McAfee Corporation's Vulnerability Manager Version 6.8 Security Target

Version 2.4

January 11, 2011

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

DOCUMENT INTRODUCTION

Prepared By:	Prepared For:
Common Criteria Consulting LLC 15804 Laughlin Lane Silver Spring, MD 20906 http://www.consulting-cc.com	McAfee, Inc. 3965 Freedom Circle Santa Clara, CA 95054 http://www.mcafee.com

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the McAfee Vulnerability Manager Version 6.8. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

AD	**Active Directory**
ADO	**ActiveX Data Objects**
API	**Application Program Interface**
CC	**Common Criteria**
CCE	**Common Configuration Enumeration**
CM	**Configuration Management**
CPE	**Common Platform Enumeration**
CVE	**Common Vulnerabilities and Exposures**
CVSS	**Common Vulnerability Scoring System**
DBMS	**DataBase Management System**
DNS	**Domain Name System**
EAL	**Evaluation Assurance Level**
ePO	**ePolicy Orchestrator**
FDCC	**Federal Desktop Core Configuration**
GUI	**Graphical User Interface**
I&A	**Identification & Authentication**
ICMP	**Internet Control Message Protocol**
IDS	**Intrusion Detection System**
IIS	**Internet Information Services**
IP	**Internet Protocol**
IPS	**Intrusion Prevention System**
IT	**Information Technology**
LDAP	**Lightweight Directory Access Protocol**
MAC	**Media Access Control**
MDAC	**Microsoft Data Access Components**
NTFS	**New Technology File System**
NTLM	**NT LAN Manager**
OS	**Operating System**
OVAL	**Open Vulnerability Assessment Language**
PP	**Protection Profile**
RAM	**Random Access Memory**
SCAP	**Security Content Automation Protocol**
SF	**Security Function**
SFR	**Security Functional Requirement**
SOAP	**Simple Object Access Protocol**
SP	**Service Pack**
SQL	**Structured Query Language**
SSL	**Secure Socket Layer**
ST	**Security Target**
TCP	**Transmission Control Protocol**
TOE	**Target of Evaluation**
TSF	**TOE Security Function**
TSFI	**TSF Interface**
UDP	**User Datagram Protocol**
XCCDF	**eXtensible Configuration Checklist Description Format**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the McAfee Vulnerability Manager Version 6.8 (formerly known as Foundstone Enterprise). The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation*, *Version 3.1*and all international interpretations through December 19, 2008. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

McAfee Corporation's Vulnerability Manager Version 6.8 Security Target, version 2.4, January 11, 2011.

1.2 TOE Reference

McAfee Vulnerability Manager Version 6.8

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 (Flaw Reporting Procedures) from the *Common Criteria for Information Technology Security Evaluation,* Version 3.1 Revision 3.

1.4 Keywords

Vulnerability, vulnerability management, vulnerability assessment, vulnerability scanner, risk management, auditing, policy auditing, compliance, compliance auditing, SOX, FISMA, HIPAA, PCI DSS, SCAP, FDCC, scanner, configuration scanner.

1.5 TOE Overview

1.5.1 Usage and Major Security Features

The TOE is a Vulnerability Management System that scans specified targets for vulnerabilities and mis-configurations. It provides a management interface to configure the system and generate reports regarding the results of the scans.

The TOE consists of the following components:

1. The Enterprise Manager provides authorized users with access to the TOE through their Web browsers. It allows them to manage and run the TOE from anywhere on the network. Access is protected by user identification and authentication.
2. One or more Scan Engines scan the network environment. Depending on the logistics and size of your network, you may need more than one Scan Engine to scan the network. The Scan Engine performs identification, interrogation, and vulnerability assessment of remote computer systems.
3. The API Service provides an interface for Enterprise Manager to store data into and retrieve data from the Foundstone Database. This interaction uses SOAP over SSL.
4. The Data Sync Service enables Vulnerability Manager to import asset information from McAfee's ePolicy Orchestrator (ePO) enterprise management system or an LDAP directory such as Microsoft Active Directory. This integration permits Vulnerability Manager to learn about assets through a mechanism other than discovery scans.

5. The Foundstone Database is the data repository for the Vulnerability Manager system. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and Scan Engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and generate reports.
6. The Report Server is responsible for generating reports requested by authorized users. It retrieves scan results from the Foundstone Database, prepares the report, and saves it for future review.

All communication between distributed components uses a trusted channel to protect the integrity and confidentiality of the data during transit. The TOE depends on cryptographic and protocol functionality provided by the IT environment for these secure channels.

1.5.2 TOE Type

IDS/IPS

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

The platform on which the Enterprise Manager software is installed must be dedicated to functioning as the Enterprise Manager. The TOE requires the following hardware and software configuration on this platform.

Table 1 - Enterprise Manager Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows Server 2003 SP2 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	IIS 6.0 Current IIS security patches World Wide Web Publishing must be running OpenSSL v1.2 PHP v5.2.1
Network Card	Ethernet
Disk Partition Formats	NTFS

The platform on which the Scan Engine software is installed must be dedicated to functioning as a Scan Engine, with the exception of the Primary Scan Engine also providing the API Service and Data Sync Service. The TOE requires the following hardware and software configuration on this platform.

Table 2 - Scan Engine Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows Server 2003 SP2 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	MDAC 2.8 SQL Client Tools (for Microsoft SQL Server 2005) OpenSSL v1.2 PuTTY SSH Client v0.60jo Microsoft Windows Script 5.6
Network Card	Ethernet
Virtual Memory	2.0 GB
Disk Partition Formats	NTFS
Required Services	NetBIOS over TCP/IP Print Spooler

The platform on which the Foundstone Database and Report Server are installed must be dedicated to functioning as the servers for these functions of the TOE. The DBMS is installed on this same platform. The TOE requires the following hardware and software configuration on this platform.

Table 3 - Foundstone Database/Report Server Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows Server 2003 SP2 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	Microsoft SQL Server 2005 SP1and all SQL hotfixes/patches
Network Card	Ethernet
Virtual Memory	2.0 GB
Disk Partition Formats	NTFS
SQL Server Memory Settings	900MB
Required Services	n/a

Authorized users can access the Enterprise Manager through their Web browser software. The TOE supports Microsoft Internet Explorer 6.0 and higher, running on a Windows operating system. Latest service packs should be applied to both your browser and operating system. The security updates in Microsoft Knowledge Base MS06-013 must be applied to the client browser. Recommended minimum screen resolution is 1024 x 768.

1.6 TOE Description

McAfee Vulnerability Manager helps organizations identify and protect their assets by detecting vulnerabilities on those assets. This solution allows managers to continuously monitor, respond to, and adjust to a changing risk environment.

Administrators configure the system, including user accounts. Users schedule discovery scans to identify the systems on the network, followed by assessment scans to determine the vulnerabilities.

1.6.1 Physical Boundary

The physical boundary of the TOE includes:

1. The Enterprise Manager application
2. The Scan Engine application software on each Scan Engine
3. The API Service application on the Primary Scan Engine
4. The Data Sync Service application on the Primary Scan Engine
5. The database on the Foundstone Database system
6. The Report Server application on the Foundstone Database system

Note specifically that the hardware, operating systems and third party support software (e.g., IIS and SQL Server) on each of the systems are excluded from the TOE boundary.

1.6.2 Logical Boundary

The logical boundaries of the TOE are defined by the functions provided by the TOE and are described in the following sections.

1.6.2.1 Scanning

The TOE scans designated systems to detect known vulnerabilities on those systems. Results of the scans are stored in the database (the DBMS is in the IT Environment), and reports based upon completed scans may be retrieved via the GUI interface of the Enterprise Manager.

1.6.2.2 Identification and Authentication (I&A)

The TOE requires users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

When interacting with the TOE via the Enterprise Manager GUI, I&A is performed by the TOE. On all three component systems, I&A for local login to the operating system (i.e., via a local console) is performed by Windows (IT Environment).

1.6.2.3 Management

The TOE’s Management Security Function provides administrator support functionality that enables a human user to configure and manage TOE components.

Management of the TOE may be performed via the Enterprise Manager. All user types may use the Enterprise Manager.

The TOE provides the following management functions:

1. User management,
2. Root organization management,
3. Workgroup management,
4. Scan Engine management,
5. Asset management,
6. Scan management,
7. Report management,
8. Known vulnerability management.

1.6.2.4 Audit

The TOE's Audit Security Function provides auditing of management actions performed by administrators.

1.6.2.5 Asset Data Import

The TOE may be configured to import data about assets from LDAP servers or McAfee ePO. The value of this functionality is that the information about the assets may be more accurate or complete than the information obtained from scans.

1.6.3 TSF Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the TOE to enforce the security policy. Authentication data enables the TOE to identify and authenticate users.

Table 4 - TOE Data

TSF Data	Description	AD	UA	GE
Asset groups	Grouping of assets for ease of configuring parameters and association with scans.			X
Assets	Systems that have been discovered by the TOE during scans.			X
Data Sources	LDAP and/or ePolicy Orchestrator servers from which asset information may be imported. Configuration of data sources is an installation activity only; synchronization updates occur during TOE operation.			X
Scan Engines configuration	Parameters associated with each Scan Engine, such as which root organization it will perform scans for			X
Reports	Reports are launched to generate information regarding the results of a specific scan and may be viewed once generated			X
Report Templates	Report templates define the information that will be included in reports as well as the frequency at which the reports are generated.			X

TSF Data	Description	AD	UA	GE
Root Organizations	The top level organization of items within the TOE. All items associated with one root organization are shielded from all other root organizations			X
Scans	Parameters that define the scanning actions to be performed by the TOE and permissions relevant to each scan granted to Foundstone Users			X
User Accounts	Root Organization, Username and password for each individual user that connects to the TOE via the Enterprise Manager web interface.	X		
User groups	Grouping of users for ease of configuring parameters and association with workgroups.		X	
User roles	The administrator type for each individual user that connects to the TOE via the Enterprise Manager web interface.		X	
Known Vulnerabilities	List of known vulnerabilities that can be associated with individual scans.			X
Workgroups	One or more levels of hierarchy under root organizations that permit access restrictions to be defined for scans and reports.			X

Legend: AD=Authentication data; UA=User attribute; GE=Generic Information

1.7 Evaluated Configuration

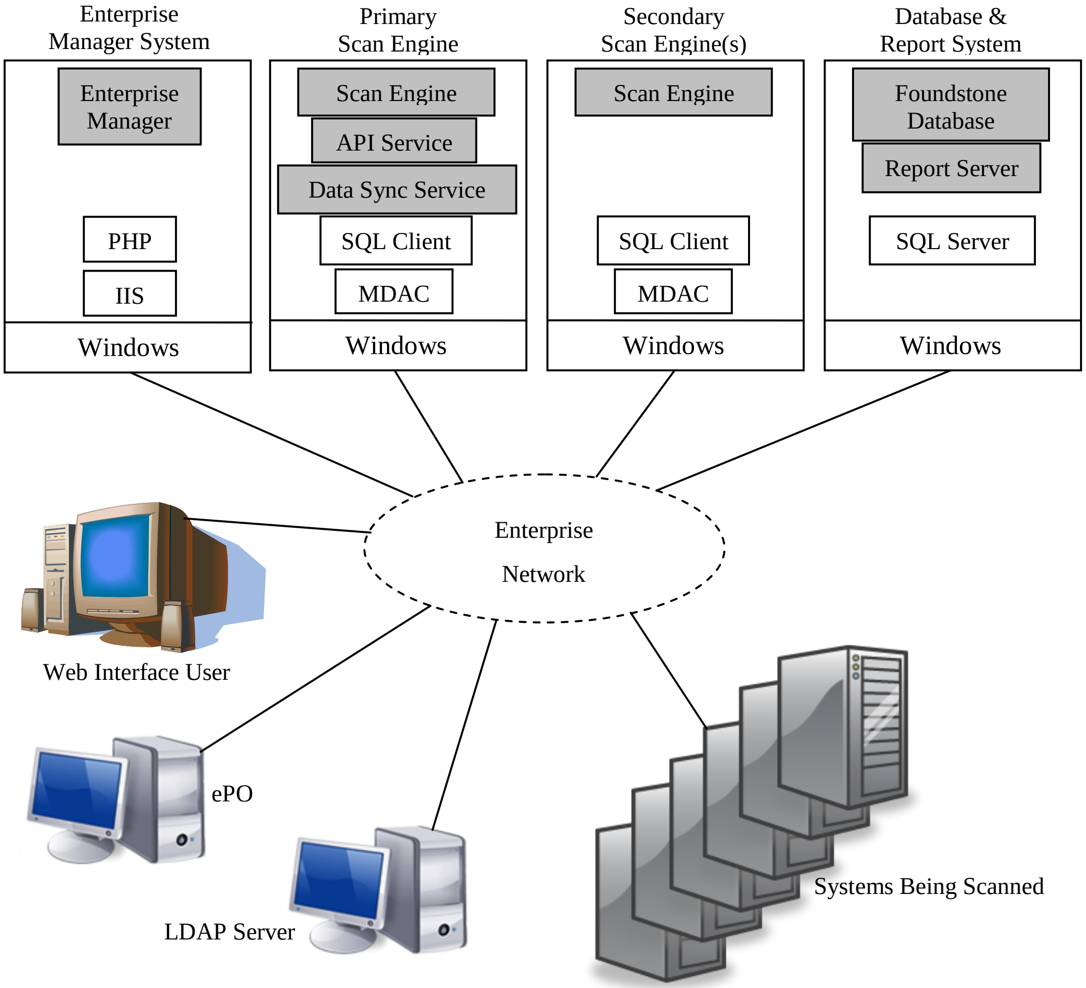
The TOE is evaluated in a Distributed Server Architecture. This architecture is appropriate for complex organizations where large disparate networks in multiple geographical regions may require multiple Scan Engines. The scan engines generate all scanning traffic on their local network segments, then send the resulting scan data to the Foundstone Database. During the installation of each component, custom certificates are installed for use with the SSL protocol that protects traffic between the components.

