCESS	X						X	X													X
P.ACCACT								X		X										X	
P.INTGTY											X										
P.PROTCT									X							X					
P.CRYPTOGRAPHY													X	X							
P.CRYPTOGRAPHY_VALIDATED													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 to protect 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 objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective 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. The OE.SELF_PROTECTION objective ensures that the TOE IT environment will have protection similar to that of the TOE.

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 objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective 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. The OE.SELF_PROTECTION objective ensures that the TOE IT environment will have protection similar to that of the TOE.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective 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. The OE.SELF_PROTECTION objective ensures that the TOE IT environment will have protection similar to that of the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the TOE.s collection and analysis functionality by halting execution of the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives objective addresses this threat by requiring the TOE to collect and analyze all events, including those attempts to halt the TOE.

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 objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.SELF_PROTECTION

objective ensures that the TOE IT environment will have protection similar to that of the TOE.

T.IMPCON The TOE may be susceptible to improper configuration by any user 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 objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

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 the TOE handle data storage overflows.

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, that 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 IT System protected data or undermines the IT System security functions. The O.IDSCAN objective counters this threat by requiring a TOE, that 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, that 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.

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 that is monitored by the TOE. The O.AUDITS and O.IDSENS objectives address this threat by requiring collection of audit and Sensor data.

T.INADVE Inadvertent activity and access may occur on an IT System that is monitored by the TOE. The O.AUDITS and O.IDSENS objectives address this threat by requiring collection of audit and Sensor data.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System. The O.AUDITS and O.IDSENS objectives address this threat by requiring collection of audit and Sensor data.

P.DETECT All 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 and O.IDSENS, and O.IDSCAN objectives require collection of audit and Sensor data.

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 be 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 administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective provides for TOE self-protection. The OE.SELF_PROTECTION objective ensures that the TOE IT environment will have protection similar to that of the TOE.

P.ACCESS All data collected and produced by the IDS shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection. The OE.SELF_PROTECTION objective ensures that the TOE IT environment will have protection similar to that of the TOE.

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 objective supports this objective by ensuring each user is uniquely identified and authenticated. OE.TIME_STAMPS ensures that the TOE IT environment provides time services.

P.INTGTY Data collected 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 collection activities. The O.OFLOWS objective requires the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

P.CRYPTO The TOE shall provide cryptographic functions for its own use, including

GRAPHY encryption/decryption operations. O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will 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). O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. O.CRYPTOGRAPHY_VALIDATED satisfies this policy by requiring that all cryptomodules for cryptographic services be NIST 140-1/2 validated. This will provide assurance that the NIST-approved security functions and random number generation will be in accordance with NIST and validated according the FIPS 140-1/2.

8.2 Rationale for Security Objectives for the Environment

The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. The remainder of the security objectives for the IT environment have been included in this ST in order to support the TOE IT environment security functions. The rationale support is documented in Section 8.1 along with the rationale for security objectives for the TOE.

8.3 Rationale for TOE Security Requirements

This section demonstrates that the functional components selected for the TOE provide complete coverage of the defined TOE security objectives. The mapping of components to security objectives is depicted in the following table.

Table 15: 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.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED
FAU_GEN.1										X				
FAU_SAR.1						X								
FAU_STG.1	X						X	X			X			
FCS_BCM_EXP.1													X	X
FCS_CKM.1													X	X
FCS_CKM.4													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.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED
FCS_COP_EXP.1													X	X
FCS_COP_EXP.2(1)													X	X
FCS_COP_EXP.2(2)													X	X
FIA_ATD.1								X						
FIA_UAU.1							X	X						
FIA_UID.1							X	X						
FMT_MOF.1	X						X	X						
FMT_MSA.2						X								
FMT_MTD.1(1)	X						X	X			X			
FMT_MTD.1(2)						X								
FMT_SMF.1(1)	X						X	X			X			
FMT_SMF.1(2)	X					X	X	X						
FMT_SMR.1								X						
FPT_ITC.1											X	X		
FPT_ITI.1											X	X		
FPT_ITT.1											X	X		
FPT_RVM.1(1)	X					X		X		X	X			
FPT_SEP.1(1)	X					X		X		X	X			
FPT_STM_EXP.1										X				
IDS_ANL_EXP.1				X										
IDS_RCT_EXP.1					X									
IDS_RDR_EXP.1						X	X	X						
IDS_SDC_EXP.1		X	X											
IDS_STG_EXP.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 prevent unauthorized modifications to the audit data [FAU_STG.1]. The System 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_EXP.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized users of the System may query and clear System and audit data, and authorized users of the TOE may modify and delete System data [FMT_MTD.1(1)]. The TOE must ensure that all functions are invoked and succeed before each function may

proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)]. FMT_SMF.1(1) and (2) support this objective by identifying the corresponding management functions.

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 System containing a Scanner is required to collect and store static configuration information of an IT System.[IDS_SDC_EXP.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 System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System [IDS_SDC_EXP.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_EXP.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_EXP.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 the audit trail of the System [FAU_SAR.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR_EXP.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)]. FMT_MSA.2 provides the administrators the ability to accept only secure values and modify security attributes. FMT_MTD.1(2) helps satisfy this objective by providing that there be a management function of the Security Administrator or an authorized IT entity that will set the time and date used to provide reliable time stamps to the TOE. FMT_SMF.1(2) supports this objective by identifying the corresponding management functions.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR_EXP.1]. The TOE is required to protect the audit data from deletion as well as prevent unauthorized modifications of the audit data [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG_EXP.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and clear System and audit data, and authorized administrators of the TOE may modify and delete System data [FMT_MTD.1(1)]. FMT_SMF.1(1) and (2) support this objective by identifying the corresponding management functions.

