Tripwire, Inc. Tripwire Enterprise Version 8.9.1 Security Target

Release Date: August 10, 2022

Version: 1.1

Prepared By: Saffire Systems
P.O. Box 40295
Indianapolis, IN 46240

Prepared For: Tripwire, Inc.
308 SW Second Ave
Suite 400
Portland, OR 97204

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

This section will provide information necessary to identify and control the Security Target and the TOE.

ST Title	Tripwire, Inc. Tripwire Enterprise Version 8.9.1 Security Target
Version:	1.1
Publication Date:	August 10, 2022
ST Author	Michelle Ruppel, Saffire Systems
Assurance Level:	EAL 2 + ALC_FLR.2

1.2 TOE Reference

The TOE claiming conformance to this ST is identified as:

Tripwire Enterprise, Version 8.9.1 (Build number r20220420091602-d875c96.b18) with:

Java Agent 8.9.1.0 (Build Number: r20220516044224-cde9c59.b4) and

Axon Agent 8.8.3.7 (Build Number: r20220417072025-7cef127.b5)

1.3 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.3.1 Acronyms

3DES	Triple Data Encryption Standard
AC	Access Control
ACL	Access Control List
ANSI	American National Standards Institute
BCCM	Bouncy Castle Cryptographic Module
CC	Common Criteria
CLI	Command Line Interface
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
EAL2	Evaluation Assurance Level 2

FIPS	Federal Information Processing Standard (NIST)
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IETF	Internet Engineering Task Force
JAR	Java Archive
JDBC	Java Data Base Connectivity
JVM	Java Virtual Machine
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
OSP	Organisational Security Policy
PP	Protection Profile
RAM	Random Access Memory
RMI	Remote Method Invocation
ROM	Read Only Memory
SACL	System Access Control List
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm 1 (NIST)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SQL	Structured Query Language for data base access
TE	Tripwire Enterprise
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UI	User Interface
VPN	Virtual Private Network

1.4 Overview

The TOE is Tripwire Enterprise Version 8.9.1. (TE v8.9.1), provided by Tripwire, Inc. The TOE type is an intrusion detection system consisting of a sensor, scanner, and analyzer to monitor IT

systems for activity that may indicate inappropriate activity on the IT system. The TOE is a software-only TOE. The TE server runs on various operating systems, including the Windows and Red Hat Enterprise Linux operating systems included in this evaluation. The Agent[1] portion of the TOE can be installed and executed on the operating systems identified in Section 1.4.2.2. TE v8.9.1 performs file-integrity monitoring, change auditing, configuration assessment, and compliance reporting. The TOE is an attribute change assessment product that also reconciles the changes against existing management systems and policies.

The TOE provides three main capabilities: File Integrity Monitor, Compliance Policy Manager, Remediation Manager. The File Integrity Monitor observes and checks the state of the integrity of critical data on a wide variety of servers and network devices (e.g., routers, switches, firewalls, and load balancers) called nodes. It does this by gathering system status, configuration settings, file content, and file metadata on the nodes and checking gathered node data against previously stored node data to detect modifications. For IT systems with a TE Agent installed, the TOE is capable of monitoring the system for changes made in real-time. The Compliance Policy Manager continually assesses IT configurations against a set of policies and standards, identifying deficiencies.[2] The Remediation Manager repairs/corrects configuration errors detected by the Compliance Policy Manager. The Remediation Manager supports only File Server nodes (i.e., the Remediation Manager is only able to repair/correct failures on File Server nodes).

TE requires a database application to support the product's storage needs. Since TE v8.9.1 supports the ability to operate with a database from differing vendors (as identified in Section 1.4.2.1), the database is considered part of the operational environment

The TOE relies upon the JVM TLS implementation in the operational environment to protect communications between the TOE and the remote IT entities (e.g., the database, user's browser, and user's shell).

1.4.1 Security Features

The TOE implements the following security functions:

- Security Audit

  The TOE generates audit records for security related audit events and provides a mechanism to allow authorized administrators to select which security-relevant events are recorded. An interface is also provided for authorized administrators to review the records. Audit records are protected from unauthorized deletion and modification and mechanisms are in place to prevent audit data loss.

- Cryptographic Support

  Cryptographic capabilities within the TE Server and TE Java Agent are provided by the FIPS-certified Bouncy Castle cryptographic module. Cryptographic capabilities within the TE Axon Agent are provided by an OpenSSL FIPS-certified cryptographic module.

[1] The term Agent or TE Agent in this ST is used to refer to either the TE Java Agent or TE Axon Agent.

[2] This evaluation did not assess whether given policy files are sufficient to confirm the intended policy or guideline, but rather assessed whether the applicable policy checks worked correctly.

These FIPS-certified cryptographic modules are used to implement the cryptography used by TLS to protect communications between distributed parts of the TOE

- User Data Protection

  The TOE implements access controls on the TE objects it maintains.

- Identification and Authentication

  The TOE provides two mechanisms for the identification and authentication of administrative users: an internal password-based mechanism and external Active Directory (an LDAP-compliant Microsoft directory) mechanism. TE enforces password complexity requirements.

- Security Function Management

  Tripwire Enterprise can be administered remotely or locally. The TOE provides four management interfaces: a graphical user interface (GUI), a command-line interface (CLI or twtool), a SOAP interface, and the tetool command. The TOE provides management functions for configuring intrusion detection behaviors, managing audit functions, managing TOE data, and managing user accounts.

- Protection of the TSF

  The TOE implements many features for protection of the integrity and management of its own security functionality. These features include the protection of sensitive data and reliable time stamps. The TOE protects remote connections to the management interfaces with HTTPS / TLS. Connections between distributed parts of the TOE are protected with TLS.

- Intrusion Detection

  TE scans the nodes collecting object attribute information for files, directories, registry keys, and registry key values. The TOE detects changes in the nodes by comparing collected information against saved values. TE can perform configured actions in response to comparison results, such as executing policy compliance tests and notifying administrators of results. TE also provides remediation options for file server nodes failing a policy compliance test.

1.4.2 Required non-TOE hardware/software/firmware

The TOE depends upon the required platforms identified below that are in the TOE environment.

The TOE relies upon the following software in the local[3] operational environment of the Tripwire Enterprise Server or the Tripwire Enterprise Java Agent.

- Java Virtual Machine – provides a runtime environment for the TOE.

The TOE assumes the following network IT entities are in the operating network environment.

[3] Local operational environment refers to software running on the same host as either the server or agent components of the TOE.

- SMTP Server – An email server is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- SNMP recipient -- A network management device is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- Syslog Server – A destination for the collection of log messages sent by the TOE.
- Workstation providing a web browser for access to the GUI
- TE Nodes
- LDAP/Active Directory server – An authentication server used to authenticate TE users when the System Login Method is set to LDAP/Active Directory.

Notification mechanisms such as email, SNMP, and syslog server are outside of the TOE boundary. The TOE implements only the client-side of these protocols. The TOE utilizes external (non-TOE) mechanisms for delivery of notifications, thus the TOE cannot guarantee delivery of notifications. Web browsers used with the web-based GUI are not part of the TOE.

1.4.2.1 Tripwire Enterprise System Requirements

The Tripwire Enterprise Server can be installed on the following platforms which are in the operating environment:

- Windows Server 2016 (x86 64-bit)
- Windows Server 2019 (x86 64-bit)
- Red Hat Enterprise Linux 8.0 (x86 64-bit)
- Red Hat Enterprise Linux 7.6 (x86 64-bit)

Tripwire Enterprise requires that one of the following Java Runtime Environment (JRE) is installed for use by the TOE on these platforms. The JRE is in the operating environment.

- Azul Zulu 64-bit OpenJDK 8, version 8u181 or the latest version

The TE administrators need to ensure that current and patched JVMs are used during operation of the TE in order to support the security functionality provided. Tripwire makes JRE update packages available for download at the same time as Tripwire provides patch release and major updates.

TE supports the following backend DBs which are in the operating environment:

- Microsoft SQL Server 2016 SP2 (x86 64-bit),
- Microsoft SQL Server 2017 (x86 64-bit),
- Oracle MySQL 8.0.x (x86 64-bit)
- Oracle 12c R2 (12.2.0.1)
- Oracle 18c
- Amazon Aurora MySQL 5.7-compatible

TE Web Admin Console supports the following web browsers which are in the operating environment:

- Microsoft Edge 90 or later
- Mozilla Firefox 68 or later

1.4.2.2 Agent Requirements

TE supports two different types of Agents what are used to assist in monitoring nodes: Tripwire Enterprise Java Agents and Tripwire Enterprise Axon Agents. The term TE Agents in this ST is used to refer to both the TE Java Agent and the TE Axon Agent. TE Agents are installed on file servers and desktops being monitored by Tripwire Enterprise.

Unless otherwise noted, either Agent can be installed on the following operating systems which are in the operating environment:

- RedHat Enterprise Linux version 8.0 (x86 64-bit) for TE Axon Agent only
- RedHat Enterprise Linux version 7.6 (x86 64-bit)
- Microsoft Windows 10 (x86 64-bit)
- Microsoft Windows Server 2016 (x86 64-bit)
- Microsoft Windows Server 2019 (x86 64-bit)

All current patches and security fixes must be installed upon these operating systems before installing the TE Agent.

1.4.2.3 Tripwire Enterprise Node Requirements

In addition to desktops and file servers, TE can operate on the following types of nodes which are in the operating environment: databases, virtual environments, directory services, network devices. These nodes are the supported systems that can be monitored by the TOE.

The Tripwire Enterprise configuration can target the following databases:

- Microsoft SQL Server 2016 or later
- Oracle 12cR2 or later
- Oracle 18c or later

The Tripwire Enterprise configuration can target the following virtual environments:

- VMware ESXi 6.5 or later

The Tripwire Enterprise configuration can target the following directory services:

- Microsoft Windows Active Directory 2016 or later

The Tripwire Enterprise configuration can target all versions the following network devices:

- Cisco IOS v15.8 or later

All current patches and security fixes must be installed upon these network devices before allowing a Tripwire Enterprise Server to target the network device.

1.5 TOE Description

The TOE monitors IT systems for activity that may indicate inappropriate activity on the IT

system. The server or network devices monitored by the TOE are called nodes. There are multiple types of nodes – a file server node, a database node, a directory server node, a network device node, virtual infrastructure node and a custom node[4]. There are two classes of nodes that the TOE can monitor, those with built-in external administration interfaces and those without. Examples of nodes with built-in administration interfaces are databases, directory servers, firewalls, routers, switches, load balancers, etc. Some of these external interfaces use web servers and allow administration via a remote web browser, and others provide command line interfaces or other custom protocols. Examples of nodes without built-in administration interfaces are Microsoft Windows systems and Linux systems. These nodes are referred to as Agent nodes (or file server nodes) and host an installation of Tripwire Enterprise Java Agent or Tripwire Enterprise Axon Agent. To create a file server node (includes desktops), a TE Agent is installed on file server. The other node types are assigned a delegate TE Agent that processes some TE functions for the node.

The Tripwire Enterprise Agents provide an interface for Tripwire Enterprise Server where none otherwise exists or to provide a more fully featured interface than an existing one. Tripwire Enterprise Agents are installed on nodes that run server-type operating system. When installed on a node, the TE Agent is always running and ready to receive instructions from the TE Server. The TE Agent executes baselines and integrity checks on its node and communicates the results from those operations to the TE Server for reporting and for integration with system-wide results. The TE Agent is capable of collecting audit events from monitored systems. The audit events are collected from logs on the systems or from the TE Event Generator. The TE Event Generator is an auditing utility for UNIX and Windows file servers that create audit events for monitored files, directories, registry keys, and registry entries. If an Event Generator is installed on an Agent system, the system can be monitored for changes made in real-time.

The TOE may also be used to monitor the configuration of its nodes, thereby identifying changes made by users or other applications, such as software-provisioning and patch-management tools that run independently of Tripwire Enterprise.

A node is represented in the TOE by its network address (hostname or IP address).

[4] A custom node is a user-created type of network device node.

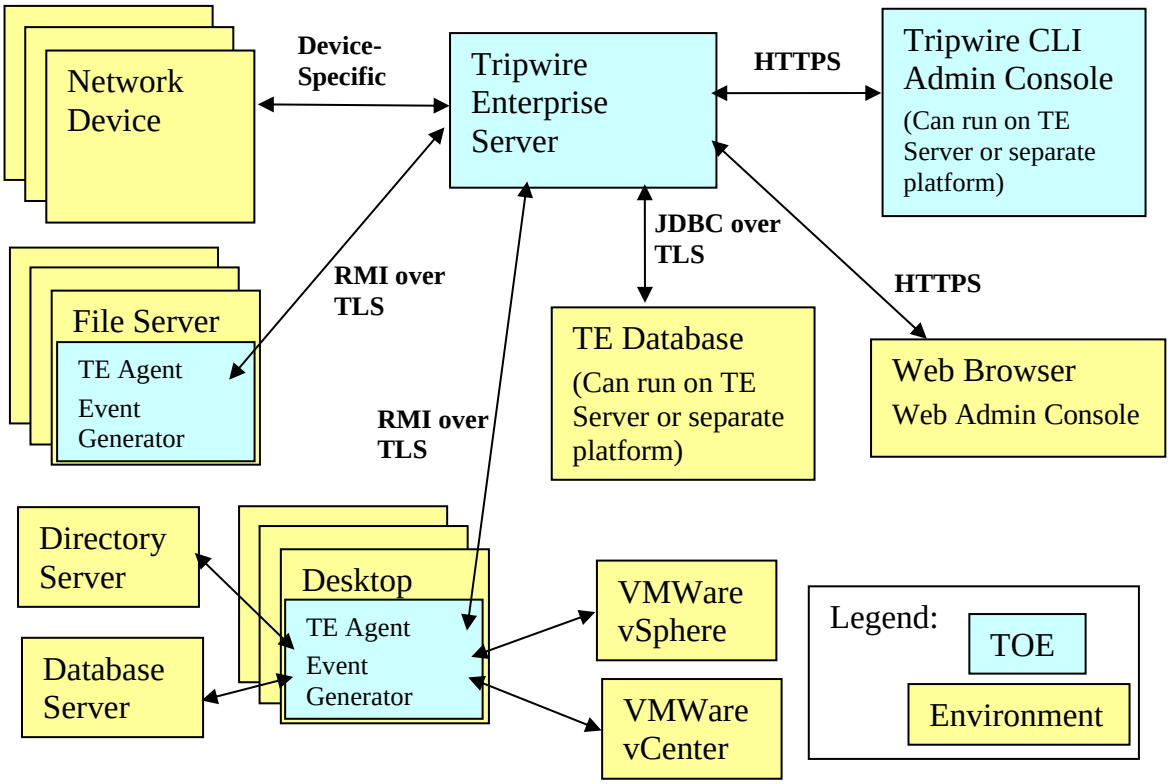

Figure 1: TOE boundary

1.5.1 Tripwire Enterprise Server

The Tripwire Enterprise Server component delegates work to Tripwire Enterprise Agents, interacts with TE nodes, analyzes information, assesses policy compliance, repairs configuration errors, and provides a web-based user interface (or a network interface that provides limited functionality using the Tripwire CLI application component as an alternative to a web browser) for managing the TOE installation. The Tripwire Enterprise Server component includes the User Interface.

The TOE provides two user friendly interface that provide access to the administrators of the system; a graphical user interface (GUI) called the Tripwire Enterprise Web Admin Console and a command line interface (CLI) called the Tripwire CLI Admin Console. They will be referred to in this document as the GUI and CLI, respectively.

The GUI is a web server running in the TOE for use by an external web browser. The connection between the web browser and the GUI uses HTTPS to protect the integrity of the connection. The GUI provides an administrator the ability to perform such functions as add users, configure and schedule integrity checks[5], configure and schedule policy compliance tests,

[5] The more general term 'integrity check' is used in this Security Target, but is intended to have the same meaning

configure remediation actions, manage nodes, and view reports. User identification and authentication is handled through the GUI.

The CLI provides an interface for scripts to perform a limited number of operations on the TOE. Its functionality is a subset of the GUI's and is insufficient to fully administer the TOE. For example, there are no CLI commands for adding or deleting users or changing passwords. The CLI provides administrator access to the Tripwire Enterprise Server. Like the GUI interface, the CLI connects to the Tripwire Enterprise Server using HTTPS[6].

The TOE provides a JDBC interface to a SQL database. Since TE v8.9.1 supports the ability to operate with a database from differing vendors (as identified in Section 1.4.2.1), the database is considered part of the operational environment. If the configuration uses a remote SQL server, the TE Server must be configured to encrypt all communications between itself and the database. The database can either be installed on the same system as the TE server or installed on a system located on a private physical network that is not globally routable and is protected from attacks and from unauthorized physical access. If the Oracle DB is used, it must be installed on a system located on a private physical network that is not globally routable and is protected from attacks and from unauthorized physical access. The database is relied upon to store, retrieve and protect data that it handles such that only the Tripwire Enterprise Server can access its own data.

The TE Node device-specific interface provides a custom interface for obtaining configuration parameters and other management data from a specific list of supported devices (nodes). The device-specific interfaces utilize protocols such as SSH[7], telnet, and FTP.[8]

1.5.2 Monitoring and Remediation

All of the compliance policy and standard assessments are performed on the TE Server.

The nodes that do not require an installed TE Agent have their own built-in external management interfaces. For these devices, TE Server uses the built-in interfaces to monitor the configurations. For the POSIX compliant UNIX systems, TE uses its proprietary Universal Device Kit (UDK) to collect information as defined by the customer.

The TE Server obtains information about the current configuration from the nodes that do not have TE Agent and compares that information to saved baseline configuration information. For each node, the TE Server uses the following access information:

- Target IP address (or hostname),
- Communications protocols, and

---

as the term 'version check' which is used in Tripwire guidance documentation.

[6] The Tripwire Enterprise Server uses the SSL provided by the operational environment for HTTPS communications.

[7] The implementation of SSH used by the TOE is not FIPS compliant. The TOE does not make any claims on the cryptography provided by the SSH implementation.

[8] Note: This use of SSH, FTP and telnet should not be confused with protocols used to manage the TOE itself. These protocols are only available for use in monitoring the management of nodes, not for managing the TOE. Only secure services are used to manage the TOE.

- Authentication credentials

Tripwire Enterprise Server uses the above information to establish a connection and authenticate itself to the agentless TE node, as if it were an administrator. It uses its device-specific knowledge of the format and structure of the management interface to collect configuration information. When verifying the integrity of the configuration, Tripwire Enterprise Server compares newly collected information with baseline configuration information.

For nodes with a TE Agent, the TE Server receives attribute values and baseline values from the TE Java Agent or TE Axon Agent (the TE Server is responsible for storing these values). The most recent set of harvested attributes is cached on the TE Agent until it can be sent to the TE Server. The TE Agent is always running and ready to receive instructions from the TE Server.

The execution of the corrective Remediation scripts is done on the Java Agent. All other actions and operations in relation to Remediation are performed on the Server.

1.5.3 Architecture Description

The components that make up the TOE are:

- Tripwire Enterprise Server – Analyzes collected information from Tripwire Enterprise nodes. Tripwire Enterprise Server includes a User Interface (UI) subcomponent that provides interfaces to both web-based (GUI) and command line (CLI) administrative interface applications.
- Tripwire Enterprise Java Agent – Collects information from monitored servers for the Tripwire Enterprise Server.
- Tripwire Enterprise Axon Agent – Collects information from monitored servers for the Tripwire Enterprise Server. This Agent includes a FIPS certified OpenSSL implementation.
- Event Generator – A real-time monitoring utility that can be installed with TE Agent on some Windows and UNIX file servers. This component is optional and is only required when real-time monitoring is desired.
- Tripwire CLI – The command-line administrative interface to the UI.
- Bouncy Castle Cryptographic Module – provides the cryptographic operations used by the TOE and the JVM.

The Tripwire Enterprise Server uses various network protocols to communicate with other parts of the TOE and with the operational environment. Depending upon the communication pathway the Tripwire Enterprise Server acts either as a server or as a client on each pathway. The following summarize the network communication pathways that exist.

- Tripwire Enterprise Server – Tripwire Enterprise Agent communication.

  The Tripwire Enterprise Server and Tripwire Enterprise Agents are peers, with either able to initiate communication to accomplish the task being performed.

  Both the Tripwire Enterprise Server and Tripwire Enterprise Agent components of the TOE use the TLS to communicate with each other. A mutually authenticated TLS connection is established that allows these components of the TOE to communicate.

- Tripwire Enterprise Server – TE Database

  The Tripwire Enterprise Server is the only component of the TOE that communicates with the database. The TE Server uses the JDBC protocol over TLS provided by the JVM in the operational environment to connect to the database.

- Tripwire Enterprise Server – TE nodes

  The Tripwire Enterprise Server initiates connections to TE nodes that do not have the TE Agent installed to obtain information made available by protocols supported by the node (e.g., FTP, Telnet, SSH). For protocols requiring user authentication, the Tripwire Enterprise Server provides login data for the specific node being accessed, then gathers information from the node as determined by rules established for that network device (e.g., a specific Cisco PIX Firewall or Netscreen device).

- Tripwire Enterprise Server – CLI & GUI

  The Tripwire Enterprise Server includes web server functionality that supports HTTP over the TLS provided by the JVM in the operational environment. Thus, the communication between the Tripwire Enterprise Server and the Tripwire CLI uses the HTTPS protocol. Similarly, communication between the Tripwire Enterprise Server and the GUI is also over the HTTPS protocol.

- Tripwire Enterprise Server – SMTP/SNMP/Syslog server

  The Tripwire Enterprise Server is a client to SMTP/SNMP/Syslog servers. The Tripwire Enterprise Server uses these servers as configurable delivery mechanisms for TOE generated messages.

Tripwire CLI does not offer any inbound network communication pathways.

The only communications accepted by Tripwire Enterprise Agents are over an authenticated TLS connection established with the Tripwire Enterprise Server.

1.5.4 Physical Boundaries

The Evaluated Configuration includes components running in the TOE boundary and components running outside the TOE boundary. Inside the TOE boundary are Tripwire Enterprise Server, Tripwire CLI running on a computer, one or more Tripwire Enterprise Agents running on remote servers, and the Bouncy Castle Cryptographic Module.

The Tripwire Enterprise Server component of the TOE can operate on several supported operating systems. Refer to Section 1.4.2 for a list of supported OSs. The host operating system for Tripwire Enterprise Server has no impact on the supported list of Tripwire Enterprise nodes that can be monitored.

The TOE, including the guidance documentation, is delivered to customers via download from the Tripwire Web site. Windows versions of the TOE software are provided in a ZIP file, and Linux version are provided in a TAR.GZ file format. Except for the release notes, the guidance documentation is provided in PDF format. Release notes are provided in HTML format.

The operational environment also includes a web browser and a network connecting all of the other components into a single LAN.

The TOE relies upon the following software in the operational environment.

- Database – Stores data for Tripwire Enterprise Server.
- Java Virtual Machine – provides a runtime environment for the TOE.
- Host Operating System – provides process-related (e.g., time) and network-related (e.g., name resolution) services for the JVM.

The TOE assumes the following network IT entities are in the operating environment.

- SMTP Server – An email server is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- SNMP recipient -- A network management device is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- Syslog Server – A destination for the collection of log messages sent by the TOE.
- Tripwire Enterprise Nodes
- LDAP/Active Directory server – An authentication server used to authenticate TE users, except the built-in "administrator" account, when the System Login Method is set to LDAP/Active Directory.

Refer Section 1.5.6 to for a list of components excluded from the TOE.

1.5.4.1 Hardware Components

The TOE is a software only TOE. All hardware used to deploy the TOE is in the operational environment.

1.5.4.2 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	Tripwire Enterprise Server, Version 8.9.1	Analyzes collected information from Tripwire Enterprise nodes. Tripwire Enterprise Server includes a User Interface (UI) subcomponent that provides interfaces to both web-based (GUI) and command line (CLI) administrative interface applications.
TOE	Tripwire Enterprise Java Agent, Version 8.9.1.0	The Java agent installed on the node that collects information from monitored servers for the Tripwire Enterprise Server

TOE or Environment	Component	Description
TOE	Tripwire Enterprise Axon Agent Version 8.8.3.7	The Axon Agent that is installed on the node to collect information from monitored servers and send it to the TE server. This includes a FIPS-certified OpenSSL cryptographic module (certificate number 2398).
TOE	Event Generator	A real-time monitoring utility that can be installed with TE Agent on some Windows and UNIX file servers. This component is only required when real-time monitoring is desired.
TOE	Tripwire CLI Admin Console	A utility that allows TE functions to be executed using a command line, without using the TE GUI.
TOE	Change-Audit License	A license certificate[9] that activates the TE change auditing for a single monitored system of a specific type.
TOE	Configuration-Assessment License	A license certificate that enables TE to run policy tests on a single node. To generate policy test results for a node, the node must have valid Configuration-Assessment licenses.
TOE	Automated-Remediation License	A license certificate that enables TE to remediate policy tests on a single file server node. To automatically remediate failed policy tests for a node, the node must have valid Change-Audit, Configuration-Assessment, and Automated-Remediation licenses.
TOE	Bouncy Castle Cryptographic Module Bouncy Castle FIPS Java API version 1.0.2.3	Provides the cryptographic operations used by the TE server, TE Java Agent, and JVM. FIPS certificate number 3514.
Environment	JVM Version 1.8.0	The Java Virtual Machine provides a TLS v1.2 implementation for communications between the TOE and remote trusted IT entities.

[9] Note: These are X.509 certificates that are generated for each customer by Tripwire based on which licenses are purchased. These certificates are changed only when the customer purchases a new or different set of features.

TOE or Environment	Component	Description
Environment	TE Server OS (Refer to Section 1.4.2.1 for additional details)	The operating system on which the TE Server is installed
Environment	Backend DB (Refer to Section 1.4.2.1 for additional details)	The database used by TE server to store all data.
Environment	TE Node (Refer to Section 1.4.2.3 for additional details)	A server or network device being monitored.
Environment	LDAP or Active Directory Server	An authentication server that is required only if the LDAP/Active Directory System login method is selected.

1.5.4.3 Guidance Documentation

Tripwire provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

The Tripwire Enterprise 8.9.1 Supplemental Common Criteria Guidance contains details regarding the common criteria specific instructions and warning provided to administrators.

These activities are documented in:

- Tripwire Enterprise v8.9.1 Reference Guide
- Tripwire Enterprise v8.9.1 User Guide
- Tripwire Enterprise v8.9.1 Installation and Maintenance Guide
- TE Console 8.9.1 Release Notes – June 2022
- Tripwire Enterprise v8.9.1 Hardening Guide
- Tripwire Enterprise v8.9.1 Supplemental Common Criteria Guidance
- Axon Agent and TE Agent Release Notes – June 2022

1.5.5 Logical Boundaries

This section identifies the security functions that the TSF provides**.**

- Intrusion Detection System (IDS)
- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

- Protection of the TSF

1.5.5.1 Intrusion Detection System

The Tripwire Enterprise Agent components of the TOE can collect object attribute information for files, directories, registry keys and registry key values. By comparing collected information against saved values, the agent monitors these resources to detect changes. Once detected, the TE Agent reports the detected change to the Tripwire Enterprise Server to allow administrator specified actions to occur. The TE Agent also checks the current monitored system/state for policy compliance. If an Event Generator is installed on an Agent system, TE can monitor the system for changes made in real-time. With real-time monitoring, the Event Generator continuously reports any detected changes to TE.

For nodes without a TE Agent, the Tripwire Enterprise Server component collects attribute information, compares the information to baselines and initiates administrator specified actions. The Tripwire Enterprise Server can monitor files, command output, and network availability using interfaces that each node provides.

TE Agent uses OpenSSL to create hashes of monitored files. The OpenSSL implementation in the TE Java Agent is not FIPS validated and is not used for the protection of any sensitive information. The TE Axon Agent uses a FIPS validated version of OpenSSL.

The Tripwire Enterprise Server component can perform actions in response to object attribute comparisons, specifically: display integrity check results to the console, send integrity check results to administrators using email, send integrity check results to administrators using SNMP, send a log message to a Syslog server, execute a command on the Tripwire Enterprise Server host operating system, execute a command on the Tripwire Enterprise Agent host operating system, and promote new element versions to be a baseline. For some TE nodes, Tripwire Enterprise Server can also restore a changed element to its baseline state on. TE also uses baselining and restoration to process software installation package data[10].

The syslog server, SMTP server, and recipient of SNMP messages are all external IT entities residing in the environment. It is the responsibility of these IT entities to complete the delivery of such communications. The TOE provides the functionality to send communications to these IT entities in the environment. The TOE does not rely upon these external IT entities to provide security for the TOE.

To test for policy compliance, the administrator downloads & installs TE policies from the Tripwire web site or creates a new TE policy in the Policy Manager. Policy compliance tests can be run on selected nodes and the results viewed in the Policy Manager. TE automatically runs the policy tests whenever a version check results in the creation of change versions for elements of the effective scope of the policy test. Running a policy test involves comparing each change version with the pass/fail criteria defined by the policy test, generating a policy test result for each change version, and updating the compliance statistics for each node in the policy test's effective scope. (This evaluation did not assess the suitability of given policy files to assess the system's compliance against the external policy or guideline, but rather assessed whether the

[10] Software installation package data is a file or directory in a software installation package on a file server.

policy checks specified worked correctly.)

Remediation is the process of resolving failures generated by a policy test. There are two types of remediation: automated and manual. With automated remediation, the TE Agent on the node for which the policy test failed runs a script or performs other actions to bring the node into compliance with the policy test. With manual remediation, a user manually performs the actions to bring the node into compliance with the policy test. In the evaluated configuration, the TOE will be configured to send an alarm when a policy test fails. [11]

The TOE provides a mechanism for authorized users to read the System data[12]. In addition, the TOE protects the collected System data from unauthorized deletion and modification at its own interfaces. It also maintains a defined amount of System data in the event of a failure. When the System data storage capacity is reached, the TOE will shut down and send an alarm. The TOE depends upon the DB to protect the data stored in it from unauthorized access via the DB interfaces.

For the automated Remediation actions, an administrator configures the TOE to execute an administrator-supplied command or script on the Agent node.

1.5.5.2 Security Audit

The TOE provides its own security audit log mechanism, with its own security audit log trail, that can generate records containing TOE management actions and security-related events. These records are referred to as Security Audit Log (SAL) messages. In addition, the TOE generates TE log messages which record a variety of events or activities in a message log. The message log is not considered security-relevant.

The security audit function implements the SAL. The TOE stores the SAL (and message log) in the Database. The term audit data in this ST refers to the SAL messages.

The TOE provides administrators the ability to manage the Tripwire Enterprise Server SAL using administrator console interfaces. Administrators can select which security-relevant events will result in the generation of an audit record. Administrators can read and sort SAL messages in the audit trail based on date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

The TOE protects the SAL messages from unauthorized deletion and prevents modifications at its own interfaces. When the SAL log storage capacity is reached, the TOE maintains all stored audit log messages, shuts down and sends an alarm. The TOE depends upon the DB to protect the data stored in it from unauthorized access via the DB interfaces.

The security audit function relies on the TOE's environment to supply a reliable date and time stamp that the TOE includes in each SAL message. The security audit function also relies upon the TOE's environment to store and protect audit data contained in a SAL message.

[11] All third-party commands, such remediation commands, issued on a device/system in the operational environment are not assured by this evaluation, other than the issuance of the command by TE.

[12] The term "system data" in this ST refers to data collected as a result of monitoring, scanning, and analyzing the monitored system.

1.5.5.3 User Data Protection

The TOE implements access controls on eleven TE objects: nodes, and node groups, rules and rule groups, actions and action groups, tasks and task groups, TE policies, policy tests, and policy test groups. Nodes and node groups are definitions of network entities upon which some integrity check and policy compliance assessment operations are to be performed. Examples of the information the Tripwire Enterprise Server retains about a node or node group are a name, the type of node(s), a description, the number of elements being checked, and last check date/time.

Access to objects is controlled by the Discretionary Access Control (DAC) policy, as defined in FDP_ACF.1 in Section 6.2.3.2, for all available operations on these objects (and their contents). Node objects have access controls that can specify the user role assigned to a user or user group to define the user permissions granted to the user. These attributes are compared against user identities and groups of subjects in order to determine whether the user is granted the user role and therefore whether the requested operations should be allowed. If the access checks fail, access will be refused.

1.5.5.4 Identification and Authentication

The TOE offers a few non security-relevant mediated functions before the user is identified and authenticated. All security-relevant mediated functions require the user to be authenticated. The TOE provides two different login methods:

Password Method	The TOE itself identifies and authenticates the username and password supplied. Always used for identifying and authenticating the built-in “administrator” account.
LDAP/Active Directory Method	The TOE is configured to request authentication services from a LDAP or Active Directory server for all user accounts except the built-in “administrator” account. In this case, TE depends upon the LDAP or AD server to be securely installed and administered.

TE always authenticates Administrator accounts with the Password login method, regardless of the selected login method. The TOE maintains the following security attributes for each user account using the Password Method: user identity, authentication data, user groups, role information, and user permissions. The TOE enforces default password complexity requirements.

Guidance provides recommendations to the users for creating strong passwords. In addition, the TOE is able to lockout user accounts if the number of consecutive unsuccessful authentication failures exceeds a threshold configured by an administrator.

1.5.5.5 Security Management

Tripwire Enterprise Server offers four interfaces for managing the TOE: a graphical user interface (GUI), a command line interface (CLI), a SOAP interface, and the tetool command. The TOE restricts the ability to execute commands by restricting access to these user interfaces, by enforcing user permissions, and by assigning roles to users. TE Server provides management tools for:

- Modifying the behavior of system data collection, analysis, and reaction
- Enabling/disabling integrity check rules
- Enabling/disabling integrity check actions
- Managing the object and user security attributes used by the discretionary access control policy
- Query and add system and audit data
- Query and modify TOE data

The TOE also protects the collected System data from unauthorized deletion and modification at the TOE interfaces.

TE also provides a tool called FastTrack that automatically runs only the first time that the administrator logs into the Console. This tool provides limited capabilities required to setup TE.

1.5.5.6 Protection of the TSF

The TOE ensures that the audit data and System data is available by protecting it from modification and deletion and by maintaining all of the stored data when storage exhaustion occurs.

The Tripwire Enterprise Server is a Java program that runs on its own JVM. The JVM also the implementation of TLS v1.2 used for communications between the TOE and remote IT products. The JVM is configured to use TLS for these communications.

TE nodes provide an interface conformant with their security model for external access to the data objects that the TOE monitors. The TOE does not rely upon the security of communication pathways to nodes for TOE's self-protection.

The TE Server and TE Java Agents include the FIPS certified BCCM that is used to implement TLS to protect communications between the TE server and TE Agents. The TE Axon Agent includes a FIPS-certified OpenSSL cryptographic module (OpenSSL FIPS Object Module SE v2.0.16 library) to implement TLS. The TE Server uses the JVM TLS implementation in the operational environment to protect communications between the TE Server and the remote IT entities. The JVM uses the FIPS compliant BCCM to provide the cryptographic operations. In the evaluated configuration, the TOE must be configured in the FIPS approved mode of operation.[13]

Communication between the server portion of the TOE and a remote DB are protected via TLS provided by the JVM or by the private, secure network on which the DB resides.

1.5.6 Items Excluded from the TOE

This section identifies any items that are specifically excluded from the TOE.

The Evaluated Configuration of the TOE does not include the Remedy AR System tickets Plug-in, the HP Openview Plug-in, or the AAA Monitoring Tool. The Remedy AR System tickets

[13] Bouncy Castle Cryptographic Module (Bouncy Castle FIPS Java API version 1.0.2.3; certificate number3514). The OpenSSL FIPS Object Module SE v2.0.16 library is associated with FIPS certificate number 2398.

Plug-in and the HP Openview Plug-in are extra tools available from Tripwire. The guidance documentation instructs that these tools not be installed. The AAA Monitoring Tool is included within the TOE delivery.

The ability to transfer logs is excluded from the evaluated configuration. This capability requires the use of the Tripwire Log Center. The guidance documentation instructs that this capability not be configured.

In addition, the ability to use the set command to specify the default userid and password during a CLI session is excluded from the evaluated configuration via providing guidance instructing administrators to not use the set command.

The Tripwire Configuration Datamart (AKA Arena) is licensed separately and is excluded from the TOE.

Dynamic Software Reconciliation (DSR) is an external tool that operates as a client of the SOAP API. DSR is an optional add-on and is excluded from the TOE.

The Tripwire Enterprise Common Agent Platform (CAP), including the Security Content Automation Protocol (which is a CAP agent) is excluded from the TOE.

Using TE Agents to monitor directory servers or database servers is excluded from the TOE.

Configurator functionality is available only when Tripwire Enterprise itself is not running.

2 Conformance Claims

2.1 CC Conformance Claims

This ST was developed to Common Criteria (CC) for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

The ST claims to be:

CC Version 3.1 Revision 5 Part 2 extended

CC Version 3.1 Revision 5 Part 3 conformant

2.2 PP and Package Claims

The ST claims to be Evaluation Assurance Level 2 augmented with ALC_FLR.2.

The ST does not claim conformance to any Protection Profiles.

2.3 Conformance Rationale

Not applicable.

3 Security Problem Definition

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

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

3.1 Threats

The threats identified in this section may be addressed by the TOE, the node being monitored or a combination of both. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

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.

3.1.1 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.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.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Attempts by an unauthorized user to access TOE data or security functions may go undetected.

3.1.2 IT System Threats

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

T.SCNCFG	An unauthorized user may exploit improper security configuration settings that 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	An unauthorized user may exploit vulnerabilities that exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	An unauthorized user may gain unauthorized access to an IT System the TOE monitors or a user may perform activities indicative of misuse on an IT system the TOE monitors.
T.INADVE	A user may inadvertently perform an activity or access data for which the user is not authorized on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors due to actions taken by threat actors or unsuspecting users.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the Intrusion Detection System Protection Profile.

P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Assumptions

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

3.3.1 Intended Usage Assumptions

A.ACCESS	The TOE has access to all of the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable[14] to the IT System the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT Systems the TOE monitors.

3.3.2 Physical Assumptions

A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. Application Note: This assumption is also intended to apply to the required items of the IT environment, such as the underlying OS, database, and private physical network.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3.3 Personnel Assumptions

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

[14] Appropriately scalable refers to the TOE being able to handle the volume of processing or traffic flow for systems which it is monitoring.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

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.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.DAC	The TOE must control access to resources based upon the identity of users, groups of users, and roles.

4.2 IT Security Objectives For The Environment

The following IT security objectives for the environment are to be addressed by the TOE's operating environment by technical means. The TOE and the operational environment work

together to address each of the following IT security objectives.

OE.AUDIT_PROTECTION The operational environment will provide the capability to protect audit information.

OE.AUDIT_SORT The operational environment will provide the capability to sort the audit information

OE.TIME The operational environment will provide reliable timestamps to the TOE.

4.3 Non-IT Security Objectives For The Environment

The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied by the TOE's operating environment through application of procedural or administrative measures.

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.

4.4 Security Objectives Rationale

4.4.1 Tracings between Security Objectives and the Security Problem Definition

This section includes two tables that demonstrate that the tracing between the assumptions, threats, and policies to the security objectives is complete. Table 1 provides a tracing between the TOE security objectives and the threats and OSPs. Table 2 provides a tracing between the security objectives on the TOE environment and the assumptions, threats, and OSPs.

	O.PROTECT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.DAC
T.COMINT	X						X	X			X	X
T.COMDIS	X						X	X				X
T.LOSSOF	X						X	X			X	X
T.NOHALT		X	X	X			X	X				
T.PRIVIL	X						X	X				
T.IMPCON						X	X	X				
T.INFLUX									X			
T.FACCNT										X		
T.SCNCFG		X										
T.SCNMLC		X										
T.SCNVUL		X										
T.FALACT					X							
T.FALREC				X								
T.FALASC				X								
T.MISUSE			X							X		
T.INADVE			X							X		
T.MISACT			X							X		
P.DETECT		X	X							X		
P.ANALYZ				X								
P.MANAGE	X					X	X	X				
P.ACCESS	X						X	X				
P.ACCACT								X		X		
P.INTGTY											X	
P.PROTCT									X			

Table 1: Tracings between Threats/OSPs and TOE Security Objectives

	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
A.ACCESS					X			
A.DYNMIC				X	X			
A.ASCOPE					X			
A.PROTCT		X						
A.LOCATE		X						
A.MANAGE				X				
A.NOEVIL	X	X	X					
A.NOTRUST		X	X					
T.IMPCON	X							
P.DETECT						X		
P.MANAGE	X		X	X				
P.ACCESS								X
P.ACCACT						X	X	
P.PROTCT		X						

Table 2: Tracings between Assumptions/Threats/OSPs and Security Objectives for the Environment

4.4.2 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the TOE environment cover that assumption.

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

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

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

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

A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The TOE can only be accessed by authorized users. The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

4.4.3 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

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 O.DAC objective provides an access control policy to protect targeted objects configuration information.

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 addresses this threat by providing TOE self-protection. The O.DAC objective provides an access control policy to protect targeted objects configuration information.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection. The O.DAC objective provides an access control policy to protect targeted objects configuration information.
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, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.
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.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. Static configuration information includes attribute information for targeted objects.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source. The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

	The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

4.4.4 Rationale For Organizational Security Policy Coverage

This section provides a justification that for each organizational security policy, the security objectives address the OSP.

P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data. The OE.TIME objective ensures that the operational environment provide reliable time stamps to the TOE for association with an audit record.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken. The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided

	documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective 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. 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 policy by providing TOE self-protection. The OE.AUDIT_PROTECTION objective ensures that the operational environment provide the capability to protect audit information.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.TIME objective ensures that the operational environment provide reliable time stamps to the TOE for association with an audit record. The OE.AUDIT_SORT objective ensures that the operational environment provide the capability to sort audit information.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of data from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

5 Extended Components Definition

This section defines the newly defined components (also known as extended components) used to define the security requirements for this ST. The extended components defined in this section are based on the existing CC Part 2 SFRs.

5.1 Class FPT: Protection of the TSF

The FPT class, as defined in CC Part 2, addresses requirements for functions providing integrity of TSF data and providing integrity and management of mechanisms that constitute the TSF.

The requirements defined in this class have no dependencies since the stated requirements embody all the necessary security functions.

5.1.1 Time stamps (FPT_STM)

This family, as defined in CC Part 2, defines requirements for reliable time stamp functions for the TOE.

Management: FPT_STM_EXT.1

There are no management functions foreseen.

Audit: FPT_STM_EXT.1

There are no auditable events foreseen.

5.1.1.1 FPT_STM_EXT.1.1 Reliable time stamps from the environment

This extended requirement is necessary since a CC Part 2 SFR does not exist that requires that the TOE obtain a time stamp from the operating environment for use by the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM_EXT.1.1 The TOE shall be able to obtain a time stamp from the operating environment for the TOE's use:

5.2 Class IDS: Intrusion Detection System

An IDS class was created to specifically address the data collected and analyzed by an IDS. The Security Audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this functional class is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data.

The requirements defined in this class have no dependencies since the stated requirements embody all the necessary security functions.

The term node is used to refer to the targeted IT system (server or network device) being monitored.

5.2.1 System Data Collection (IDS_SDC)

This family defines requirements for collecting system data information from nodes. This family has one component: IDS_SDC.1

Management: IDS_SDC.1

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

- Modifying the behavior of system data collection.

Audit: IDS_SDC.1

There are no auditable events foreseen.

5.2.1.1 IDS_SDC.1 System Data Collection

This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the collection of information on system data from nodes.

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_SDC.1.1 The TSF shall be able to collect the following information from the node(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*].**

Application Note: Malicious code includes viruses, worms, simple Trojan horses, etc. Access control configuration includes access control lists, search for writeable files and directories, etc. Service configuration includes identification of network services and/or associated network ports, host services, versions of services, protocols acknowledged by services, etc. Authentication configuration includes cracking passwords, configuration settings (e.g., minimum password length, duration between allowed and required password changes), acceptable authentication means (e.g., NTLM, kerberos), defined guest accounts, account authorisations, etc. Accountability policy configuration includes size of audit trails, whether audit is enabled, what to do when the audit trail fills, etc. Known vulnerabilities is fairly open ended, but may include installed patches, checks for common or default configuration errors, etc.

IDS_SDC.1.2 At a minimum, the TSF shall collect and record the following information from the nodes:

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

b) The additional information specified in the *Details* column of Table 3 System Events.

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	**none**
IDS_SDC.1	Identification and authentication events	**User identity, location, source address, destination address**
IDS_SDC.1	Data accesses	**Object IDS, requested access, source address, destination address**

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

Table 3: System Events

Application Note: In the case where a Sensor is collecting host-based events, for the identification and authentication event, the source address could be a subject IDS on a local machine and the destination is defined by default. For the data access and data introduction events, the source address could be filename and the destination address may be target location for the file.

5.2.2 Analyser Analysis (IDS_ANL)

This family defines requirements for performing analysis function(s) on all IDS data received from the node(s). This family has one component: IDS_ANL.1

Management: IDS_ANL.1

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

- Modifying the behavior of analyzer analysis function(s).

Audit: IDS_ANL.1

There are no auditable events foreseen.

5.2.2.1 IDS_ANL.1 Analyser analysis

This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the analysis of information on system data collected from nodes.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

Application Note: Statistical analysis involves identifying deviations from normal patterns of behavior. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a System. For example, patterns of System settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing System settings or user activity at some point in time with those of another point in time to detect differences.

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

a) Date and time of the result, type of result, identification of data source; and

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

Application Note: The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.

5.2.3 Analyser react (IDS_RCT)

This family defines the response to be taken in case of a detected intrusion. This family has one component: IDS_RCT.1

Management: IDS_RCT.1

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

- Modifying the behavior of analyzer reaction(s).

Audit: IDS_RCT.1

There are no auditable events foreseen.

5.2.3.1 IDS_RCT.1 Analyser analysis

This extended requirement is necessary since a CC Part 2 SFR does not exist that requires a response to occur if an intrusion is detected by the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Note: There must be an alarm, though the operations should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The Analyser may optionally perform other actions when intrusions are detected; these actions should be defined. An intrusion in this requirement applies to any conclusions reached by the analyser related to past, present, and future intrusions or intrusion potential.

5.2.4 System Data Storage (IDS_STG)

This family defines the requirements for the TSF to be able to create and maintain a location to store system data collected from node(s). This family has two components: IDS_STG.1 and IDS_STG.2.

IDS_STG.1 Guarantees of System Data Availability, specifies the guarantees that the TSF maintains over the system data given the occurrence of an undesired condition.

IDS_STG.2 Prevention of System Data Loss, specifies actions in case the location where the system data is stored is full.

Management: IDS_ STG.1

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

- Maintenance of the parameters that control the system data storage capability.

Management: IDS_ STG.2

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

- Maintenance (deletion, modification, addition) of actions to be taken in case of system data storage failure.

Audit: IDS_ STG.1

There are no auditable events foreseen.

Audit: IDS_ STG.2

The following actions should be auditable if IDS_SDC System Data Collection is included in the PP/ST:

- Basic: Actions taken due to the system data storage failure.

5.2.4.1 IDS_STG.1 Guarantee of System Data Availability

This extended requirement is necessary since a CC Part 2 SFR does not exist that requires a response to occur if an intrusion is detected by the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_STG.1.1 The TSF shall protect the stored System data from unauthorised deletion.

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

Application Note: Authorised deletion of data is not considered a modification in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The TSF shall ensure that [**assignment: *metric for saving System data***] System data will be maintained when the following conditions occur: [**selection: *System data storage exhaustion, failure, attack***].

Application Note: The amount of System data that could be lost under the identified scenarios needs to be defined.

5.2.4.2 IDS_STG.2 Prevention of System Data loss

This extended requirement is necessary since a CC Part 2 SFR does not exist that requires a response to occur if an intrusion is detected by the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6 Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST.

TOE Security Functional Requirements (from CC Part 2)	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1a-d	Cryptographic operation
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication with a third party
FIA_UID.1	Timing of identification with a third party
FMT_MOF.1a-c	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FTA_SSL.4	User-initiated termination

Extended Security Functional Requirements	
FPT_STM_EXT.1	Reliable time stamps from the environment
IDS_SDC.1	System data collection
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_STG.1	Guarantee of system data availability
IDS_STG.2	Prevention of system data loss

Table 4: Security Functional Requirements

6.1 Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify the operations completed in this ST by the ST author.

Assignment made in ST: **indicated with bold text**

Selection made in ST: indicated with underlined text

Refinement made in ST: ***additions indicated with bold text and italics***

deletions indicated with strike-through ~~bold text and italics~~

Iteration made in ST: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

6.2 Security Functional Requirements

6.2.1 Security audit (FAU)

6.2.1.1 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 basic level of audit; and

c) Access to the System and access to the TOE and System data, *TOE integrity checks on monitored nodes*.

Application Note: The auditable events for the basic level of auditing are included in Table 5: Auditable Events.

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access

Component	Event	Details
FAU_GEN.1	TOE integrity checks on monitored nodes.	
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
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.1a, b, c	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	Object identity being accessed
FMT_MSA.1	All modifications of the values of security attributes	
FMT_SMF.1	Use of the management functions	

Table 5: Auditable Events

ST Application Note: For the basic level of auditing of FMT_MSA.3, the CC Part 2 requires the following actions be audited: 1) modifications of the default setting of permissive or restrictive rules and 2) all modifications of the initial values of security attributes to be audited. As noted in FMT_MSA.3 below, the TOE does not allow alternative initial values to be specified when an object or information is created, so this is not an auditable event for the TOE.

Application Note: The IDS_SDC and IDS_ANL requirements address the recording of results from IDS scanning, sensing, and analyzing tasks (i.e., 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 (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **the additional information specified in the Details column of Table 5: Auditable Events**.

6.2.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator role and a user with both Load Log Manager and Delete Log Message permission** with the capability to read **all audit information** from the audit records.

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

6.2.1.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users

that have been granted explicit read-access.

6.2.1.4 FAU_SAR.3 Selectable audit review

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

6.2.1.5 FAU_SEL.1 Selective audit

FAU_SEL.1 The TSF shall be able to select the set of events to be audited from the set of auditable events based on the following attributes**:**

a) event type

b) **None**.

6.2.1.6 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that **all** stored audit records will be maintained when the following conditions occur: audit storage exhaustion.

6.2.1.7 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall prevent audited events, except those taken by the authorised user with special rights and **send an alarm** if the audit trail is full.

6.2.2 Cryptographic Support (FCS) [15]

6.2.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate ***asymmetric*** cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA and ECC schemes** and specified cryptographic key sizes **2048, 3072 bits for RSA and P-256, P-384, P-521 for ECC** that meet the following: **FIPS PUB 186-4, "Digital Signature Standard (DSS)" (Appendix B.3for RSA and Appendix B.4 for ECC)**.

6.2.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **cryptographic key zeroization method** that meet the following: **FIPS 140-2**.

[15] The TOE includes a FIPS certified module, BCCM (FIPS certificate number 2768). TE Agent uses OpenSSL, which is not FIPS validated, to create hashes of monitored files.

6.2.2.3 FCS_COP.1a Cryptographic operation (hashing)

FCS_COP.1.1a The TSF shall perform **cryptographic hashing operations** in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512** and cryptographic key sizes **not applicable**[16] that meet the following: **FIPS Pub 180-3, "Secure Hash Standard"**.

ST Application Note: The TSF includes two cryptographic implementations of these hashing operations. The BCCM provides all hashing operations except for file attribute hashing.

6.2.2.4 FCS_COP.1b Cryptographic operation (encryption/decryption)

FCS_COP.1.1b The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **AES operating in CBC, and GCM mode** and cryptographic key sizes **128, 192, and 256 bits** that meet the following: **FIPS Pub 197, "Advanced Encryption Standard (AES)"**.

6.2.2.5 FCS_COP.1c Cryptographic operation (RSA signature services)

FCS_COP.1.1c The TSF shall perform **RSA digital signature generation and verification** in accordance with a specified cryptographic algorithm **RSA Digital Signature Algorithm** and cryptographic key sizes **2048 and 3072 bits** that meet the following: **FIPS Pub 186-4, "Digital Signature Standard (DSS)"**.

6.2.2.6 FCS_COP.1d Cryptographic operation (message authentication code)

FCS_COP.1.1d The TSF shall perform **message authentication code operations** in accordance with a specified cryptographic algorithm **HMAC-SHA-1, HMAC-SHA-256** and cryptographic key sizes **32-byte** that meet the following: **FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code" and FIPS Pub 180-3, "Secure Hash Standard"**.

6.2.3 User data protection (FDP)

6.2.3.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **Discretionary Access Control Policy** on

Server Subjects: All server users;

Server Objects: nodes and node groups, rules and rule groups, actions and action groups, tasks and task groups, TE policies, policy tests and policy test groups

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

[16] SHA-1 does not use cryptographic keys in its calculation. The message digest size is 160, 224, 256, 384, or 512 bits, depending upon the algorithm.

6.2.3.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Discretionary Access Control Policy** on objects based on the following:

Server subject attributes: user identity, group memberships and user roles

Server object attributes: access controls (ACs) (which is comprised of user identity or group membership and the assigned user role pair).

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) If an AC has not be created for the TE object or any of the groups containing the TE object and if the user role grants the requesting user identity the requested access, the requested access is allowed;

b) If the AC (via the assigned user role) grants the requesting user identity the requested access, the requested access is allowed;

c) If the user identity is a member of a group and the AC grants the group the permissions of the user role in a matching TE object's access control, and the permission grants the requested access, the requested access is allowed;

d) Otherwise access is denied, unless access is explicitly authorized in accordance with the rules specified in FDP_ACF.1.3.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

a) If the server subject is the default administrator account, the requested access is allowed.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

6.2.4 Identification and authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within **a settable, non-zero number** ***of*** unsuccessful authentication attempts occur related to **administrative user logins**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall **lock out the user account for a settable number of minutes and if configured, send an e-mail notification to the user**.

6.2.4.2 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) User identity

b) Authentication data

c) User group memberships

d) Role.

6.2.4.3 FIA_SOS.1 Verification of secrets

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

- **Minimum password length 8 or greater**
- **Minimum number of numeric characters 1 or greater**
- **Minimum number of uppercase characters 1 or greater**
- **Minimum number of non-alphanumeric characters 1 or greater.**
- **Not reuse any of the user's previous 100 passwords.**

6.2.4.4 FIA_UAU.1 Timing of authentication with a third party

FIA_UAU.1.1 The TSF shall allow **SOAP locale management, twtool URL generation, twtool, common option settings, twtool version display, twtool help** 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.

6.2.4.5 FIA_UID.1 Timing of identification with a third party

FIA_UID.1.1 The TSF shall allow **SOAP locale management, twtool URL generation, twtool, common option settings, twtool version display, twtool help** 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.

6.2.5 Security management (FMT)

6.2.5.1 FMT_MOF.1a Management of security functions behavior

FMT_MOF.1.1a The TSF shall restrict the ability to modify the behavior of the functions **of System data collection, analysis and reaction** to **authorised system administrators.**

6.2.5.2 FMT_MOF.1b Management of security functions behavior

FMT_MOF.1.1b The TSF shall restrict the ability to disable, enable the functions **related to the specification of integrity check rules** to **authorised system administrators.**

Application Note: For TE, the ability to enable integrity check rules is interpreted as the ability to execute an integrity check. The ability to disable integrity check rules is interpreted as the ability to perform an operation that causes the check to not execute, such as to delete the rules, delete the elements or disable a scheduled task.

6.2.5.3 FMT_MOF.1c Management of security functions behavior

FMT_MOF.1.1c The TSF shall restrict the ability to disable, enable the functions **related to the specification of integrity check actions** to **authorised system administrators.**

Application Note: For TE, the ability to enable integrity check action is interpreted as the ability to execute an action, directly or indirectly. The ability to disable integrity check actions is interpreted as the ability to perform an operation that causes the

action to not be used, such as to delete the action, or disable a scheduled task.

6.2.5.4 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Discretionary Access Control Policy** to restrict the ability to query, modify, delete the security attributes **ACs** to **Administrator, and users with the appropriate Create ACL permission**.

6.2.5.5 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **Discretionary Access Control Policy** to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow ***~~the~~* no user role** to specify alternative initial values to override the default values when an object or information is created.

6.2.5.6 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query, **and add** the **System and audit data** ***and shall restrict the ability to*** *query,* ***create and*** *modify* ***all other TOE data*** to **the roles as defined in** Table 6.

Role	**Action**	**TOE Data**
Administrator, Power User Rule Manager Users with the associated Rule Management Link and Load permissions and the corresponding permissions: To create, Create To create command output rules, Create and Create Command Output Rules To delete, Delete To update, Update To update command output rules, Update and Update Command Output Rules	modify	integrity check rules
Administrator Power User Rule Manager Rule User Monitor User Regular User Users with Rule Management Load permission	query	integrity check rules

Role	Action	TOE Data
Administrator Power User Users with the associated Action Management Load permission and the corresponding permissions: To create, Create, Create Execution Actions, and Link To delete, Delete and Link To update, Update, Update Execution Actions, and Link To update (move around file hierarchy), Update, Update Execution Output Rules, and Link	modify	integrity check actions
Administrator Power User Monitor User Regular User Users with the Action Management Load permission	query	integrity check actions
Not allowed for any role	modify	current attributes of elements collected from nodes
Administrator Power User Monitor User Regular User Users with the Node Management Load and View permission	query	current attributes of elements collected from nodes
Administrator User Administrator Users with the User Management Load permission and the corresponding User Management permissions, if applicable: Create, Delete, Update permissions.	create modify query	user security attributes and user role membership
Administrator	query modify	all integrity check ‘User’ reports stored on the server
Power User Regular User Monitor User Users with the Report Management Load permission	create	their own integrity check ‘User’ reports stored on the server
Monitor User Users with the Report Management Load permission	modify	their own integrity check ‘User’ reports stored on the server

Role	Action	TOE Data
Administrator Users with the Report Management permissions: Load and Manage System Reports	modify	integrity check ‘System’ reports stored on the server
Administrator Power User Monitor User Regular User Users with the Report Management Load permission	query	integrity check reports stored on the server
Not allowed for any role	add	audit data (SAL messages) stored on the server
Administrator Users with Load Log Manager and Delete Log Message permissions	query delete	audit data (SAL messages) stored on the server
Administrator Power User Monitor User Regular User Users with Node Management Load and View permissions	query	System data
Not allowed for any role	add	System data
Administrator users with the Miscellaneous Manage Login Methods permission	modify query	login method and authentication settings
Administrator Power User Monitor User Regular User Users with Node Management Load and View permissions	query	Local Variable
Administrator Power User Users with the Create Variable and Node Management Load and View permission	create	Local Variable
Administrator Power User Users with the Update Variable and Node Management Load and View permission	modify	Local Variable

Role	Action	TOE Data
Administrator Power User Users with the Delete Variable permission and Node Management Load and View permission	delete	Local Variable
Administrator Power User Users with Load Variable permissions	query	Global Variable
Administrator Power User Users with the Create Variable permission	create	Global Variable
Administrator Power User Users with the Update Variable permission	modify	Global Variable
Administrator Power User Users with the Delete Variable permission	delete	Global Variable
Administrator Power User Users with the permissions to create, update, delete, close, assign remediation jobs Users with the permission to approve remediation actions-	create modify query	Remediation Work Orders
Administrator Power User Monitor User Regular User	query	All collected System data

Table 6: TOE Management

6.2.5.7 FMT_SMF.1 Specification of Management Functions

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

- **management of System data collection, analysis and reaction**
- **specification of integrity check rules**
- **specification of integrity check actions**
- **management of access control security attributes**
- **management of TOE data**.

6.2.5.8 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the ***following*** roles **User Administrator, Monitor User, authorised system administrators[17], Administrator, Policy Manager, Policy User, Power User, Regular User, Rule Manager, and Rule User**.

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

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

6.2.6.2 FPT_STM_EXT.1 Reliable time stamps from the environment

FPT_STM_EXT.1.1 The TOE shall be able to obtain a time stamp from the operating environment for the TOE's use.

6.2.7 TOE access (FTA)

6.2.7.1 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.8 Intrusion Detection System (IDS)

6.2.8.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The TSF shall be able to collect the following information from the node(s):

a) Data accesses, security configuration changes, data introduction, access control configuration, authentication configuration., accountability policy configuration; and

b) **none.**

IDS_SDC.1.2 At a minimum, the TSF shall collect and record the following information from the node:

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

b) The additional information specified in the *Details* column of Table 7 System Events.

Component	Event	Details
IDS_SDC.1	Data accesses	**Object IDS, requested access, source address, destination address**
IDS_SDC.1	Security configuration changes	**Source address, destination address]**

[17] Users assigned any role or permission, except User Administrator and Monitor User, are considered authorised system Administrators.

Component	Event	Details
IDS_SDC.1	Data introduction	**Object IDS, location of object, source address, destination address]**
IDS_SDC.1	Access control configuration	**Location, access settings]**
IDS_SDC.1	Authentication configuration	**Account names for cracked passwords, account policy parameters** [18]
IDS_SDC.1	Accountability policy configuration	**Accountability policy configuration parameters**

Table 7: System Events

6.2.8.2 IDS_ANL.1 Analyser analysis

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

a) integrity; and

b) **policy compliance tests**.

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

a) Date and time of the result, type of result, identification of data source; and

b) **For nodes with an Agent installed, the user that made the change**.

Application Note: The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.

6.2.8.3 IDS_RCT.1 Analyser react

IDS_RCT.1.1 The TSF shall send an alarm to **any of the following as configured by an administrator: administrator console, administrator email address, SNMP server, or syslog server** and take **one or more of the following actions as configured by an administrator**

a) Execute a command on the TE Agent host operating system

b) Promote new resource version to be a baseline, or

c) Restore a changed resource to its baseline

when an intrusion is detected.

6.2.8.4 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1 The TSF shall protect the stored System data from unauthorised deletion.

IDS_STG.1.2 The TSF shall protect the stored System data from modification.

IDS_STG.1.3 The TSF shall ensure that **all stored** System data will be maintained when the following conditions occur: System data storage exhaustion.

[18] The TOE collects information on user account configuration changes, such as minimum password length settings, but does not collect cracking password information.

6.2.8.5 IDS_STG.2 Prevention of System Data loss

IDS_STG.2.1 The TSF shall prevent System data, except those taken by the authorised user with special rights and send an alarm if the storage capacity for collected System data has been reached.

6.3 TOE Security Assurance Requirements

The Security assurance requirements (SARs) provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment). The table below identifies the security assurance requirements for the TOE drawn from CC Part 3: Security Assurance Requirements that meet an Evaluation Assurance Level 2 augmented with ALC_FLR.2 as defined by the CC.

Assurance Class	Assurance Component ID	Assurance Component Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample

Assurance Class	Assurance Component ID	Assurance Component Name
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 8: Security Assurance Requirements

6.4 Security Requirements Rationale

6.4.1 Rationale For Not Satisfying All Dependencies

This section includes a table of all the TOE security functional requirements and their associated dependencies with a rationale for any dependencies that are not satisfied.

SFR	Dependencies	Met by the TOE?
FAU_GEN.1	FPT_STM.1	Addressed by OE.TIME on the operational environment and FPT_STM_EXT.1
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes, via FAU_STG.2 which is hierarchical to FAU_STG.1
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Yes
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
FCS_COP.1a-d	FDP_ITC.1 or FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4	Yes
FDP_ACC.2	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes, via FDP_ACC.2 which is hierarchical to FDP_ACC.1 Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	None	N/A
FIA_SOS.1	None	N/A

FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	None	N/A
FMT_MOF.1a, b, c	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes, via FDP_ACC.2 which is hierarchical to FDP_ACC.1 Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes
FMT_SMR.1	FIA_UID.1	Yes
FMT_SMF.1	None	N/A
FPT_ITT.1	None	N/A
FPT_STM_EXT.1	None	N/A
FTA_SSL.4	None	N/A
IDS_SDC.1	None	N/A
IDS_ANL.1	None	N/A
IDS_RCT.1	None	N/A
IDS_STG.1	None	N/A
IDS_STG.2	None	N/A

Table 9: SFR Dependencies

6.4.2 TOE SFR to TOE Security Objective Tracings

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.DAC	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION

FAU_GEN.1										X					
FAU_SAR.1						X									
FAU_SAR.2							X	X							
FAU_SAR.3						X								X	
FAU_SEL.1						X				X					
FAU_STG.2	X						X	X	X		X				X
FAU_STG.4									X	X					
FCS_CKM.1	X														
FCS_CKM.4	X														
FCS_COP.1a	X	X		X											
FCS_COP.1b-d	X														
FDP_ACC.2												X			
FDP_ACF.1												X			
FIA_AFL.1								X				X			
FIA_ATD.1								X				X			
FIA_SOS.1								X							
FIA_UAU.1							X	X				X			
FIA_UID.1							X	X				X			
FMT_MOF.1a	X						X	X							
FMT_MOF.1b	X						X	X							
FMT_MOF.1c	X						X	X							
FMT_MSA.1	X						X					X			
FMT_MSA.3	X					X	X					X			
FMT_MTD.1	X						X	X			X				
FMT_SMF.1	X						X	X			X	X			
FMT_SMR.1								X							
FPT_ITT.1	X										X				
FTA_SSL.4						X	X								
ADV_ARC.1	X					X		X		X	X				
FPT_STM_EXT.1										X			X		
IDS_SDC.1		X	X												
IDS_ANL.1				X											
IDS_RCT.1					X										
IDS_STG.1	X						X	X	X		X				
IDS_STG.2									X						

Table 10: Mappings between TOE SFRs and Security Objectives

6.4.3 TOE SFR Rationale

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

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

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.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.1a, b, c]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE restricts the ability to query, modify, or delete ACs to the Administrator [FMT_MSA.1]. By default, the TOE creates every server object without an AC. Subsequently, access can be granted to other users, but there is no method to specify access other than the default during creation [FMT_MSA.3]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TE Server and TE Java Agent include the FIPS certified Bouncy Castle Cryptographic Module to provide the cryptography used by the JVM TLS implementation which protects remote communications with the TOE. The TE Axon Agent includes a FIPS certified OpenSSL cryptographic module to implement TLS. Both cryptographic modules perform key generation, key distribution, key destruction, hashing, encryption/decryption, public key generation, message authentication code and digital signing. [FCS_CKM.1, FCS_CKM.4, FCS_COP.1a-d]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted between distributed TOE components [FPT_ITT.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

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

A 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]. The TOE uses one-way hash function to store static information used to determine the integrity of files and registry entries [FCS_COP.1a].

O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS. A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1].
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1]. The TOE uses one-way hash function to store static information used to determine the integrity of files and registry entries [FCS_COP.1a].
O.RESPON	The TOE must respond appropriately to analytical conclusions. The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SEL.1]. By default, the TOE creates every server object without an AC. Subsequently, access can be granted to other users, but there is no method to specify access other than the default during creation [FMT_MSA.3]. The TOE must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3]. The TOE provides the ability for users to terminate their session [FTA_SSL.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.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.1a, b, c]. The TOE restricts the ability to query, modify, or delete ACs to the Administrator [FMT_MSA.1]. By default, the TOE creates every server object without an AC. Subsequently, access can be granted to other users, but there is no method to specify access other than the default during creation [FMT_MSA.3]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TOE provides the ability for users to terminate a session with the TOE by logging into the TOE from another entity causing the TOE to terminate the original session [FTA_SSL.4]
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. The TOE provides restrictions on the complexity of passwords, including password length and password reuse [FIA_SOS.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE provides the ability to disable (lock out) user accounts after a consecutive number of unsuccessful authentication attempts [FIA_AFL.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.1a, b, c]. Only authorized administrators of the System may query and add System and audit 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 TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.

	The TOE is required to protect the audit data from unauthorized deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The System must prevent the loss of audit data in the event its audit trail is full [IDS_STG.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1]. Time stamps associated with an audit record must be reliable [FPT_STM_EXT.1].
O.INTEGR	The TOE must ensure the integrity of all audit and System data. The TOE is required to protect the audit data from unauthorized deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted between distributed TOE components [FPT_ITT.1]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].
O.DAC	The TOE must control access to resources based upon the identity of users, groups of users, and roles. The TOE must enforce the DAC policy on all server subjects for all available operations on nodes and node groups (and their contents) [FDP_ACC.2]. The TOE must enforce the rules defined by the DAC policy based on server object ACs and user security attributes (user ID, groups of

users, and roles). The ACs and user security attributes are compared to determine whether the requested operation should be allowed [FDP_ACF.1]. The TOE maintains security attributes for each user, including user ID, authentication data, group memberships, and roles [FIA_ATD.1]. The TOE successfully identifies and authentications users before allowing any TSF-mediated actions for that user [FIA_UAU.1, FIA_UID.1]. The TOE provides the ability to disable (lock out) user accounts after a consecutive number of unsuccessful authentication attempts [FIA_AFL.1]. The TOE restricts the ability to query, modify, or delete ACs to an Administrator [FMT_MSA.1]. By default, the TOE creates every server object without an AC. Subsequently, access can be granted to other users, but there is no method to specify access other than the default during creation [FMT_MSA.3]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1].

OE.AUDIT_PROTECTION The operational environment will provide the capability to protect audit information.

The TOE is required to protect the audit data from unauthorized deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE protects the audit data from deletion at its own interfaces. The audit data is stored in the database in the operational environment. The TOE relies upon the database to provide access control mechanisms to protect the audit information.

OE.AUDIT_SORT The operational environment will provide the capability to sort audit information.

The operational environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3]. The TOE provides interfaces to allow authorized users to review, sort and manage the audit trail. Since the audit data is stored in the database in the operational environment, the TOE relies upon the database to provide the capabilities necessary for reviewing, sorting, and managing the audit trail.

OE.TIME The operational environment will provide reliable time stamp to the TOE.

Time stamps associated with an audit record must be reliable [FPT_STM_EXT.1]. The TOE relies upon hardware and operating system in the operational environment to provide reliable time stamps upon request.

6.4.4 SAR Rationale

The TOE and this ST are EAL2 conformant, augmented with ALC_FLR.2.

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for

design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the system may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the system will have incurred a search for obvious flaws to support its introduction to the non-hostile environment. EAL2 was augmented with ALC_FLR.2 to provide assurance that Tripwire follows good, commercial practices with respect to security flaw reporting between the vendor and the users of the TOE.

7 TOE Summary Specification

This chapter describes the TOE security functions.

7.1 Intrusion Detection System

The TOE provides three main IDS capabilities: File Integrity Monitor, Compliance Policy Manager, Remediation Manager.

7.1.1 File Integrity Monitor

The TOE manages and monitors the configuration and status of a set of external networked components called nodes. Discovered unauthorized or unexpected modifications to nodes are reported using one or more of the available notification mechanisms. Users can configure other actions to be performed automatically when changes are detected, including for some node types, restoring the baseline configuration.

Monitoring the integrity of a node consists of taking a node snapshot (a collection of the current values of a specific set of node elements) and comparing it against the node's baseline (a previously stored set of presumed good values for those node elements). If the resource's attributes differ between the snapshot and the baseline, the resource is determined to have changed and one or more of the available notification mechanisms may be invoked depending upon the administrator's configuration choices. Administrators define the frequency of monitoring specific nodes. Frequency can be any interval of N minutes, hourly, daily, weekly, monthly, or just once.[19]

For nodes without a TE Agent installed, the Tripwire Enterprise Server performs the necessary steps to monitor the node using the IP address, communication protocols, and authentication credentials offered by the specific node. For TE Agent nodes, the agent performs the integrity check and passes the results to the Tripwire Enterprise Server for auditing, notification and reporting. Node elements are specific to the type of node and how the monitoring is configured. Monitoring can be configured to include the content and attributes of files, registry values, and other node configuration parameters.

Other node configuration parameters can be collected and monitored using a command output capture rule or command output validation rule which runs a command on a node or device to generate and capture the output. This information can then be captured in a snapshot for subsequent monitoring. For example, the physical memory capacity of servers or the software and firmware version numbers can be monitored using this mechanism.

The date and time of the result, type of result, and identity of data source are recorded as a result of each integrity scan. For nodes with an Agent installed, the user that made the change is also recorded.

Node snapshots are saved as a record of a node's configuration at a specific point in time. Each node may have an unlimited number of snapshots, but only one is flagged as the current baseline.

Authorized administrators use the TOE's Graphical User Interface to configure the integrity

[19] The time between snapshots is a window of time in which an attribute could be changed and then changed back with no detection.

checking mechanism, creating integrity check rules that specify node elements and corresponding attributes to monitor. Note that the administrator can make changes to node baselines in addition to using the TOE to perform integrity checks at regular intervals.

The TOE can monitor various types of nodes and node elements. While some types of nodes require the installation of a Tripwire Enterprise Agent on the node, other node types provide suitable interfaces and do not require the installation of a Tripwire Enterprise Agent. In the latter case, the monitoring is handled by the Tripwire Enterprise Server. The following node types and elements can by monitored:

- Agent Nodes requiring Tripwire Enterprise Agents (mostly operating systems)
  - Files (the file element attributes monitored are listed below)
  - Directories (the directory element attributes monitored are listed below)
  - Registry keys and values (for the Windows operating system only, the registry element attributes monitored are listed below)
- TE Nodes not requiring TE Agents
  - Files content attributes
  - Command output (run command and capture output to check node settings or parameters)
  - Availability (network connectivity)

In the case of nodes hosting Tripwire Enterprise Agents, the TOE can monitor file, directory, and registry keys/values as follows:

- UNIX file element attributes monitored:
  - The access control list for a file or directory
  - The last date and time when a file or directory was accessed
  - The last date and time when file or directory metadata was modified (or created)
  - The UNIX user group that owns a file or directory
  - The MD5[20] hash for a file
  - The last time file or directory content was changed by a user
  - A hash that associates a file with a software-installation package, also referred to as the "packages" attribute
  - Permission and file mode bits
  - The SHA-1, SHA-256, or SHA-512[21] hash for a file
  - The size of a file
  - The owner of the file or directory
- Windows file element attributes monitored:

[20] MD5 is not a FIPS Approved algorithm. Guidance instructs users to use SHA-1 only.

[21] This implementation of SHA is not FIPS certified.

  - The last time a file or directory was accessed by a user
  - Archive flag
  - A flag that indicates whether the file or directory is compressed
  - The date and time when a file or directory was created
  - A list that specifies the level of file or directory access granted to Windows users or user groups
  - The Windows user group that owns a file or directory
  - Hide flag
  - The MD5 hash of a file
  - Offline flag
  - The owner of the file
  - A hash or version string that associates a file with a software-installation package, also referred to as the “packages” attribute
  - Read-only flag
  - A list that controls the generation of audit log entries for attempts to access a securable object.
  - The SHA-1, SHA-256, or SHA-512 hash of a file
  - The size of a file
  - The number of alternate data streams on a file or directory
  - The MD5 hash for the file or directory alternate data stream(s)
  - The SHA-1, SHA-256, or SHA-512 hash for the file or directory alternate data stream(s)
  - System flag
  - Temp flag
  - The date and time when file or directory content was last changed
  - DACL that identifies the users and groups allowed or denied access to the object
  - SACL that controls how the system audits attempts to access the object
- Windows registry key element attributes monitored:
  - A list that specifies the level of access granted to Windows users or user groups
  - Indicates the type of data in a value
  - The Windows user or user group that owns a registry key
  - The MD5 hash of data in a registry value
  - The owner of a registry key
  - A string that associates a registry key or value with a software-installation package
  - A list that controls the generation of audit log entries for attempts to access a registry key
  - The SHA-1, SHA-256, or SHA-512 hash of data in a value
  - The size of data in a value

- The date and time when a key was last changed
- DACL that identifies the users and groups allowed or denied access to the object
- SACL that controls how the system audits attempts to access the object

Authorized administrators configure the integrity checking mechanism by specifying actions to take in response to integrity checks. For actions relying upon an external IT entity (i.e., email, SNMP, syslog), the TOE is only capable of sending the integrity check results or log message. The TOE relies upon the operational environment to complete delivery. The TOE is capable of the following actions when a change is detected.

- Display integrity check results to the console
- Send integrity check results to administrators using email
- Send integrity check results to administrators using SNMP
- Send a log message to a Syslog server
- Execute a command on either the Tripwire Enterprise Server or a node using an Agent
- Promote new element versions to baseline
- Restore a changed element to its baseline state (although not all types of elements can be restored).

The baseline and restoration features are also used by TE to process software installation package data from file servers.

If auditing is enabled in the underlying operating system, TE can be configured to collect the user ID that performed the monitored event/action.

This component collects the following system events: data accesses, security configuration changes, data introduction, and access control configuration. Data accesses events are collected by configuring TE monitoring specific files or directories for read, write and delete access. (Read access is determined by monitoring the file access time.) Security configuration changes are collected by configuring TE to monitor the specific file or registry entry in which the security configuration settings are stored. Data introduction events are collected by configuring TE to monitor a directory for new files or directories being added and a registry for new entries. Access control configuration events are collected by monitoring the permission bits on UNIX or the ACLs on Windows for changes to the lists.

TE can be configured to use the information obtained from the audit records stored and collected by the underlying OS to determine the identity of the entity requesting access to, including modifications to, the objects.

If an Event Generator is installed with TE Agent on Windows and UNIX file servers, TE can monitor the system for changes made in real-time. With real-time monitoring, the Event Generator monitors the Agent's OS, as well as the registry if the Agent is a Windows server continuously reports any detected changes to the TE Agent, becoming the audit event source for an Agent system. At an administrator defined interval, the TE Agent runs a version check of the monitored objects for which the current collection of audit events indicates a change. At the end of the version check, the Agent forwards the audit events and all new change versions to the TE server. The Event Generator can also be configured to identify the entity requesting access or

performing the event.

7.1.2 Compliance Policy Manager

The administrator defines TE policies. TE policies can be downloaded from the Tripwire web site or the administrator can define the TE policy. Loaded TE policies can be used to assess compliance with federal regulations or internal guidelines.[22] New TE policy tests must define the test's effective scope and pass/fail criteria.

Once the new policy test is defined, the policy test should be run manually.

When running a policy test, the TOE compares the current version of each element of the test's effective scope with the pass/fail criteria defined by the policy test. The TOE generates test results for each current version indicating whether or not the policy test passed or failed. The TOE can also create compliance statistics for each node in the test's effective scope.

After the initial execution of a policy test, the TE server automatically runs the policy test whenever a version check results in the creation of change versions for elements of the test's effective scope.

This component collects the following system events: security configuration changes, authentication configuration and accountability policy configuration

The date and time of the result, type of result, and identity of data source are recorded as a result of each policy compliance test. For nodes with an Agent installed, the user that made the change is also recorded.

7.1.3 Remediation Manager

Remediation is the process of resolving failures generated by a policy test. There are two types of remediation: automated and manual. With automated remediation, the TE Agent on the node that the policy test failed runs a script or performs other actions to bring the node into compliance with the policy test. With manual remediation, a user manually performs the actions to bring the node into compliance with the policy test. In the evaluated configuration, the TOE will be configured to send an alarm when a policy test fails.

7.1.4 System Data Storage

The collected System data (object attribute information) collected by both the TE Server and TE Agents are stored in the database.

7.1.5 SFR Mapping

The IDS function is designed to satisfy the following security functional requirements:

[22] The evaluation did not test federal compliance validation, such as SCAP. The evaluation did not include an assessment of whether or not a policy file is sufficient to confirm the external policy or guideline. The evaluation only assessed whether or not the checks and tests in the policy file work correctly.

- FCS_COP.1a: TE Agents uses OpenSSL to provide the SHA hashing capability used to monitor files and Windows registry entries on the nodes.
- IDS_SDC.1: The Tripwire Enterprise Agents component of the TOE contributes to the monitoring of files, directories, and registry keys and values of node resource(s) by collecting object attribute information. The collected information is stored in the database. The Tripwire Enterprise Server can monitor files, command output, and availability of node resource(s) by collecting object attribute information. Since the TOE does not collect account names for cracked passwords, this detailed information is not included in the collected data.
- IDS_ANL.1: The Tripwire Enterprise Server component or the Tripwire Enterprise Agent can compare collected attribute information from node resources using administrator-configured rules. These rules determine the frequency of the monitoring activity and the action taken by the TOE when a change is detected. The policy manager performs the analysis features used to assess compliance.
- IDS_RCT.1: The File Integrity Monitor of the Tripwire Enterprise Server component can perform actions in response to element attribute comparisons, specifically: display integrity check results to the console, send integrity check results to administrators using email, send integrity check results to administrators using SNMP, send a log message to a Syslog server, execute a command on either the Tripwire Enterprise Server host operating system or on the Tripwire Enterprise Agent host operating system, promote new element versions to baseline, restore a changed element to its baseline state (note that not all types of elements can be restored). The Remediation Manager resolves failures generated by a policy test using either automated and manual remediation.
- IDS_STG.1: The Tripwire Enterprise Server component protects the collected system data from unauthorized deletion and prevents modifications to the collected system data at the TOE's interfaces. In addition, the TOE ensures that collected system data will be saved when storage exhaustion occurs. The TOE depends upon the DB to protect the data stored in it from unauthorized access via the DB interfaces.
- IDS_STG.2: If the system data storage location becomes full, the TOE will send an alarm and the system will shut down.

7.2 Security audit

The TOE provides its own security audit log (SAL) mechanism that can generate records containing TOE management actions and security-related events. These records are referred to as Security Audit Log (SAL) messages. The TOE stores its SAL messages in the database.

Each SAL message includes date and time of the event, category (type of event), subject identity (system-initiated event or user-initiated event), and the outcome (success or failure) of the event. Additional information is stored in the SAL message for certain types of events. The object IDS and requested access type are recorded for "access to the TOE and System data" audit events. The user identity and location are recorded for user identification and authentication audit events. The user identity is recorded is recorded for "modifications to the group of users that are part of a role" audit events.

The auditable events stored in the SAL include:

- Successful and unsuccessful attempts to start-up and shutdown the Security Audit Log component.
- Successful and failed requests to perform an operation that requires access to an object covered by the SFP
- Successful and unsuccessful attempts to read audit records
- All modifications to audit configuration
- Use of the management functions:
    - Specification of integrity check rules,
    - Specification of integrity check actions,
    - Promotion of collected object attributes to baselines,
    - Review of integrity check reports.
    - Specification of role assignments
- Successful and unsuccessful user identification and authentication
- Modifications to the values of security attributes and TSF data
- Modifications to the group of users that are part of a role
- Access to the System
- Access to the TOE and System data
- TOE integrity checks on monitored nodes

The TOE provides the ability for administrators to select which type of events will generate an audit record (pre-selection).

The Log Manager in the GUI provides the ability for users with the Administrator role and users with both the Load Log Manager and Delete Log Message permissions to view and configure the Security Audit Log trail. This includes the ability to delete audit records. To sort the SAL messages displayed by the Log Manager, the administrative user simply clicks on the column header of which sorting is desired.

The TOE does not provide a mechanism for modifying the audit records. When the SAL trail is full, the TOE throws an exception (alarm) to the console/monitor/screen and the TOE shuts down, preventing any additional auditable events. If the SAL trail is full and the TOE is restarted, the TOE generates additional exceptions indicating that the TOE cannot allocate more temporary space and the TOE does not operate. To resume TOE operations, the space allocated to the database used by the SAL must be increased to allow the administrator to login to the GUI and delete audit records.

7.2.1 SFR Mapping

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates SAL messages for many security related events, including startup and shutdown of audit functions, for TOE management events and for user identification and authentication attempts.
- FAU_SAR.1: The TOE provides users with the Administrator role and users with both the Load Log Manager and Delete Log Message permissions the ability to read from the SAL trail using administrator console interfaces.
- FAU_SAR.2: The TOE protects the SAL messages by restricting read access to only those users that have been granted read access to the audit records.
- FAU_SAR.3: The TOE provides administrators the ability to sort SAL messages using administrator console interfaces based on date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.
- FAU_SEL.1: The TOE provides the ability to select which type of events will generate a SAL message (pre-selection).
- FAU_STG.2: The TOE protects the stored SAL messages from unauthorized deletion and prevents modifications to the messages at the TOE's own interfaces. In addition, the TOE ensures that all stored SAL messages will be saved when storage exhaustion occurs. The TOE depends upon the DB to protect the data stored in it from unauthorized access via the DB interfaces.
- FAU_STG.4: If the SAL trail becomes full, the TOE will send an alarm and the system will shut down.

7.3 User data protection

The TOE implements a discretionary access control (DAC) policy for object access based on:

- user identities,
- user group memberships,
- user roles, and
- Access Controls (ACs).

A user role is a collection of user permissions that may be assigned to a user account or access control. A user permission is a system-wide permission enables a user to view, add, change, or delete data in Tripwire Enterprise. (See Section 7.5 for more information on user roles and user permissions.)

An access control grants specified user accounts and/or user groups exclusive access to a TE object via the user role assigned to that access control.

The TOE objects directly subject to this policy are nodes and node groups, rules and rule groups, actions and action groups, tasks and task groups, TE policies, policy tests, and policy test groups. There are no other objects. A node is represented by the network address of a server, router, switch, firewall, or load balancer that contains objects that Tripwire Enterprise may monitor. A node group is an object containing a collection of nodes. Access controls on individual TE objects always overrides access controls on TE object groups.

While user identities can be used in ACs to assigned specific access permissions to specific users, the TOE also supports user groups. A user group is a collection of user accounts. Note that both users and groups can be members of groups and each user or group can be a member of multiple groups. A user with the Administrator or user administrator role may grant group membership to a user.

User groups provide a convenient way to grant and revoke permissions to more than one user in a single statement. If a user is a member of a user group that does not have access to an object, but the user has been explicitly granted access to the object, the user will be able to access the object. Permissions granted to specific users override permissions granted to user groups.

Users acquire permission based upon the role assigned to their user account. An access control is comprised of a user role and list of user accounts and groups. The user role defines the level of access granted to each user account and user group associated with that access control entry.

The following process is used to determine permissions.

1. If a user is identified in an access control for a specific TE object, the user role associated with that access control becomes the user's permission to that node, otherwise.
2. If a user group is identified in an access control for a specific TE object, the user role associated with that access control becomes the user's permission to that node, otherwise.
3. If a user is identified in an access control for a specific TE object group, the user role associated with that access control becomes the user's permission to that node, otherwise.
4. If a user group is identified in an access control for a specific TE object group, the user role associated with that access control becomes the user's permission to that node, otherwise.
5. Repeat the previous 2 steps for each containing TE object group.
6. If no permissions are found apply permissions based upon the user's role.

Note: If a user accesses a node contained within multiple, nested node groups with access controls, the applicable access control is determined by proximity to the node. In other words, the access control of the lowest node group in the node hierarchy determines if the user has permission to the node and, if so, what permission is granted the user.

The default administrator account has a privilege associated with it that allows discretionary access override, meaning that it can access any object even if the default administration account does not otherwise have access to the object. This makes some configuration errors correctable which would not be correctable otherwise. The default administrator account is the one created when the TOE is installed.

7.3.1 SFR Mapping

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2: All server subjects are subject to the DAC policy for all available operations on nodes and node groups (and their contents).
- FDP_ACF.1: Server objects have ACs and can define groups and these attributes are compared against user identities in order to determine whether the request operation should be allowed. Alternately, a user may have a role that explicitly grants the requested access regardless of the normal access check. If both of these checks fail, access will be refused.

7.4 Identification and authentication

The TOE allows the following limited non security-relevant mediated functions to be performed before the user is identified and authenticated:

- SOAP locale management (getLocales SOAP action reference) – manage the list of locales (time zone formats)
- twtool URL generation (twtool licurl) – generates a URL for the TE Launch in Context feature that can be copied and pasted into a browser; this utility does not connect to the TE server
- twtool common option settings (twtool set) – define and save a default argument for a common option (client preferences)
- twtool version display (twtool version) – displays the current version of the CLI (twtool)
- twtool help – displays help information of the CLI (twtool)

The TOE provides two different login methods:

Password Method	The TOE itself identifies and authenticates the username and password supplied. Always used for identifying and authenticating the built-in “administrator” account.
LDAP/Active Directory Method	The TOE is configured to request authentication services from a LDAP or Active Directory server for all user accounts, except the built-in “administrator” account.

TE always authenticates Administrator accounts with the Password login method, regardless of the selected login method.

The TOE maintains a username and password for every user account. If the LDAP/Active Directory Method is selected, the TE usernames must match the LDAP/AD usernames. The password maintained by the TOE is only used if the Password login method is used to authenticate the user account. User accounts can be established as either regular user accounts or administrator accounts via the assignment of roles, as described in the Security Management function (below). User login names and hashed passwords are stored as part of the TOE’s configuration data.

During login, the TOE checks its user account database for the username provided. If the username is not in the user account database, the login attempt fails. If the username is a valid TE username, the TOE determines which login method applies to the user account.

For the Password Method, the TOE provides its own identification and authentication mechanism. In order to access the Tripwire Enterprise Server, a login account, including a login name and password, must be created for the user. The TOE hashes the password and compares the resulting

value to that stored in the TOE configuration data. If either the login name or password is incorrect the login request will fail and no additional functions will be made available.

When configured to use the LDAP/Active Directory (AD) Method, the TOE sends the username and password entered by the user to the LDAP or AD server unless the built-in "administrator" account username is provided. The LDAP or AD server verifies the identity and authentication of the user and sends a response back to TE indicating if the user had been authenticated. The TOE supports LDAP version 2 and 3. If not, the login request will fail and no additional functions will be made available to the user.

As a result of a successful login, a subject is created on behalf of the client. The TOE assigns the subject the roles and groups associated with the TE user account.

To login to the TOE using the graphical user interface (GUI), the user provides the login name and password at the prompt. To access the TOE using the command line interface (CLI), the user provides the login name and password as arguments to every CLI command that accesses a TOE object. The TOE's CLI interface provides a shortcut, however, letting the user set the login name and password, after which the CLI will automatically add these values as userid and password arguments to every command. Guidance recommends that users provide their userid and password manually with each command they enter.

In addition to user name and password, any user groups, roles and user permissions assigned to the user are also stored as a part of the TOE configuration data. User permissions enable a user to view, create, or modify data in TE. A role is a collection of user permissions that may be assigned to a user account or access control. A user group is a collection of user accounts. Note that groups are used to simplify access control management.

By default, TE user passwords must meet the following password complexity rules. [23] TE prevents the user from reusing their previous 100 passwords. In addition, guidance directs the administrator that in the evaluated configuration, the password complexity feature and following rules must be enabled:

- the minimum password length must be at least nineteen (8) characters
- the minimum number of numeric characters must be at least one (1)
- the minimum number of uppercase characters must be at least one (1)
- the minimum number of non-alpha numeric characters must be at least one (1)

If enabled, TE will lock out local user accounts after an administrator-configured number of consecutive failed login attempts. The number of minutes that a TE user account is locked out after exceeding the threshold is configured by the administrator. If selected, TE will also send an e-mail notification to the user when their account is locked out.

In addition to implementing a log out capability which allows users to terminate their current session, the TOE implements the ability to terminate a user session when the user logs into the TOE from another entity. In other words, while still logged in from Computer A if the user then

[23] Note that guidance provides additional recommendations on a stronger password, but the TOE does not enforce any other password complexity features.

logs in from Computer B; the user's session initiated from Computer A is terminated.

7.4.1 SFR Mapping

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: The TOE disables (locks out) user accounts after a specified number of consecutive failed login attempts.
- FIA_ATD.1: The TOE defines user identities, authentication data (passwords), user groups, user permissions, and role information.
- FIA_SOS.1: The TOE enforces restrictions on the complexity of a password, including password length and password reuse.
- FIA_UAU.1: The TOE offers selected non-security relevant functions until the user is authenticated. The TOE can be configured to perform user authentication or request user authentication be performed by an LDAP/Active Directory server.
- FIA_UID.1: The TOE offers selected non-security relevant functions until the user is identified. The TOE can be configured to perform user identification or request user authentication be performed by an LDAP/Active Directory server.
- FTA_SSL.4: The TOE implements the ability for users to terminate their own sessions.

7.5 Security management

The TOE provides four interfaces to control how it operates: a graphical user interface (GUI), provided by a built-in web server, a command-line interface (CLI or twtool), the SOAP interface, and the tetool command. The GUI is a full-functioned interface from which a user with appropriate permissions can completely administer the TOE. The CLI provides a subset of the GUI functionality that is insufficient to completely administer the TOE. For the most part, the CLI is a front-end for the TE SOAP interface. There are a few CLI commands that are not also expressed as TE SOAP interfaces. The CLI, for example, provides no functionality to add or delete users or to change user passwords (these functions are available only through the GUI). When each interface provides access to the same administrative functions, they have the same restrictions. The CLI is provided to support the execution of remote scripts. In the CC evaluated configuration, only the built-in TE administrator account, which has all TE permissions, can use the TE SOAP interface and twtool commands that require identification and authentication. The tetool command is a command-line front-end utility that provides functionality for the installer, troubleshooting, and customer support. Except for the fips subcommand, which is only to be executed during initial setup, the tetool subcommands are either disabled or considered non-SFR interfering.

During initial configuration, the default administrator password is required to be changed and then FastTrack is automatically executed. FastTrack configures the first TE Administrator user and allows the installer to configure the initial TE monitoring infrastructure, including setting up rules and policies. FastTrack cannot be executed after the initial configuration.

A user permission is a system-wide permission that enables a user to view, add, change, or delete data in Tripwire Enterprise. The common types of user permissions are:

- Create permissions – authorize users to create a class of Tripwire Enterprise objects and groups or a component of the Settings Manager. For example, the create nodes permission authorizes users to create nodes and node groups.
- Create ACL permissions – authorize users to create access controls for objects in a specific Manager.
- Delete permissions – authorize users to permanently remove objects or groups from the system or a component of the Settings Manager. For instance, with the delete nodes permission, one can delete both nodes and node groups.
- Edit permissions – enable users to modify data in a specific component of the Settings Manager
- Link permissions – authorize users to create links between objects in a specific Manager or a component of the Settings Manager.
- Load permissions – provide read-only access to a class of Tripwire Enterprise objects and groups. For instance, the load rules permission grants access to the Rule Manager. In the Rule Manager, users can review all rules and rule groups.
- Manage permissions – authorize users to work with system reports, system searches, or a component of the Settings Manager.
- Update permissions – enable users to modify the properties of a class of Tripwire Enterprise objects and groups or a component of the Settings Manager. For example, one can change the properties of nodes and node groups with the update nodes permission.
- Use permissions – authorize users to use a rule or rule group in a baseline or version check operation.
- View permissions – authorize users to view the properties of nodes, node groups, and associated access controls in the Node Manager.

The *Tripwire Enterprise User Guide* contains a complete list of user permissions available in TE.

A user role is a collection of user permissions that may be assigned to a user account or access control. Tripwire Enterprise provides nine (9) default user roles:

Role	**Capability**
Administrator	Full control of all TE objects and features in all TE Managers
Monitor User	Read-only access in all TE Managers and the ability to modify their own user reports
Policy Manager	Full control of all TE objects and features in the Policy Manager
Policy User	Run and link TE objects in the Policy Manager and create and modify waivers

Role	Capability
Power User	Full control of TE objects and features in the Node Manager, Rule Manager, Account Manager, Task Manager, Policy Manager, and some components of the Settings Manager
Regular User	Read access to all TE Managers and the ability to run policy tests, run version checks, and change the properties of nodes
Rule Manager	Full control of all TE objects and features in Rule Manager
Rule User	Use rules in baseline operations and version checks
User Administrator	Create, edit, delete user accounts, user roles, and user groups

Four of the default user roles (Administrator, Power User, Regular User, and Monitor User) are organized hierarchically. In other words, each role possesses the permissions granted to lesser roles, as well as an additional set of permissions. The Administrator role has the most permissions, followed by the Power User role, the Regular User role and the Monitor User role has the least permissions. The User Administrator role is orthogonal to the other roles and has permissions to manipulate user accounts. The Policy Manager, Policy User, Rule Manager, and Rule Use default roles are used in access controls applied to pre-configured TE objects. To preserve the intended purpose of these roles, administrators are instructed in guidance to avoid assigning them to user accounts. Additional user roles can be created by the User Administrator.

Data collection and reaction can be performed by the any of the default user roles, except for Monitor User and User Administrator. Data Analysis can be performed by any of the default user roles, except for User Administrator.

When the TOE is installed, the nodes to be monitored must be added to the TOE configuration. After nodes are added, rules are created to specify which elements on each node are to be monitored. Actions can then be created to cause the TOE to take remedial measures in response to changes detected by integrity checks. After actions are added, rules are defined that specify how the TOE will check selected elements for changes. Integrity checks of selected nodes can then be scheduled by creating one or more Rule Tasks.

Rule Tasks are used to schedule integrity checks of nodes and/or node groups. An integrity check starts by taking a snapshot of (collecting a set of object attributes from) a node. The snapshot is then compared to a previous snapshot that has been saved as a baseline, using snapshot check rules established by the administrator.

Administrators can create baselines when a rule task is created (initialize baselines) or after the previous steps have been completed. Administrators can also promote a collected set of object attributes (snapshot) to baseline status at any time. Both of these actions require the Administrator role.

Objects do not have an ACL assigned to them when they are created. This allows the objects to be accessed by any subject. Access can be granted subsequently to specific users. The first such

access specified creates an ACL for the object.

When the TOE reporting mechanism is configured, the Administrator role can define reports with varying levels of detail about the results of integrity checks as follows:

- Change Process Compliance - This report identifies authorized and unauthorized changes to specified nodes over a period of time. An authorized change is associated with a valid change request ticket ID.
- Change Rate - This report shows the total number of changes (additions, removals, and modifications) detected on specified nodes over a period of time. Within the selected time period, the report displays the number of detected changes at a regular interval (or 'frequency'); for instance, daily, weekly, or monthly.
- Change Variance - This report shows the total number of rules and elements associated with detected changes on specified nodes. As appropriate, you can limit report output to specific nodes, rules, and/or element names. Typically, this report is executed immediately after deployment of a patch or other software package. To determine which new element versions should be promoted, you may review the report for inconsistencies across the updated systems.
- Changed Elements - This report lists all changed elements identified by the specified criteria. Report output specifies exactly which attributes changed for each element.
- Changes by Node or Group - This report displays the number of changes detected on one or more nodes (or node groups). The change comparison calculates the total number of changes for each node, as well as the totals for each type of change (added, removed, or modified).
- Changes by Severity - This report shows the total number of changes detected on one or more nodes (or node groups) that fall within a specified range of severity levels.
- Detailed Changes - This report compiles comprehensive change information for elements on specified nodes.
- Device Inventory - This report identifies the make, model, and version of specified nodes.
- Frequently Changed Nodes - This report ranks the most frequently changed nodes that meet the specified criteria. The report includes the total number of changes for each node, as well as the totals for each type of change (added, removed, or modified).
- Inventory Changes - For your Tripwire Enterprise implementation, this report calculates the number of nodes that have been added, modified, and deleted over a specified period of time.
- Monitoring Policy - This report identifies the criteria set associated with one or more file system rules or Windows registry rules and, optionally, the times when those rules should apply.
- Nodes with Changes - For the specified criteria, this report identifies the number of nodes that have changed over a given period of time.

- Reference Node Variance - This report identifies all elements that differ between one node (the reference node) and another (the compare node). In a single report, the reference node may be compared with one or more compare nodes.
- System Access Control - This report provides security-related information on specified user accounts, user roles, user groups, and/or access controls.

In addition to providing an administrative interface that allows the role to review the system data, the TOE also protects the collected System data from unauthorized deletion and modification at the TOE interfaces.

7.5.1 SFR Mapping

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1a: The TOE restricts the ability to modify the behavior of System data collection, analysis, and reaction to authorised system administrators.
- FMT_MOF.1b: The TOE restricts the ability to enable and disable integrity check rules and reporting options, to authorised system administrators.
- FMT_MOF.1c: The TOE restricts the ability to enable and disable integrity check actions to authorised system administrators.
- FMT_MSA.1: The ability to manage object attributes is restricted by enforcing the permissions of the Administrator role.
- FMT_MSA.3: By default, every object is created without an ACL, which gives access to all users. Subsequently, ACLs can be explicitly added to limit access to specific users. The TOE does not provide the ability to specify alternative initial values when an object is created.
- FMT_MTD.1: The TOE restricts the ability to manage TSF data as specified in Section 6.2.5.6.
- FMT_SMR.1: The TOE provides system-defined user roles to be assigned to user accounts. The default user roles provided by the TOE are User Administrator, Administrator, Monitor User, Policy Manager, Policy User, Power User, Regular User, Rule Manager, and Rule User. (Users assigned any role or permission, except User Administrator and Monitor User, are considered authorised system administrators.) Users assigned a permission are also considered to have a role.
- FMT_SMF.1: The TOE provides security management functions for use by the administrators.

7.6 Protection of the TSF

The TOE is an application that runs on a host operating system. The TOE is instantiated as services on Windows platforms and as daemons on UNIX-based platforms. The remainder of this discussion will refer to “process” as a non-platform specific term for “service” and “daemon”. The Tripwire Enterprise Server runs on a JVM in a host operating system provided process. The host operating system is expected to provide process isolation to each process with

its own unique address space and separation from all other processes. The TOE relies upon the underlying hardware and host operating system in the operational environment to provide reliable time stamps.

Tripwire Enterprise Server is a JAVA program that runs in a customer-supplied JVM. The Tripwire Enterprise Server manages its users and access controls internally. The TOE itself distinguishes actions of TOE users within the TOE by associating users with threads running within the JVM. The TOE does not provide a general programming interface to TOE users. The user community of the TOE has no relationship to the users of the underlying operating system.

The startup and shutdown of the JVM is controlled by the TOE and only TOE software is executed within the JVM. The TOE JAR files are signed and unsigned code cannot be loaded in the JVM started by the TOE. The TE server requires a JRE bundle with strong encryption; if a JRE bundle that does not have strong encryption is used, the TE server will fail to start.

In the evaluated configuration (i.e., FIPS mode is enabled), during installation of the Tripwire Enterprise Server an X.509 signing certificate[24] is generated, which is used to sign another X.509 certificate that is host specific. These certificates are created using ECDSA and 2048-bit RSA. The public key of the signing certificate, the public key of the host-specific certificate, and the private key of the host-specific certificate are then stored in BCCM Key Store format and made available to the JVM. When the Tripwire Enterprise Server or Tripwire Enterprise Java Agent start, they ensure the JVM is using these certificates, and configure the JVM to require mutual authentication on TLS connections.

The Tripwire Enterprise Server uses various network protocols to communicate with other parts of the TOE and with the operational environment. Depending upon the communication pathway the Tripwire Enterprise Server acts either as a server or as a client on each pathway. The Tripwire Enterprise Server and Tripwire Enterprise Java Agents use the TLS implementation provided by the BCCM to communicate with TOE components. In the evaluated configuration, the BCCM must be in the FIPS Approved mode of operation. The TE Axon Agent uses a FIPS approved OpenSSL FIPS Object Module SE v2.0.16 library (FIPS certificate number 2398) to implement TLS. The following summarize the network communication pathways that exist.

- TE Server – TE Java Agent communication.

  The TE Server and TE Java Agents are peers, with either able to initiate communication to accomplish the task being performed. Both the TE Server and TE Java Agent use the TLS to communicate with each other. A mutually authenticated TLS connection is established that allows these components of the TOE to communicate.

- TE Server – TE Axon Agent communication.

  The TE Server and TE Axon Agents are peers, with either able to initiate communication to accomplish the task being performed. Both the TE Server and TE Axon Agent use the TLS to communicate with each other. After the TE Axon Agent registers with the TE Server, it requires mutual authentication using certificates on TLS connections between the TE Axon Agent and TE Server. Authentication is

[24] A signing certificate is a certificate that will be used to sign another certificate.

accomplished using X509 certificates.

- TE Server – TE Database & LDAP/AD server.

  The TE Server is the only component of the TOE that communicates with the database. The TE Server is also the only component of the TOE that communicates with the LDAP/AD server. The TSF negotiates a mutually authenticated TLS connection between the database and the Tripwire Enterprise Server and between the LDAP/AD server and the TE Server. Authentication is accomplished using X509 certificates for both the Tripwire Enterprise Agent and the Tripwire Enterprise Server. The TE Server uses the JDBC protocol over TLS provided by the JVM in the operational environment to connect to the database.

- TE Server – TE nodes

  The TE Server initiates connections to TE nodes that do not have the TE Agent installed to obtain information made available by protocols supported by the node (e.g., FTP, Telnet, SSH). For protocols requiring user authentication, the Tripwire Enterprise Server provides login data for the specific node being accessed, then gathers information from the node as determined by rules established for that network device (e.g., a specific Cisco IOS or Oracle 18c device).

- TE Server – CLI & GUI

  The TE Server implements web server functionality that supports HTTP over the TLS (HTTPS) provided by the JVM in the operational environment. The communication between the TE Server and the Tripwire CLI uses the HTTPS protocol. Similarly, communication between the TE Server and the GUI is also over the HTTPS protocol. The TE Server separates user network connections based on individual administrative GUI and CLI connections.

- TE Server – SMTP/SNMP/Syslog server

  The TE Server is a client to SMTP/SNMP/Syslog servers. The TE Server uses these servers as configurable delivery mechanisms for TOE generated messages.

- TE Server and TE Java Agent – remote IT entities

  The TE server and TE Java Agents use the JVM TLS v1.2 implementations in the operational environment to protect communications between the TOE and the remote IT entities (e.g., the database, user's browser, and user's shell). The JVM is configured to use TLS for these communications.

- TE Agent – TE Console

  For TE Agent to TE console TLS communications, TE Server and TE Java Agent uses the BCCM implementation, which uses AES 128/256-bit strength encryption. TE Axon Agent uses its OpenSSL module to implement TLS. For the connections it also requires both sides to be authenticated via the certificates discussed previously, preventing any man-in-the-middle attacks.

The only communications accepted by Tripwire Enterprise Agents are over an authenticated TLS

connection established with the Tripwire Enterprise Server.

The BCCM used by TE Server and TE Java Agent implements the following validated algorithms:

Algorithms / Key Sizes	**Uses**
AES 128/192/256-bit (CBC and GCM modes)	TLS
RSA (2048, 3072-bit keys) following FIPS PUB 186-4, Appendix B.3	TLS/key generation and signature services
ECC (P-256, P-384, P-521) following FIPS PUB 186-4, Appendix B.4	TLS
HMAC with SHA-1, SHA-256 (32-byte key size)	TLS
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	TLS

The TE Axon Agent OpenSSL implements the following validated algorithms:

Algorithms / Key Sizes	**Uses**
AES 128/256-bit (GCM mode)	TLS
RSA (2048-bit keys) following FIPS PUB 186-4, Appendix B.3	TLS/key generation and signature services
SHA-256, SHA-384	TLS

7.6.1 SFR Mapping

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The cryptographic modules protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE. The TE Server and TE Java Agent request the JVM provide a secure channel using TLS. The TE Axon Agent OpenSSL implementation provides the secure channel using TLS.
- FPT_STM_EXT.1: The TOE relies upon the underlying hardware and host operating system in the operational environment to provide reliable time stamps. The TOE obtains and uses this reliable time appropriately.
- FCS_COP.1a: TE includes a FIPS certified cryptographic module that provides the SHA hashing capability used to implement TLS.
- FCS_COP.1b-d: The FIPS certified cryptographic modules perform the cryptographic operations as listed in the SFR. These operations are used to implement TLS.

- FCS_CKM.1: The FIPS certified cryptographic modules performs key generation necessary to implement TLS.
- FCS_CKM.4: The FIPS certified cryptographic modules destroys the cryptographic keys as specified in FIPS 140-2.