In this architecture the following components exist:

1. One instance of Enterprise Manager on a dedicated platform
2. One instance of Scan Engine, API Service and Data Sync Service on a dedicated platform (Primary Scan Engine)
3. Zero or more instances of Scan Engine on additional dedicated platforms (secondary scan engines)
4. One instance of the Foundstone Database and Report Server hosted on a separate dedicated platform (together with the DBMS)

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.

Figure 1 - Typical Vulnerability Manager Configuration



The following configuration options are required in the evaluated configuration:

1. Root Organization Administrators are not permitted to switch to Global Administrator access (the user must log out and log back in as a Global Administrator)

The following items are excluded from the evaluation:

1. Remediation management and tickets – this is optional functionality requiring the purchase of an additional license. Not evaluated in the evaluated configuration.
2. Notification service - this is optional functionality requiring the purchase of an additional license. Not evaluated in the evaluated configuration.

1.8 Rationale for Non-Bypassability and Separation

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied OSs.

Non-bypassability

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. All systems on which the TOE executes are dedicated systems.

Non-interference

The TOE is implemented with well defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple administrators by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components uses secure channels to protect the information exchanged from disclosure or modification. The secure channels rely upon cryptographic functionality provided by the OS or third party software.

2. Conformance Claims

2.1 Common Criteria Conformance

The McAfee Vulnerability Manager Version 6.8 is compliant with the Common Criteria (CC) Version 3.1 Revision 3, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL2 and augmented by ALC_FLR.2 (Flaw Reporting Procedures).

2.2 Protection Profile Conformance

The McAfee Vulnerability Manager Version 6.8 does not claim conformance to any registered Protection Profile.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 5 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
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.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.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.ALARM	The DBMS will generate an alarm if storage space in the database is exhausted.

3.3 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also 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.

The following table identifies threats to the TOE.

Table 6 - TOE Threats

T.Type	TOE Threats
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.Type	TOE Threats
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.
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.

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

Table 7 - IT System Threats

T.Type	IT System Threats
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.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of data received from all data sources.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.FALACT	Issues resulting from scans of monitored systems may fail to be acted upon because the information is not disseminated from the TOE to other IT systems that are responsible for tracking or correcting the issues.

3.4 Organisational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 8 - Organizational Security Policies

P.Type	Organizational Security Policy
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 data received from data sources 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.INTGTY	Data collected and produced by the TOE shall be protected from modification.

P.Type	Organizational Security Policy
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 9 - Information Technology (IT) Security Objectives

Objective	Definition
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
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.
O.IDANLZ	The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
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 System data storage overflows.
O.INTEGR	The TOE must ensure the integrity of all System data.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.IMPORT	The TOE shall provide mechanisms to import data about assets from LDAP servers and ePO.
O.SCAP	The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.

4.2 Security Objectives for the Operational Environment

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

Table 10 - Security Objectives of the Environment

Objective	Definition
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 System.
OE.INTROP	The TOE is interoperable with the IT System it monitors
OE.TIME	The IT Environment will provide reliable timestamps to the TOE
OE.PROTECT	The IT environment will protect itself and the TOE from external

Objective	Definition
	interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to the TOE allowing access to TOE functions and data on the Scan Engine.
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information generated by the TOE.
OE.AUDIT_REVIEW	The IT environment will provide the capability to review audit information generated by the TOE.
OE.CRYPTO	The IT Environment will provide the cryptographic functionality and protocols required for the implementation of secure channels between the TOE components and between the TOE and external IT systems.
OE.ALARM	The DBMS will generate an alarm if storage space in the database is exhausted.

5. Extended Components Definition

5.1 Extended Security Functional Components

All of the components in this section are taken from the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

IDS_STG.2.1 has been modified from the PP to delete the text "and send an alarm". An alarm is sent by the DBMS, which is part of the operational environment. Therefore, that portion of the SFR from the PP has been deleted but is addressed by A.ALARM and OE.ALARM.

5.1.1 IDS_SDC.1 System Data Collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) [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

b) [assignment: *other specifically defined events*].

IDS_SDC.1.2 At a minimum, the System 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 **the table below**.

Table 11 - System Data Collection Events and Details

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	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 policy parameters

Component	Event	Details
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Management:

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

a) Configuration of the events to be collected.

Audit:

There are no auditable events foreseen.

5.1.2 IDS_ANL.1 Analyser analysis

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC.1 System Data Collection

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

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

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

IDS_ANL.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. [assignment: *other security relevant information about the result*].

Management:

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

a) Configuration of the analysis to be performed.

Audit:

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

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

5.1.3 IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection

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

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

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

Management:

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

a) maintenance (deletion, modification, addition) of the group of users with read access right to the system data records.

Audit:

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

a) Basic: Attempts to read system data that are denied.

b) Detailed: Reading of information from the system data records.

Application Note: The audit event definition is consistent with CCEVS Policy Letter #15, which states that only access failures are auditable at the Basic level of audit.

5.1.4 IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection

IDS_STG.2.1 The System shall [selection: *'ignore System data'*, *'prevent System data, except those taken by the authorised user with special rights'*, *'overwrite the oldest stored System data'*] if the storage capacity has been reached.

Management:

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

a) maintenance (deletion, modification, addition) of actions to be taken in case system data storage capacity has been reached.

Audit:

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

a) Basic: Actions taken if the storage capacity has been reached.

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

Explicitly stated requirements are included in this ST. The names of these requirements start with IDS_.

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

The functional security requirements for the TOE consist of the following components, summarized below.

Table 12 - TOE SFRs

Functional Components	
FAU_GEN.1	Audit Data Generation
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_TDC.1	Inter-TSF Basic TSF Data Consistency
IDS_SDC.1	System Data Collection
IDS_ANL.1	Analyzer analysis
IDS_RDR.1	Restricted Data Review
IDS_STG.2	Prevention of System data loss

6.1.1 5.1.1 Security Audit (FAU)

6.1.1.1 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 not specified level of audit; 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 information detailed in the following table*.

Table 13 - TOE SFRs

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FIA_UAU.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, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_TDC.1	Successful use of TSF data consistency mechanisms	Data Source
IDS_ANL.1	None (the analysis function is always enabled)	
IDS_RDR.1	None (the user is not given the option of accessing unauthorized system data)	
IDS_STG.2	None (a common database is used for system data and audits; if the database is full, all new information is discarded)	

6.1.2 Identification and authentication (FIA)

6.1.2.1 FIA_ATD.1 User Attribute Definition

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

a) *Login name;*

b) *Password;*

c) *User role;*

d) *Lock status;*

e) *Organization;*

f) *Workgroup membership;*

g) *Group membership and*

h) *Scan permissions.*

6.1.2.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet *the following metrics:*

a) Contains at least 8 characters

b) Contains at least one number

c) *Contains at least one non-alpha-numeric character (`~!@#$%^&*()-_=+).*

6.1.2.3 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow *no actions* 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.

6.1.2.4 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* 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.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions *of System data collection and analysis* to *Foundstone Users with permissions for specific scans, Global Administrators, Root Organization Administrators and Workgroup Administrators*.

6.1.3.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query *and add System data*, **and shall restrict the ability to query and modify all other TOE data** to *the roles associated with specific data and operations as shown in the following table*.

Table 14 - TSF Data Access Permissions

TSF Data	Global Administrator	Root Organization Administrator	Workgroup Administrator	Foundstone User
Asset groups	None	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
Assets	None	Modify properties within the same root organization	Modify properties within the workgroups	None
Data Sources	None	Performed during installation only	None	None
Known Vulnerabilities	Create, Delete, Modify	None	None	None
Scan Engines	Modify properties	Modify properties within the same root organization	None	None
Reports	None	Submit or Cancel within the same root organization	Report access is determined by the access permissions listed below	Report access is determined by the access permissions listed below
Report Templates	None	View and Edit within the same root organization	Report access is determined by the access permissions listed below	Report access is determined by the access permissions listed below
Root Organizations	Create, Delete, Modify properties	Modify properties	None	None
Scans	View status	Create, Delete, Modify properties, Launch within the same root organization	Create, Delete, Modify properties, Launch within the workgroups	Scan access is determined by the access permissions listed below
User Accounts	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	Modify the user’s own password
User groups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
User roles	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
Workgroups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None

Table 15 - Scan/Report Access Permissions

Scan Access	Description
View	View the reports, templates and other information displayed in the Enterprise Manager for the selected scan. Reports may be submitted and canceled for any reports for which the user has View access.
Edit IP	Allow the user or group to edit the IP ranges for the selected scan.
Edit Body	Allow the user or group to edit the selected scan's settings, other than the IP ranges and schedule.
Schedule	Allow the user or group to change the times when the selected scan is scheduled to run.
Delete	Allow the user or group to delete the selected scan.
Full	All of the above. Allow the user or group to edit, launch, or delete any scan in the organization or workgroup.

6.1.3.3 FMT_SMF.1 Specification of Management Functions

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

1) *User management,*

2) *Root organization management,*

3) *Workgroup management,*

4) *Asset management,*

5) *Scan management,*

6) *Report management,*

7) *Scan Engine management,*

8) *Known vulnerability management*.

6.1.3.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles*: Foundstone User, Root Organization Administrator, Workgroup Administrator, and Global Administrator*.

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

6.1.4 Protection of the TSF (FPT)

6.1.4.1 FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1(1) The TSF shall provide the capability to consistently interpret *assets* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2(1) The TSF shall use *the following rules* when interpreting the TSF data from another trusted IT product.

1) *For LDAP servers, the data is interpreted according to the LDAP version 3 protocol.*

2) *For EPO, the data is interpreted according to McAfee's schema for the ePO database.*

3) *When conflicting information is received from different sources, highest priority is given to ePO data, then to LDAP server data.*

FPT_TDC.1.1(2) The TSF shall provide the capability to consistently interpret *known vulnerabilities* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2(2) The TSF shall use *the SCAP Benchmark Assessment XCCDF and OVAL standards* when interpreting the TSF data from another trusted IT product.

6.1.5 IDS Component Requirements (IDS)

Rationale for explicitly stated SFR: This family of IDS requirements is copied from the IDS System PP to specifically address the data collected and analysed 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 system 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.

6.1.5.1 IDS_SDC.1 System Data Collection

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

a) access control configuration, service configuration, authentication configuration, detected known vulnerabilities and

b) *no other events*.

IDS_SDC.1.2 At a minimum, the System 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 **the table below**.

Table 16 - System Data Collection Events and Details

Component	Event	Details
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 policy parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Application Note: Access control configuration refers to configuration settings used to restrict access for individual users/roles. Service configuration refers to services made available to users via the network interface and protocol stack. Authentication configuration refers to settings regarding password content parameters and authentication attempts.

6.1.5.2 IDS_ANL.1 Analyser analysis

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

a) signature; and

b) *the following analytical functions: operating system identification, registry queries (when credentials are provided), and positive and negative responses to packets transmitted to the scanned systems*.

IDS_ANL.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. *Criticality of the asset on which the vulnerability was detected*

c. *Risk factor of the detected vulnerability*.

6.1.5.3 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The System shall provide *Foundstone User, Root Organization Administrator and Workgroup Administrator* with the capability to read *the system data listed in the table below* from the System data.

Table 17 - System Data Access

User Type	Access
Foundstone User	System data associated with specific scans they are authorized to view
Workgroup Administrator	System data associated with all workgroups the Workgroup Administrator is associated with
Root Organization Administrator	System data associated with all scans in the same root organization

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

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

6.1.5.4 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall ignore System data if the storage capacity has been reached.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 18 - EAL2 Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system

Assurance Class	Component ID	Component Title
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw Reporting Procedures
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

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 19 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No Other Components	FPT_STM.1	Satisfied by the IT Environment (OE.TIME)
FIA_ATD.1	No Other Components	None	N/A
FIA_SOS.1	No Other Components	None	N/A
FIA_UAU.1	No Other Components	FIA_UID.1	Satisfied
FIA_UID.1	No Other Components	None	N/A
FMT_MOF.1	No Other Components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No Other Components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No Other Components	None	N/A
FMT_SMR.1	No Other Components	FIA_UID.1	Satisfied
FPT_TDC.1	No Other Components	None	N/A
IDS_SDC.1	No Other Components	FPT_STM.1	Satisfied by the IT Environment (OE.TIME)
IDS_ANL.1	No Other Components	FPT_STM.1 IDS_SDC.1	Satisfied by the IT Environment (OE.TIME) Satisfied
IDS_RDR.1	No Other Components	IDS_SDC.1	Satisfied
IDS_STG.2	No Other Components	IDS_SDC.1	Satisfied

7. TOE Summary Specification

7.1 Scanning

The TOE performs scanning of designated systems to detect known vulnerabilities on those systems. In order to be able to delegate management of this process to appropriate levels, the TOE supports a hierarchical organization consisting of one or more root organizations and one or more levels of subordinate workgroups. Root organizations are hidden from each other; administrators and users can only view the scans and data that pertain to the organization to which they belong.

Associated with each root organization or workgroup are users, groups, scans, IP addresses, and scan engines. The IP addresses for subordinate levels (e.g., workgroups within root organizations) must be subsets of the IP addresses defined for the higher levels. The scan engines for subordinate levels must also be subsets of the scan engines defined for the higher levels.

Scans may be defined for root organizations or workgroups. A scan includes a list of IP addresses to be scanned, parameters concerning the types of network and service scanning to be performed, the time and frequency at which the scan should be executed, and the vulnerabilities to be scanned for. On a per-scan basis, credentials may be defined for logons to the scanned systems for more in-depth scanning.

Scan timing may be either on-demand or scheduled to run at a later time. On-demand scans are intended to be run ad-hoc and are launched manually by the administrator when needed. Scheduled scans are intended to be run at specific a date and time in the future. Scheduled scans will run automatically based on the schedule set by the administrator.

As scans are performed, details about systems within the designated address list are learned. As new systems are discovered during a scan, they are listed as assets. The assets may be associated with one or more scans for future scanning.

Scan results rely upon signature comparisons as well as other analytical functions. For example, when scanning for service configurations, results are determined from responses received as well as the absence of responses. In addition, the responses to multiple packets sent to the scanned systems are used to attempt operating system identification, which enables finer-grained scanning. If login credentials are provided for an asset, access control settings and authentication configuration settings available via remote login (i.e., registry settings) are analyzed.

Results of the scans are stored in the database. The information included with the results are the name of the scan, the time and date the scan was executed, the name of the asset scanned, the criticality of the asset, vulnerabilities detected on each asset, and the risk factor associated with any detected vulnerabilities. Administrators are advised to purge old scan data from the database on a periodic basis and to configure the database to expand in size as necessary up to the limits of the file system. In the unlikely event storage space exhaustion does occur, the TOE discards the most recent results.

Vulnerability Manager supports benchmark scans utilizing all six of the SCAP standards - CVE, CPE, CCE, CVSS, XCCDF, and OVAL - as well as direct import off SCAP data-feeds. Therefore, systems can be assessed using open community-developed security benchmarks and content, including FDCC benchmarks for Windows XP, Windows Vista, Internet Explorer 7, and more. Benchmark assessment inputs and outputs fully meet SCAP requirements, allowing the results to be used to monitor and audit compliance in accordance with regulatory mandates and other customer requirements.

Reports may be generated from the scan results. Reports may be produced in human readable form or as SCAP-conformant XML files suitable for exchange with other systems. Reports may be viewed according to the following restrictions:

Table 20 - Report Access

User Type	Access
Foundstone User	Reports for specific scans they are authorized to view
Workgroup Administrator	Reports for all scans associated with workgroups the administrator is associated with
Root Organization Administrator	Reports for all scans in the same root organization

7.2 Identification and Authentication (I&A)

The TOE enables an authorised user to manage the TOE via a web interface on the Enterprise Manager. The TOE requires users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication.

Each user of the web interface has a root organization, user identity, user password and role associated with their user account. The role defines the functionality the user is allowed to perform. If the role is Workgroup Administrator or Foundstone User, the user also has associations with workgroups within the root organization.

Authentication is required (cannot be bypassed) and the password is configured when the user account is created. The TOE implements restrictions on the passwords:

1) Contains at least 8 characters
2) Contains at least one number
3) Contains at least one non-alpha-numeric character (`~!@#$%^&*()-_=+)

The TOE also protects the password from visual detection by echoing back asterisks (“*”) for the entered passwords.

7.3 Management (MGMT)

The TOE’s Management Security Function provides administrator support functionality that enables a human user to configure and manage TOE components.

Management of the TOE may be performed via the Enterprise Manager. All user types may use the Enterprise Manager.

The TOE provides the following management functions:

1. User management,
2. Root organization management,
3. Workgroup management,

4. Scan Engine management,
5. Asset management,
6. Scan management,
7. Report management,
8. Known vulnerability management.

7.3.1 User Management

Each User Account must be defined to the TOE. In addition to a login name and password, a user includes the following security attributes: user role, lock status (whether the account is administratively enabled), organization, workgroup membership, group membership and scan permissions. A role may be any of the following: Global Administrator, Root Organization Administrator, Workgroup Administrators, or Foundstone User. User Accounts may be associated with one or more groups, which may be used to assign permissions to all members of a group rather than individual users. The purpose of each role is described in the following table.

Table 21 - Role Descriptions

Role	Description
Global Administrator	The Global Administrator sets up the top-level organization(s), and creates an administrator for the organization(s). The Global Administrator can also set up workgroups under an organization, and can create users and user groups. The Global Administrator can also move top-level organizations to become workgroups under other organizations.
Root Organization Administrator	The Root Organization Administrator can manage assets, scan configurations, user accounts, and scan engines. These administrators also have full access to any workgroups created under their organization. The Root Organization Administrator manages the Scan Engine settings from the Enterprise Manager.
Workgroup Administrators	The Workgroup Administrator can manage assets, scan configurations, and user accounts. These administrators also have full access to any workgroups created under their workgroup.
Foundstone User	Each Foundstone User is granted access to scans. Users are associated with an organization and may be granted access to any or all workgroups within that organization, and any or all scans defined for that organization. Scan access is configurable per scan.

Administrative capabilities for each role are described in the following table.

Table 22 - Administrative Capabilities

TSF Data	Global Administrator	Root Organization Administrator	Workgroup Administrator	Foundstone User
Asset groups	None	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None

TSF Data	Global Administrator	Root Organization Administrator	Workgroup Administrator	Foundstone User
Assets	None	Modify properties within the same root organization	Modify properties within the workgroups	None
Data Sources	None	Performed during installation only	None	None
Known Vulnerabilities	Create, Delete and Modify	None	None	None
Scan Engines	Modify properties	Modify properties within the same root organization	None	None
Reports	None	Submit or Cancel within the same root organization	Report access is determined by the access permissions listed below	Report access is determined by the access permissions listed below
Root Organizations	Create, Delete, Modify properties	Modify properties	None	None
Scans	View status	Create, Delete, Modify properties, Launch within the same root organization	Create, Delete, Modify properties, Launch within the workgroups	Scan access is determined by the access permissions listed below
User Accounts	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	Modify the user's own password
User groups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
User roles	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
Workgroups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None

Foundstone Users may be associated with one or more groups within a root organization, or with a root organization as a whole. Scan access for Foundstone Users may be any of the following:

Table 23 - Scan/Report Access Descriptions

Scan Access	Description
View	View the reports, templates and other information displayed in the Enterprise Manager for the selected scan. Reports may be submitted and canceled for any reports for which the user has View access.

Scan Access	Description
Edit IP	Allow the user or group to edit the IP ranges for the selected scan.
Edit Body	Allow the user or group to edit the selected scan's settings, other than the IP ranges and schedule.
Schedule	Allow the user or group to change the times when the selected scan is scheduled to run.
Delete	Allow the user or group to delete the selected scan.
Full	All of the above. Allow the user or group to edit, launch, or delete any scan in the organization or workgroup.

7.3.2 Root Organization Management

Root organizations are configured by the Global Administrator. The IP addresses and scan engines available to the root organization are part of this configuration. When a root organization is created, a single Root Organization Administrator must also be defined.

Root Organization Administrators may configure users, groups and scans within their root organization. Root Organization Administrators, Workgroup Administrators and Foundstone Users may only belong to a single root organization.

7.3.3 Workgroup Management

Workgroups are configured by the Root Organization Administrators. The IP addresses and scan engines available to the workgroup are part of this configuration and must be a subset of the IP addresses and scan engines configured for the root organization. When any workgroup is created, an administrator group is automatically created for that workgroup. Users are designated as Workgroup Administrators by associating the user account with the appropriate administrator group(s).

Workgroup Administrators may configure users, groups and scans within their workgroups.

7.3.4 Scan Engine Management

A Root Organization Administrator may configure the following security-relevant settings for any engine associated with the same root organization.

Table 24 - Scan Engine Management

Area	Parameter	Description
Engine Connection	Address	Enter the IP address, DNS name, or NetBIOS name for the Web server running the Enterprise Manager.
	Port	Enter the port number that the Web server uses to receive McAfee information.
	Use SSL	Use Secure Socket Layer between this Scan Engine and the Enterprise Manager. This option is always selected for the evaluated version.
	Authentication Scheme	Shows the authentication method being used to communicate from the Enterprise Manager to the Scan Engine.
Enterprise Manager Connection	Address	Enter the IP address, DNS name, or NetBIOS name for the Web server running the Enterprise Manager.
	Port	Enter the port number that the Web server uses to receive McAfee information.

Area	Parameter	Description
	Use SSL	Use Secure Socket Layer between this Scan Engine and the Enterprise Manager. This option is always selected for the evaluated version.
	Authentication Scheme	Shows the authentication method being used to communicate from the Enterprise Manager to the Scan Engine.
Default Ports	Host Detection Ports	Specifies the default TCP and UDP ports to be used during scans to discover hosts.
	Service Detection Ports	Specifies the default TCP and UDP ports to be used during scans to discover services running on scanned systems.

7.3.5 Asset Management

Assets are systems being scanned by the TOE. Assets are automatically created as scans are performed. A Root Organization Administrator or Workgroup Administrator may associate a Criticality with individual assets. The defined Criticality values are None, Low, Limited, Moderate, Significant and Extensive. Vulnerabilities found on hosts marked with a lower criticality count less than vulnerabilities found on hosts with a high criticality level.

A Root Organization Administrator or Workgroup Administrator can combine multiple assets into groups, organizing them into hierarchies. This makes it easier to manage assets, add groups of assets to scans, and monitor risk. Any number of groups and sublevels of groups may be created. A Criticality may be assigned to an entire asset group. An asset can belong to only one group at a time.

The Root Organization Administrator can delete any asset group. The Workgroup Administrator can delete asset groups if the group only contains assets belonging to the IP pool for that workgroup. If the asset group contains assets from other workgroups, only the assets belonging to that IP pool are removed and the asset group itself is not deleted.

7.3.6 Scan Management

Scans may be created by Root Organization Administrators and Workgroup Administrators. They may be modified by those same roles as well as Foundstone Users with appropriate permissions. The parameters that may be configured are:

1. IP addresses/assets to be included in the scan
2. ICMP, TCP and UDP protocol options for discovery scans
3. Credentials to be used during scans to help identify access configuration settings
4. Service discovery
5. Vulnerability scans to be performed; the list of known vulnerabilities may be updated so that the scans are kept current as new vulnerabilities are identified
6. Web application assessment
7. Schedule a recurring scan
8. The scan engine and network interface to be used
9. Windows (time slots) during which the scan may execute

7.3.7 Report Management

Reports may be generated for any scan by users with View access to that scan. Reports are generated based upon Report Templates, which specify the format of the output, the frequency with which the report is generated, the assets to be addressed by the report, and the type of information to be included in the report. Many templates are supplied with Vulnerability Manager and additional templates may be created by users.

The assets specified by IP address in a report template are limited by the following restrictions:

Table 25 - Report Template IP Address Restrictions

User Type	Assets by IP Address
Root Organization Administrator	All IP addresses in the organization's IP Pool
Workgroup Administrator	All IP addresses in the workgroup's IP Pool
Foundstone User with View access to a scan	All IP addresses included in the scan
Foundstone User with privilege to edit the IP addresses associated with a scan	All IP addresses within the workgroup to which the scan belongs. If the scan belongs to the organization, this user has access to all IP addresses within the organization.

Users may cause reports to be generated for any scan for which they have View access. Once a report is initiated, it is generated by the Report Service executing on the system with the Foundstone Database. Reports in the process of being generated are displayed in a queue and may be canceled by any user with View access to the associated scan.

The three most recent reports associated with each scan are saved. Older reports are automatically deleted.

7.3.8 Known Vulnerability Management

Global Administrators may import (create) known vulnerabilities by importing XML files conforming to the SCAP Benchmark Assessment XCCDF and OVAL standards. After the information has been imported it is available for association with scans.

Global Administrators may customize the Windows Policy settings, Registry Key permissions, File and Root File permissions, and Service settings in these vulnerability definitions.

Global Administrators may also export these vulnerability definitions to XML files conforming to the SCAP Benchmark Assessment XCCDF and OVAL standards.

7.4 Audit

FAU_GEN.1 Audit Data Generation

The TOE’s Audit Security Function provides auditing of management actions performed by administrators. The following audit information is collected:

1. Start-up and shutdown of audit functions
2. Access to the TOE and System data, including the information being accessed and the type of access
3. Successful and unsuccessful I&A attempts, including the supplied user identity and IP address of the browser session

4. All modifications in the behavior of the functions of the TSF
5. All modifications to the values of TSF data
6. Use of the management functions, including the IP address of the browser session (user identity) and the function used
7. Modifications to the group of users that are part of a role, including the IP address of the browser session (user identity)

The audit records generated by the TOE include the items listed in Table 13 and are categorized by the following event types:

1. Administrator actions
2. User actions
3. System actions

Administrator actions are those that are specific to authorized administrator activities (i.e. add-remove- change user attributes and system attributes.) User actions are those that are specific to user activities (i.e. logon and logoff.) System actions are specific to the TOE performing system operations (i.e. running queries, requesting or setting scan configurations, request scan status, verifying license information, verifying access rights.)

The following information is provided for an audit record generated by the TOE:

1. Date and Time of the event
2. Type (i.e. category and action) of the event
3. Subject (i.e. user and IP address) identity
4. Description (i.e. action performed, success or failure, etc.) of event

Audit records are stored in the database. Administrators are advised to configure the database to expand to the limits of the file system. In the unlikely event storage space exhaustion does occur, the TOE discards the most recent results. The database in the IT environment may optionally be configured to send alert notifications to administrators when capacity limits are reached so corrective actions may be taken.

7.5 Asset Data Import

The TOE dynamically learns about assets when it conducts scans. The TOE may also be configured to import data about assets from external Data Sources, such as LDAP servers or ePO servers in the IT environment. Both LDAP and ePO databases contain detailed information about computer assets that may be of interest to administrators. This information may be imported from these Data Sources to be used by the TOE. The value of this functionality is that the information about the assets may be more accurate or complete than the information obtained from scans. Note that the integration of the TOE with ePO is for data import only; ePO does not provide any management functionality of the TOE.

Information may be learned about new or existing assets. If conflicting information is learned from different sources, the following precedence rules are applied (from highest to lowest):

1. Information obtained from ePO

2. Information obtained from LDAP servers
3. Information obtained from scans

The TOE must associate an IP address for each asset learned from a Data Source. This may be obtained from the IP Address attribute or by resolving the address from the NetBIOS Name and DNS Name attributes. Assets learned from a Data Source are automatically associated with a workgroup or organization based upon the asset's IP address and the IP address pool for the workgroups and organizations. If the asset's IP address does not correspond to any workgroup or organization, the asset is initially placed into the Unassigned Assets group.

The information that can be imported for an asset is:

1. NetBIOS Name
2. DNS Name
3. IP Address
4. Domain/Workgroup Name
5. MAC Address
6. Operating System Name (from ePO data sources only)
7. Operating System Version (from ePO data sources only)

This function is performed according to the frequency configuration of each configured Data Source.

8. Protection Profile Claims

This chapter provides detailed information in reference to Protection Profile conformance.

8.1.1 Protection Profile Reference

This Security Target does not claim conformance to any Protection Profile.

8.1.2 Protection Profile Refinements

This Security Target does not claim conformance to any Protection Profile.

8.1.3 Protection Profile Additions

This Security Target does not claim conformance to any Protection Profile.

8.1.4 Protection Profile Rationale

This Security Target does not claim conformance to any Protection Profile.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat, assumption and policy, the security objective(s) that address it.

Table 26 - Assumptions, Threats and Policies to Security Objectives Mapping

	O.PROTCT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.INTEGR	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	O.AUDITS	O.IMPORT	O.SCAP	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.ALARM
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.DATABASE																					X				
A.ALARM																									X
T.COMINT	X				X	X		X										X							
T.COMDIS	X				X	X												X							
T.LOSSOF	X				X	X		X																	
T.NOHALT		X	X		X	X																			
T.PRIVIL	X				X	X																			
T.IMPCON				X	X	X			X																
T.SCNCFG		X													X	X									
T.SCNMLC		X													X	X									
T.SCNVUL		X													X	X									
T.FALREC			X																						
T.FALASC			X																						
T.FACCNT														X											
T.FALACT																X									
P.DETECT		X												X			X						X		
P.ANALYZ			X																						
P.MANAGE	X			X	X	X			X		X	X													
P.ACCESS	X				X	X													X	X	X				
P.INTGTY								X														X		X	
P.PROTCT							X			X								X						X	
P.ACCACT						X								X											

9.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat, assumption and policy to security objectives mapping.

Table 27 - Threats, Assumptions and Policies to Security Objectives Rationale

x.TYPE	Security Objectives Rationale
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 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.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.
A.ALARM	The DBMS will generate an alarm if storage space in the database is exhausted. The OE.ALARM objective ensures that the DBMS will generate an alarm if storage space in the database is exhausted.
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.PROTECT objective supports the TOE protection from the IT Environment.
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.PROTCT objective

x.TYPE	Security Objectives Rationale
	addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
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.
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 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 and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes 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.
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 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.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 O.IMPORT objective supports this threat by requiring the TOE to be able to import information about assets so that scanning may be configured for all appropriate IT systems. The O.SCAP objective supports this threat by requiring the TOE to be able to import additional benchmark assessments, enabling the TOE to address new configuration requirements as they are identified.
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, which contains a Scanner, to collect and store static configuration information that might be indicative of malicious code. The O.IMPORT objective supports this threat by requiring the TOE to be able to import information about assets so that scanning may be configured for all appropriate IT systems. The O.SCAP objective supports this threat by requiring the TOE to be able to import additional benchmark assessments, enabling the TOE to new checks for malicious code as they are identified.
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

x.TYPE	Security Objectives Rationale
	Scanner, collect and store static configuration information that might be indicative of a vulnerability. The O.IMPORT objective supports this threat by requiring the TOE to be able to import information about assets so that scanning may be configured for all appropriate IT systems. The O.SCAP objective supports this threat by requiring the TOE to be able to import additional benchmark assessments, enabling the TOE to address new vulnerabilities as they are identified.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on 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 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.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.FALACT	Issues resulting from scans of monitored systems may fail to be acted upon because the information is not disseminated from the TOE to other IT systems that are responsible for tracking or correcting the issues. The O.SCAP objective addresses this threat by requiring the TOE to support the export of scan and analysis results in SCAP Benchmark Assessment format so that the information may be imported by other IT systems.
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 and O.IDSCAN objectives address this policy by requiring collection of audit and Scanner data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records. The OE.AUDIT_REVIEW objective supports this policy by providing the ability to review audit events generated by the TOE.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from each data source 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 addresses this policy by providing TOE self-protection.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses via the Foundstone Enterprise Manager web interface. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and

x.TYPE	Security Objectives Rationale
	OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION objective counters this threat via IT Environment protections of the system data trail. The O.PROTCT objective addresses this policy by providing TOE self-protection.
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 within the TSC. The OE.AUDIT_PROTECT objective ensures the integrity of audit records in the database generated by the TOE. The OE.CRYPTO objective requires the IT Environment to provide secure channels via cryptographic functionality and protocols that can be used by the TOE to protect the data during transit.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. 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.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 28 - TOE SFRs to Security Objectives Mapping

	O.PROTCT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.INTEGR	O.AUDITS	O.IMPORT	O.SCAP
FAU_GEN.1									X		
FIA_UAU.1					X	X					
FIA_ATD.1						X					
FIA_SOS.1						X					
FIA_UID.1					X	X					
FMT_MOF.1	X				X	X		X			
FMT_MTD.1	X				X	X					
FMT_SMF.1						X					
FMT_SMR.1						X					
FPT_TDC.1(1)										X	
FPT_TDC.1(2)											X
IDS_SDC.1		X									
IDS_ANL.1			X								
IDS_RDR.1				X	X	X					
IDS_STG.2							X				

The following table provides the detail of TOE security objective(s).

Table 29 - TOE Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. 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 add System data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.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 System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC.1].
O.IDANLZ	The TOE must 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.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1].
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.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 add System data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
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.1]. Security attributes of subjects use 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]. Minimum standards are defined for the passwords so that the authentication process is robust [FIA_SOS.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 add System data, and authorized administrators of the TOE may query and modify all other TOE data [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 set of management functions to be restricted are identified [FMT_SMF.1].
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows. The System must prevent the loss of system data in the event its trail is full [IDS_STG.2].

Security Objective	SFR and Rationale
O.INTEGR	The TOE must ensure the integrity of all System data. Only authorized administrators of the System may query or add System data [FMT_MTD.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].
O.IMPORT	The TOE shall provide mechanisms to import data about assets from LDAP servers and ePO. The TOE defines management functionality to import asset data from configured sources [FPT_TDC.1(1)].
O.SCAP	The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data. The TOE includes mechanisms to exchange SCAP Benchmark Assessment data with external systems [FPT_TDC.1(2)].

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence and source code, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

C) Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

9.3 TOE Summary Specification Rationale

This section demonstrates that the TOE’s Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE’s Security Functions and the SFRs and the rationale.

Table 30 - SFRs to TOE Security Functions Mapping

	Scanning	I&A	Management	Audit	Asset Data Import
FAU_GEN.1				X	

	Scanning	I&A	Management	Audit	Asset Data Import
FIA_UAU.1		X			
FIA_ATD.1		X			
FIA_SOS.1		X			
FIA_UID.1		X			
FMT_MOF.1			X		
FMT_MTD.1			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_TDC.1(1)					X
FPT_TDC.1(2)			X		
IDS_SDC.1	X				
IDS_ANL.1	X				
IDS_RDR.1	X				
IDS_STG.2	X				

Table 31 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	**Audit –** Management actions performed by administrators are audited.
FIA_ATD.1	**I&A** – User security attributes are associated with the user upon successful login via the Foundstone Enterprise Manager.
FIA_SOS.1	**I&A** – Minimum standards for passwords are defined and enforced to ensure that the I&A process is robust.
FIA_UAU.1	**I&A** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_UID.1	**I&A** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FMT_MOF.1	**Management** – The User Type identifies the privilege level of the user. The User Type determines the level of ability to alter the scan configuration and parameters.
FMT_MTD.1	**Management** – The User Type identifies the privilege level of the user. The User Type determines the permissions for access to the TSF data.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the user type is specified. Global Administrator is implicit for FoundScan Engine users.
FPT_TDC.1(1)	**Asset Data Import** – The TOE provides the functionality to import asset data information from LDAP servers and ePO and correctly interpret the information.

SFR	SF and Rationale
FPT_TDC.1(2)	**Management** – Global Administrators can import and customize SCAP Benchmark Assessment data and export reports in SCAP-conformant XML files.
IDS_SDC.1	**Scanning** – The TOE performs scans of specified systems in order to detect vulnerabilities present on those systems in the areas of access control and service configuration. Scan results are stored in the database.
IDS_ANL.1	**Scanning** – The TOE analyzes the results of the scanning performed to identify known vulnerabilities on those systems. Vulnerability information in stored in the database.
IDS_RDR.1	**Scanning** – The TOE provides the ability for authorized administrators to retrieve reports from the database that describe the vulnerabilities detected on the scanned systems. Access is limited to reports for which each administrator is authorized.
IDS_STG.2	**Scanning** – If the storage space is exhausted, the oldest data is saved and the most recent data is ignored.

9.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Section 8.4 Protection Profile Rationale.