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

The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR_EXP.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.1]. The System 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_EXP.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.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized users of the System may query and clear System and audit data, and authorized users of the TOE may modify and delete System data [FMT_MTD.1(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 [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)]. FMT_SMF.1(1) and (2) support this objective by identifying the corresponding management functions.

O.OFLOWS The TOE must appropriately handle potential System data storage overflows. The System 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 [IDS_STG_EXP.1].

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 ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)]. Time stamps associated with an audit record must be reliable [FPT_STM_EXP.1].

O.INTEGR The TOE must ensure the integrity of all audit and System data. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG_EXP.1]. Only authorized users of the System may query and clear System and audit data, and authorized users of the TOE may modify and delete System data [FMT_MTD.1(1)]. The System must protect the collected data from modification, disclosure, and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1], or a separate part of the TOE [FPT_ITT.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1(1)]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1(1)]. FMT_SMF.1(1) supports this objective by identifying the corresponding management functions.

O.EXPORT When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data. The TOE must protect all data from modification, disclosure, and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1], or a separate part of the TOE [FPT_ITT.1].

O.CRYPTO The FCS requirements satisfy this objective by levying requirements that ensure

GRAPHY the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-1/2 validation. FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensively the module is tested. FCS_CKM.1 ensures that, if necessary, the TOE is capable of generating cryptographic keys. FCS_CKM.4 mandates the standards (FIPS 140-1/2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. FCS_COP_EXP.1 requires that a NIST approved random number generator is used. FCS_COP_EXP.2(1) and FCS_COP_EXP.2(2) require for data decryption and encryption that a NIST approved algorithms are used, and that the algorithms meet the FIPS PUB 140-1/2 standard.

O.CRYPTO GRAPHY_ VALIDATED The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-1/2 validation. FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensively the module is tested. FCS_CKM.1 ensures that, if necessary, the TOE is capable of generating cryptographic keys. FCS_CKM.4 mandates the standards (FIPS 140-1/2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. FCS_COP_EXP.1 requires that a NIST approved random number generator is used. FCS_COP_EXP.2(1) and FCS_COP_EXP.2(2) require for data decryption and encryption that a NIST approved algorithms are used, and that the algorithms meet the FIPS PUB 140-1/2 standard.

8.4 Rationale for TOE IT Environment Security Requirements

This section demonstrates that the functional components selected for the TOE IT Environment provide complete coverage of the defined TOE IT Environment security objectives. The mapping of components to security objectives is depicted in the following table

Table 16: Requirements vs. Objectives Mapping

	OE.TIME_STAMPS	OE.SELF_PROTECTION
FPT_RVM.1(2)		X
FPT_SEP.1(2)		X
FPT_STM.1	X	

OE.TIME_STAMPS

[FPT_STM.1] requires that the TOE IT environment be able to provide reliable time stamps for its own use and that of the TOE. Time stamps include date and time and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.

OE.SELF_PROTECTION

The TOE IT environment must protect itself in a manner similar to that provided for the TOE. [FPT_SEP.1(2)] ensures the environment provides a domain that protects itself from untrusted users. If the environment cannot protect itself it cannot be relied upon to enforce its security policies. [FPT_RVM.1(2)] ensures that the environment makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies.

8.5 Rationale for Assurance Requirements

EAL2 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 System 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 EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.6 Rationale for Satisfying all Dependencies

Each functional requirement, including explicit requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. With the exception of dependencies related to FMT_MSA.2, all dependencies in this ST have been satisfied. FMT_MSA.2 is included in this ST as a dependency of the Cryptographic Support family (FCS_COP and FCS_CKM). It is used there to ensure that security attributes related to cryptographic objects (e.g. cryptographic keys) are protected. However, FMT_MSA family is also used to ensure the protection of security attributes related to access control policies (FDP_IFC and FDP_AFC) and includes a dependency upon those Security Functional Requirements. However, this ST does not require that the TOE implement an access control policy and those requirements have not been included in the ST.

8.7 Rationale for Explicitly Stated Requirements

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

Table 17 presents the rationale for the inclusion of the remaining explicit requirements found in this ST.

Table 17: Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale
FCS_BCM_EXP.1	Baseline cryptographic module	This explicit requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.
FCS_COP_EXP.1	Random number generation	This explicit requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes. FCS_COP_EXP.1 requires FIPS approved random number generation to be used for all cryptographic functionalities, while FCS_CKM.1 is limited to cryptographic key generation.
FCS_COP_EXP.2	Cryptographic Operation	This explicit requirement is necessary because it describes requirements for a cryptomodule rather than the entire TSF.

8.8 Rationale for Strength of Function

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in this ST.

Password-based authentication mechanisms (via serial console and GUI) have the following specific SOF claims:

Shared key: administrators authenticate to sensors locally using the shared key. The shared key must be at least 6 characters and at most 36 characters in length. Characters 32 to 126 of the ASCII character set can be used in the password. This yields a minimum of 95^6 (over 735 billion) possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000. The possibility of randomly guessing the shared key in 60 seconds is less than 1 in 100,000 as the shared key is entered via the 115,200 bit per second serial port and the minimum shared key length is 6 characters.

User password: users and administrators authenticate remotely using a password that is at least 6 characters and at most 36 characters. Characters 32 to 126 of the ASCII character set can be used in the password. This yields a minimum of 95^6 (over 735 billion) possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000. The possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000 due to the performance limitation of the embedded web server that is used to enter the password.

8.9 TOE Summary Specification Rationale

Rationale for security functions is presented in Section 6.2.

9 Acronyms

CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions