Security Target

AccessData Cyber Intelligence and Response Technology v2.1.2

Document Version 0.9.5

September 26, 2012

Prepared For:

AccessData Group, LLC

384 South 400 West

Lindon, UT 84042

www.accessdata.com

Prepared By:

Apex Assurance Group, LLC

555 Bryant Street, Ste. 804

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the AccessData Cyber Intelligence and Response Technology v2.1. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: AccessData Cyber Intelligence and Response Technology v2.1
ST Revision	0.9 .3
ST Publication Date	September 26, 2012
Author	AccessData and Apex Assurance Group

1.2 TOE Reference

TOE Reference	Cyber Intelligence and Response Technology v2.1.2 build 10, also denoted as 2.1.2.10.
TOE Type	Data Protection

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE

SECTION	TITLE	DESCRIPTION
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
Administrator	An entity that has complete trust with respect to all policies implemented by the TSF.
API	Application Programming Interface
Authorized User	Users of the system that may, in accordance with the SFRs, be permitted to perform one or more operations for which they have granted permissions.

CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
External Entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
GHz	Gigahertz
GUI	Graphical User Interface
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
IIS	Microsoft Internet Information Services
Installation	The procedures that an entity has to perform normally only once after receipt and acceptance of the TOE to progress it to the secure configuration as described in the ST including the embedding of the TOE in its operational environment. If similar processes have to be performed by the developer they are denoted as "generation" throughout ALC: Life-cycle support. If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation here.
IP	Internet Protocol
IT	Information Technology
MB	Mega Byte
NTP	Network Time Protocol
Operator	A user type assumed by an authorized user (human) conducting data collection or analysis activities.
OS	Operating System
OSP	Organizational Security Policy
PC	Personal Computer
RAM	Random Access Memory
RPC	Remote Procedure Call
SFP	Security Function Policy
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSFI	TSF Interface

Table 2 – Acronyms and Terms Used in Security Target

1.6 TOE Overview and Description

The TOE is the Cyber Intelligence and Response Technology v2.1.2 (also referenced as "TOE" or "CIRT"). The primary purpose of the TOE is to provide a means for the identification and management of inappropriate data hosted on corporate end user workstations, file shares, and email message servers. Users ranging in experience from business executives to IT staff members can search end user

workstations for inappropriate files then view results via a graphical, drill down interface. Workstations containing inappropriate data can be targeted for remediation action including acquisition, replacement, and deletion of files, or the termination of executing processes.

Searches and remediation tasks may be conducted manually or scheduled for repeated, unattended, execution. The Agent (in the IT Environment) periodically executes a Query and if inappropriate data is identified, a Remediation task may be executed and/or send a Notification. The Agent, operating on end user workstations, runs regardless of network connectivity or location. Any acquisition or remediation tasks executed in the absence of network connectivity are cached locally on the workstation for later transmission to the TOE's central management facility, or Proxy Server, when network connectivity is re-established.

1.6.1.1 User Authentication

All users of the system must use a user account in order to access the console. Users are given a unique username and a password. The username is a string at least 7 characters in length and not exceeding 32 characters in length. Usernames may include alpha or numeric characters. In addition, all users are required to have a password of at least 7 characters in length and no more than 20 characters. Passwords may include alphanumeric and special characters but must include at least one alpha character and one special character.

Only administrators, and users with the Manage Users permission, can manage (create, modify, delete) user accounts and associate access permissions. User credentials (username, password, and friendly name) are stored in a database operating entirely within the private network. Usernames may not be modified once created.

All users are required to present proper credentials before accessing the console. Two text entry fields are presented to the user when attempting to access the system: username and password. Usernames are reflected in readable text on the screen while the user is typing. Passwords are presented as a dot for each character entered to mask the characters. The login screen is the only location where the username and password are displayed together. Once authenticated, a friendly name (separate from the username and defined when the user record is created) appears on any pages that display the name of the user.

Users are allowed to make five incorrect authentication attempts before being locked out of the system. The account can be unlocked by an administrator or will be automatically unlocked after 20 minutes. which requires an authenticated Administrator to reset their password.

1.6.1.2 Permissions Management

Users of the system are considered as either the role of administrator or a non-administrator or operator. Administrators have all rights to the system. Administrators are responsible for managing user accounts

including authentication credentials and access permissions. Operators are responsible for operating the system to the level their permissions permit.

Administrators can complete operator functions but operators generally do not execute Administrator duties. The one exception is that an operator can be given the Manage Users permission which allows them to create and manage other users. These operators with Manage Users permissions may grant up to the same permissions that they have, but no more.

Once a user has been created they may be assigned access permissions. Permissions are divided into the following two classes:

- Administrator permissions involving the management of user security information
- Custom permissions that limit the operator's access to CIRT operational functionality.

Any user that has been granted Administrative permissions is deemed to be an Administrator, all others are considered operators.

1.6.1.3 Security Audit Logging

The TOE includes a Security Audit Log facility used to house any security related event executed by any user of the TOE. Each entry includes: username, date and time the operation was executed and a description of the event. Because TOE users may be working in multiple time zones, the date/time recorded with each entry utilizes the system time of the server hardware upon which the TOE software is running.

1.6.2 Physical Boundary

The TOE is a software TOE and includes:

1. An instance of the AccessData Cyber Intelligence and Response Solution (CIRT) application executing on a system dedicated for this purpose including:
    a. CIRT Web Server (UI Server).
    b. CIRT Client Software (Business Logic).
    c. Infrastructure Services (Authentication and Security Audit Log facility).
2. Product Operating Manual: Cyber Intelligence and Response Technology User Guide.
3. The TOE includes only the software (1) excluding the operating system upon which they execute.

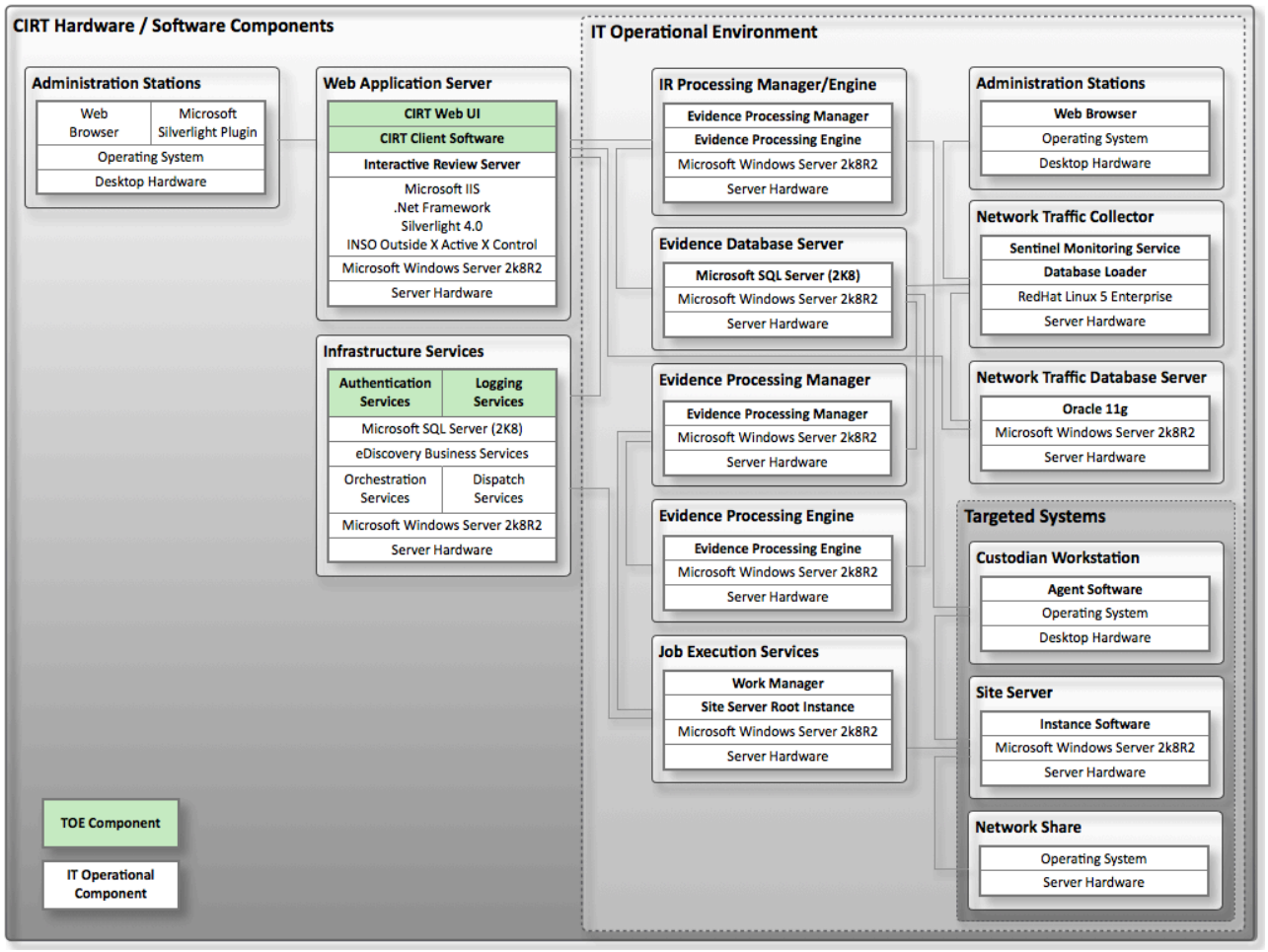

Figure 1 – TOE Boundary

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
Software	CIRT v2.1.2
Hardware for TOE (IT Environment)	A general purpose computing platform running an operating system currently supported by the developer that supports the following web browsers: Internet Explorer 7 or 8.
Hardware for Management Platform (IT Environment) (Minimum requirements are listed. Recommended requirements depend on the operating environment.)	Processor: 2.4 GHz (x64 processor) Memory: 4 GB RAM Disk: 100 GB free space Super VGA (800 × 600) or higher resolution monitor DVD Drive, Keyboard and mouse

TOE COMPONENT	VERSION/MODEL NUMBER
Web Application Software for Management Platform (IT Environment)	Microsoft Windows Server 2008 R2 Service Pack 1 Microsoft IIS 7.5 or higher Microsoft .Net Framework 4.0 or higher Microsoft Silverlight 4.1 Microsoft SQL Server 2008 R2 PostgresSQL 9.0.1 or higher INSO Outside X Active X Control 1.0

Table 3 – Evaluated Configuration for the TOE

The management interface to the TOE utilizes a web-based administrative interface (Figure 1) that uses an HTTPS communication channel.

1.6.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Security Audit	The TOE generates audit records for security events. The Administrator has access to the audit trail and the ability to view the audit trail.
User Data Protection	The TOE allows only authorized access to TOE data via the Administration console.
Identification and Authentication	The TOE requires valid authentication credentials (username and password) before allowing access to any part of the TOE or TOE data.
Security Management	The TOE provides a wide range of security management functions. Administrators can configure the TOE, manage users, configure the access control policy, and audit.
TOE Access	The TOE monitors user activity and makes the console illegible when an inactivity threshold is reached.

Table 4 – Logical Boundary Descriptions

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant and augmented with ALC_FLR.2.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL3 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

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

3.1 Threats

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

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.PRIVILEGE	Compromise of TOE components may occur as a result of actions taken by careless, willfully negligent or hostile administrators or other privileged Operator.
T.PWD_SHARE	If user passwords are shared, contrary to the organizational policy, an unauthorized agent could access confidential assets.
T.KEY_LOSS	A non-hostile user may inadvertently forget the Administrator password denying administrative access to authentication and authorization resources.

Table 5 – Threats Addressed by the TOE

The IT Environment does not explicitly address any threats.

3.2 Organizational Security Policies

The TOE is required to meet the following organizational security policies:

POLICIES	DESCRIPTION
P.AUTHORIZED_USERS	Only those users who have been authorized to access the information or resources within the TOE may access the TOE.

POLICIES	DESCRIPTION
P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their actions, regarding the management of security parameters, within the TOE.

Table 6 – OSPs Addressed by the TOE

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.DEPLOYMENT	The installation procedures must be carried out by trained (AccessData) staff to install and configure the product prior to handover (delivery) to the customer. Installation may be performed either on customer site, or off-site at a central installation and distribution site. These procedures are semi-automated and will: • Ensure a private network for the TOE servers has been established • Distribute public certificates thought the system • Establish one or more Administrator accounts
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL	The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
A.COOP	Authenticated users possess the necessary authorization rights to access at least some of the information or resources managed by the TOE and are expected to act in a cooperating manner.
A.NETWORK	All network communication between components of the TOE that operate within a private network with those outside the private network is conducted over secure network communication sessions.

Table 7 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.AUTHORIZATION	The TSF must ensure that only authorized users gain access to the TOE.
O.AUDITING	The TSF must record the security relevant actions of users of the TOE.
O.MANAGE	The TSF must provide the facilities necessary to limit the management of user security data to Administrators.
O.ENFORCEMENT	The TSF must ensure that the security functions are enforced throughout the TOE.

Table 8 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMIN_GUIDANCE	Appropriate guidance documentation must be provided to enable administrators to manage and operate the TOE in a manner that maintains IT security objectives.
OE.USER_GUIDANCE	Appropriate guidance documentation must be provided to enable Operators to manage and operate the TOE in a manner in accordance with the security objectives.
OE.NOEVILADMIN	Administrators of the TOE and IT Environment must not be careless, willfully negligent or hostile, and must follow the instructions provided in the administrator guidance documentation.
OE.NETWORK	The Administrator will install and configure a network that supports secure communication between the distributed TOE components operating outside the private network. The administrator will ensure that this network functions properly.
OE.INSTALL	The Administrator of the TOE must ensure that the TOE is installed according to the administrator guidance.
OE.CREDEN	The Administrator of the TOE must ensure that all access credentials are protected by the users in a manner that maintains security objectives and those credentials are assigned appropriately.
OE.TIME_STAMP	The Operational Environment will provide reliable time stamps for accountability purposes.

Table 9 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.PRIVILEGE	T.PWD_SHARE	T.KEY_LOSS	P.AUTHORIZED_USERS	P.ACCOUNTABILITY	A.DEPLOYMENT	A.MANAGE	A.NO_EVIL	A.COOP	A.NETWORK
O.AUTHORIZATION	✓		✓	✓						
O.AUDITING	✓									
O.MANAGE	✓		✓							
O.ENFORCEMENT		✓								
OE.ADMIN_GUIDANCE		✓				✓	✓	✓		
OE.USER_GUIDANCE									✓	
OE.NOEVILADMIN								✓		
OE.NETWORK										✓
OE.INSTALL						✓	✓			
OE.CREDEN							✓		✓	
OE.TIME_STAMP					✓					

Table 10 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1.1 Rationale for Security Objectives of the TOE

OBJECTIVE	RATIONALE
T.PRIVILEGE	O.AUTHORIZATION helps to mitigate this threat by requiring a user to present verifiable credentials before being granted access to restricted areas of the TOE. O.AUDITING help mitigate this threat by recording every security related event in the Audit log, and O.MANAGE limits access to the Audit log to Administrators.
T.PWD_SHARE	OE.ADMIN_GUIDANCE helps to mitigate this problem through Administrator instruction on the proper management of user security data and if the user data is compromised, O.ENFORCEMENT helps to mitigate the threat by providing the ability to restrict access to the TOE.
T.KEY_LOSS	O.AUTHORIZATION helps to mitigate this threat by requiring a user to present verifiable credentials before being granted access to restricted areas of the TOE. O.MANAGE allows an Administrator to manage (modify, delete) user security data.

OBJECTIVE	RATIONALE
P.ACCOUNTABILITY	OE.TIME_STAMP is used when recording the actions executed by Administrators and Operators. Each security related operation is recorded on a server with a consistent time stamp regardless of the time zone in which the user is working.
P.AUTHORIZED_USERS	O.AUTHORIZATION requires a user to present verifiable credentials before being granted access to restricted areas of the TOE.
A.DEPLOYMENT	OE.ADMIN_GUIDANCE assumes that proper documentation is provided necessary to install the TOE in accordance with the assumptions set for by OE.INSTALL.
A.MANAGE	OE.ADMIN_GUIDANCE assumes that guidance documentation must be provided to enable Administrators to install (OE.INSTALL), manage, and operate the TOE. OE.CREDEN assumes that users present proper authentication credentials in order to gain access to some of the information and resources managed by the TOE.
A.NO_EVIL	OE.NOEVILADMIN assumes that all Administrators must not be careless, willfully negligent or hostile, and follow the instructions provided in the administrator guidance documentation (OE.ADMIN_GUIDANCE).
A.COOP	OE.CREDEN assumes that users present proper authentication credentials in order to gain access to some of the information and resources managed by the TOE. It is also assumed that users are following the procedures outlined in the user guidance documentation OE.USER_GUIDENCE.
A.NETWORK	OE.NETWORK assumes that an Administrator will install and configure the TOE such that all network communication between components of the TOE that operate within a private network with those outside the private network are conducted within secure network communication sessions.

Table 11 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

There are no extended components in this Security Target.

6 Security Requirements

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

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Protected Audit Trail Storage
User Data Protection	FDP_ACC.1	Complete Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure 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
TOE Access	FTA_SSL.3	TSF-Initiate Session Termination

Table 12 – TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take [the following configurable actions: lockout a given users account, render the users console illegible] upon detection of a potential security violation.

6.1.1.2 FAU_GEN.1 – Audit Data Generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified*] level of audit; and

c) [The events in column two of Table 13 – Auditable Events]

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, [information specified in column three of Table 13 – Auditable Events].

SFR	EVENT	DETAILS
FMT_SMR.1	Modifications to the permissions given to a user.	The identity of the Administrator performing the modification and the user identity whose permissions are being modified
FIA_UID.2	All use of the user identification mechanism.	None
FIA_UAU.2	Any use of the user authentication mechanism.	None
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	The identity of the Administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the Administrator performing the operation

Table 13 – Auditable Events

6.1.1.3 FAU_SAA.1 Potential Violation Analysis

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

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

a) Accumulation or combination of [failed authentication attempt events] known to indicate a potential security violation;

b) [no other rules].

6.1.1.4 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [an Administrator] 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.

6.1.1.5 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.

6.1.1.6 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply [searches, sorting, ordering] of audit data based on any of [the following: all audit record fields specified by value].

6.1.1.7 FAU_STG.1 – Protected Audit Trail Storage

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

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

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Access Control Security Policy] on [

Subjects: All users

Objects: security management pages

Operations: credentials and permissions management]

6.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Access Control Security Policy] to objects based on the following: [user identity and authorization rights]

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

1. Administrators may view and export the Audit log entries.

2. Administrators may view, create, modify, or delete User data.

3. Operators may grant to others permissions they have been granted].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [authorization permissions].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [account name, password string, and a list authorization rights].

6.1.3.2 FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [at least 7 characters in length and no more than 20 characters in length composed of at least 1 alphanumeric and at least 1 non-alphanumeric character].

6.1.3.3 FIA_UAU.2 – User Authentication before Any Action

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

6.1.3.4 FIA_UID.2 – User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1 – Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*modify the behavior of, enable, disable*] the functions [Access Control Security Policy] to [an Administrator].

6.1.4.2 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Access Control Security Policy] to restrict the ability to [*query, modify, delete*] the security attributes [authentication credentials, administration permissions] to [the Administrator].

6.1.4.3 FMT_MSA.2 – Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [authentication credentials].

6.1.4.4 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Access Control Security Policy] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*query, modify, delete*] the [authentication credentials, administration permissions] to [the Administrator].

6.1.4.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [Management of User authorization credentials and verify User security credentials].

6.1.4.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles~~s~~ [Administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with the roles~~s~~ [Administrator].

6.1.5 TOE Access (FTA)

6.1.5.1 FTA_SSL.3 – TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after [20 minutes] of user inactivity after identification of that user.

6.2 Security Functional Requirements for the IT Environment

There are no Security Functional Requirements for the IT Environment.

6.3 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.4.4 – Security Assurance Requirements.

6.4 Security Requirements Rationale

6.4.1 Dependencies

The following table identifies the dependencies of the requirements in this ST, including the requirements explicitly defined in this ST. As indicated in the table, all of the dependencies are satisfied.

ST Requirement	CC Dependencies	ST Dependencies
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1
FAU_GEN.1	FPT_STM.1	FAU_GEN.1 (satisfied by IT environment)
FAU_SAA.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1

ST Requirement	CC Dependencies	ST Dependencies
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3
FIA_ATD.1	none	none
FIA_SOS.1	None	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.1
FMT_MSA.2	FMT_MSA.1 and FMT_SMR.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_MSA.1 and FMT_SMR.1 FDP_ACC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	none	none

Table 14 – SFR Dependencies

6.4.2 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.AUTHORIZATION	O.AUDITING	O.MANAGE	O.ENFORCEMENT
FAU_ARP.1				✓
FAU_GEN.1		✓		
FAU_SAA.1		✓		
FAU_SAR.1		✓		
FAU_SAR.2		✓		
FAU_SAR.3		✓		

SFR \ OBJECTIVE	O.AUTHORIZATION	O.AUDITING	O.MANAGE	O.ENFORCEMENT
FAU_STG.1		✓		
FDP_ACC.1	✓			✓
FDP_ACF.1	✓			✓
FIA_ATD.1	✓			
FIA_SOS.1	✓			
FIA_UAU.2	✓			
FIA_UID.2	✓			
FMT_MOF.1			✓	
FMT_MSA.1			✓	
FMT_MSA.2			✓	
FMT_MSA.3			✓	
FMT_MTD.1			✓	
FMT_SMF.1			✓	
FMT_SMR.1			✓	
FTA_SSL.3				✓

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

6.4.3 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

TOE Security Objectives	RATIONALE
O.AUTHORIZATION	This objective is met by • FDP_ACC.1, which requires all users to provide security credentials before gaining access to security related pages. • FDP_ACF.1, which limits access to security related data to authorized users • FIA_ATD.1, which specifies the list of security attributes belonging to individual users • FIA_SOS.1, which specifies minimum requirements for passwords • FIA_UAU.2, which requires operator authentication before any action • FIA_UID.2, which requires operator identification before any action

TOE Security Objectives	RATIONALE
O.AUDITING	This objective is met by • FAU_GEN.1, which specifies auditing requirements for the TOE • FAU_SAA.1, which records unsuccessful user login events • FAU_SAR.1, which ensures audit information can be read by the Administrator • FAU_SAR.2, which prohibits all users read access to the audit records, except those users that have been granted explicit read-access. • FAU_SAR.3, which allows [searches, sorting, ordering] of audit data based on any of all audit record field values • FAU_STG.1, which ensures audit records are protected from unauthorized access or deletion
O.MANAGE	This objective is met by • FMT_MOF.1, which restricts configuration of the Access Control Security Policy to an Administrator • FMT_MSA.1, which restricts the ability to modify or delete the security attributes defined in Access Control Security Policy to the Administrator • FMT_MSA.2, which ensures that only secure values are accepted for the security attributes listed with Access Control Security Policy • FMT_MSA.3, which ensures the TOE provides restrictive default values for the Access Control Security Policy • FMT_MTD.1, which restricts control of user and TOE data to an Administrator • FMT_SMF.1, which specifies management functions available in the TOE • FMT_SMR.1, which specifies roles utilized by TOE Administrators
O.ENFORCEMENT	This objective is met by • FAU_ARP.1, which specifies security alarms for the TOE • FTA_SSL.3, which provides session termination after 20 minutes of idle time • FDP_ACC.1 and FDP_ACF.1, which provides the access control functions for security management operations

Table 16 – Rationale for TOE SFRs to Objectives

6.4.4 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.2 Flaw Reporting Procedures. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional Specification with Complete Summary
	ADV_TDS.2	Architectural Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
ALC: Lifecycle Support	ALC_CMC.3	Authorization Controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	Flaw Reporting Procedures
	ALC_LCD.1	Developer defined life-cycle model
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.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 17 – Security Assurance Requirements at EAL3

6.4.5 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3 augmented with ALC_FLR.2. EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is Basic, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.4.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: AccessData Cyber Intelligence and Response Technology v2.1.2

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_FSP.3 Functional Specification with Complete Summary	Functional Specification: AccessData Cyber Intelligence and Response Technology v2.1.2
ADV_TDS.2 Architectural Design	Architectural Design: AccessData Cyber Intelligence and Response Technology v2.1.2
AGD_OPE.1 Operational User Guidance	User Guide: AccessData Cyber Intelligence and Response Technology v2.1.2
ALC_CMC.3 Authorization Controls	Life-Cycle Management: AccessData Cyber Intelligence and Response Technology v2.1.2
ALC_CMS.3 Implementation representation CM coverage	Life-Cycle Management: AccessData Cyber Intelligence and Response Technology v2.1.2
ALC_DEL.1 Delivery Procedures	Life-Cycle Management: AccessData Cyber Intelligence and Response Technology v2.1.2
ALC_DVS.1 Identification of Security Measures	Life-Cycle Management: AccessData Cyber Intelligence and Response Technology v2.1.2
ALC_LCD.1 Developer defined life-cycle model	Life-Cycle Management: AccessData Cyber Intelligence and Response Technology v2.1.2
ALC_FLR.2 Flaw Reporting Procedures	Life-Cycle Management: Access Data Cyber Intelligence and Response Technology v2.1.2
ASE_CCL.1 Conformance claims	Security Target: Access Data Cyber Intelligence and Response Technology v2.1.2
ASE_ECD.1 Extended components definition	Security Target: Cyber Intelligence and Response Technology v2.1.2
ASE_INT.1 ST introduction	Security Target: Access Data Cyber Intelligence and Response Technology v2.1.2
ASE_OBJ.2 Security objectives	Security Target: Access Data Cyber Intelligence and Response Technology v2.1.2
ASE_REQ.2 Derived security requirements	Security Target: Access Data Cyber Intelligence and Response Technology v2.1.2
ASE_SPD.1 Security problem definition	Security Target: Access Data Cyber Intelligence and Response Technology v2.1.2
ASE_TSS.1 TOE summary specification	Security Target: Access Data Cyber Intelligence and Response Technology v2.1.2
ATE_COV.2 Analysis of Coverage	ATE-Functional Test: AccessData Cyber Intelligence and Response Technology v2.1.2
ATE_DPT.1 Testing: Basic Design	ATE-Functional Test: AccessData Cyber Intelligence and Response Technology v2.1.2
ATE_FUN.1 Functional Testing	ATE-Functional Test: AccessData Cyber Intelligence and Response Technology v2.1.2

Table 18 – Security Assurance Rationale and Measures

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

7.2 Security Audit

Incorporated in the TOE is a security audit log facility maintained while the system is operational. The TOE provides a single location in which the distributed elements of the TOE register audit log entries. Each audit record contains a number of fields that describe the event.

The set of fields that appear in each audit record appears in Table 19.

NAME	DESCRIPTION
Recorded Date/Time	The date and time the event is recorded in local time of the server that hosts the audit service.
Username	The username that initiated the action propagating the audit record.
Description	A human readable text string that describes the audit record.

Table 19 – Fields for Event Records

Each time a users engages in an activity that may affect user security data or modify the contents of the Security Audit Log (other than record an event), the TOE automatically generates an entry in the Security Audit Log.

The TOE does not provide a means of suspending or resuming the Security Audit Log service. The TOE never purges Security Audit records – though a means is provided for authorized Administrators to purge records from the log. When executed, all of the records are deleted and a new entry is made that records that the log was purged, the user that purged the log, and date/time it was purged.

All security related events are entered into the Security Audit log. The TOE automatically generates the log entries. These actions include:

NAME	DESCRIPTION
System startup	The date and time the Security Audit Service becomes operational. The system time of the host servers is used as the time stamp for the initial entry and all subsequent events.
System shutdown	When the Security Audit Service log service is terminated normally, an event is entered indicating the Security Audit Service log is no longer available is made.
User authentication events	An entry is made upon each successful user authentication.
User lockout	When a user fails to provide authentication credentials within the allowable number of attempts, the failure attempt is recorded.
User creation	An event is recoded when a new user (Administrator or Operator) is executed.
User modification	An event is recorded when user security data is modified.
Assignment of permissions	An event is recorded when an Administrator or Operator assigns authorization permissions to another user.
Removal of permissions	An event is recorded when an Administrator or Operator removes authorization permissions from another user.
User deletion	An event is recorded when a user is deleted.
Accesses the Audit Log	When an Administrator accesses the Audit log, the event is recorded.
Purging the Audit log	When an Administrator purges entries from the Audit log, the event is recorded. If the Administrator purges all Audit log records, an event is entered indicating that the entire log was just purged.

Table 20 – Actions that generate Security Audit Log Entries

The TOE restricts access to the Audit log to Administrators. An Administrator may sort the Audit log on any displayed field. The Audit log may also be filtered by the contents of any field. Any combination of fields may be involved in defining the filter with individual value ranges for each field.

Time and date information is provided by the host OS and imported to the TOE when an event is recorded regardless of the location of the user performing the action.

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

- FAU_GEN.1, which specifies auditing requirements for the TOE
- FAU_SAR.1, which ensures audit information can be read by the Administrator
- FAU_SAR.2, which prohibits all users read access to the audit records, except those users that have been granted explicit read-access.
- FAU_SAR.3, which allows [searches, sorting, ordering] of audit data based on any of all audit record field values
- FAU_STG.1, which ensures audit records are protected from unauthorized access or deletion

7.3 User Data Protection

The TOE enforces an access control policy for management operations.

The TOE protects three types of data: user security credentials, user authorization permissions, and Security Audit log information. User security credentials include the username, password, and the name of the user. Authorization permissions are used to control the UI elements presented to an authenticated user. The Security Audit log is used as the recording facility of security related events.

The username consists of a string of printable characters that identifies a specific user and must be unique relative to all other usernames hosted by the TOE. The username is stored as a field within a record in a database in clear text. Usernames are managed, *created*, *modified*, and *deleted*, by authorized Administrators and operators with the Manage Users permission.

The password consists of a string of non-printable characters, separate from the username, used to further verify the identity of the user attempting to gain access to the system. The password is stored as a hash derived from the password string; the password is never stored in clear text. Passwords are managed by both Administrators and users. Administrators, and operators with the Manage Users permission are permitted to *create* and *modify* passwords for any user. Users are permitted to *modify* their own password.

User authorization permissions are represented as a set of binary values each corresponding to permission. One of the results of a successful user authentication process is to read the permissions field of the user record which is maintained in memory and associated with the user's communication session. Those permissions are then used by the CIRT Web UI server when generating the user interface elements presented through the browser. Management of the permissions, *assign*, *remove*, is restricted to Administrators. An Administrator may purge (remove) all of the entries in the Security Audit log, presumably to free up disk space, however, after the log is purged an entry is made indicating the log was purged.

The Security Audit log is stored on disk as a database table separate from the CIRT Operations log. The contents only of the Security Audit log is limited to security related events which differs from the Operations log that contains system function events. Management of the Security Audit log, *view*, *purge*, is restricted to Administrators by permission.

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

- FDP_ACC.1 and FDP_ACF.1, which limits access to user management facilities to authenticated Administrators.
- FAU_ARP.1.1, which renders the monitor illegible and executes a session lockout (requiring user authentication) upon detection of a violation.

- FAU_SAA.1.1, which indicates potential security violations by applying a set of rules when monitoring user activities.
- FAU_STG.1.1, FAU_STG.1.2, which restricts the purging of audit records to authenticated Administrators.

7.4 Identification and Authentication

The TOE performs identification and authentication of all users and administrators accessing the TOE. The TOE has the ability to authenticate operators locally using a password or can integrate with a remote authentication server. In the evaluated configuration, The TOE will perform the authentication locally. Operators enter a username and password which is validated by The TOE against the information stored by the TOE. If the authentication succeeds, the operator receives a session token that is used for identification of subsequent requests during that session.

Administrators and Operators are required to submit valid authentication credentials (username and password) before being permitted to access to any part of the TOE. Usernames must comply with minimum formatting requirements and be unique (relative to the other usernames in the system). Passwords must conform to minimum format specifications.

Username formatting requirements include:

- Usernames must be at least 7 characters in length
- Usernames shall not exceed 32 characters in length
- Usernames may use any combination of:
    - uppercase and lowercase alpha characters
    - numeric characters
- Username character formatting shall not be enforced

Minimum password formatting requirements include:

- Passwords shall be at least 7 characters in length
- Passwords shall not exceed 20 characters in length

- Passwords may use any combination of:
    - Uppercase and lowercase alpha characters
    - At least one alpha character (non-numeric, non-punctuation)
    - All numeric characters
- Must include at least one alpha and one numeric character
- Must include at least one non-alphanumeric character
- Password character formatting is enforced

Users are required to enter correct credentials each time they attempt to use the system. Usernames and passwords are stored in a local database and compared each time an Administrator or Operator authenticates.

The user is allowed 5 attempts to submit proper authentication credentials before their account is locked out for 20minutes. An administrator or operator with the Manage Users permission can unlock the account.

The TOE maintains a table, separate from the users table, that houses the list of permissions a user may be assigned; one of those permissions is designated “Administrator” which when granted allows that user to execute any operation on the TOE. Maintenance of user records is restricted to users that have been granted Administrator permissions; a user with non-Administrator permissions may be restricted from certain operations within the CIRT that are not germane to the TOE.

In addition to username and password hash fields, each user record contains a unique userID field and each Role record also contains a unique roleID field. When an Administrator assigns permissions to a user, a third table is generated that contains the combination of the userID and the roleID. A row in this third table is made for each permission granted to a user; or removed from if a permission is denied. Upon successful authentication, the TOE searches this Roles Assignment Table for the permissions granted to the authenticated user. A memory structure is then created and associated with the users other session information. As the user navigates the user interface, the permission structure is interrogated by the code that generates the UI elements. If the permission is there, the UI element is generated and presented to the user, if not, nothing is generated preventing the user from gaining access to the pages associated with a permission. This holds for the pages that allow the modification of the permissions themselves.

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

- FIA_ATD.1, which specifies the list of security attributes belonging to individual users
- FIA_SOS.1, which specifies minimum requirements for passwords
- FIA_UAU.2, which requires operator authentication before any action
- FIA_UID.2, which requires operator authentication before any action.

7.5 Security Management

The TOE provides security management functions via a browser interface. The Administrator logs onto the TOE from a protected network and performs all management functions through the browser interface. The administrator has the ability to control all aspects of the TOE configuration including: user management, information flow policy management, audit management, and system start-up and shutdown.

Administrators, and operators with the Manage Users permission, set the access control policy rules on a per user basis. When the administrator adds a new user, the administrator defines the user access. Users are granted permissions individually. By default, user access is restrictive but the administrator may override the default upon rule creation.

The user permissions configuration page is managed in the same way of any other user interface element of the TOE. The permissions management pages are not generated by the CIRT Web Server if the authenticated user has not been granted the Administrator permission. The only way to modify the permissions is through the web browser interface.

If a user has been granted the Administrator or Manage User permissions, that user is allowed to gain access to the user management pages that facilitate:

- The viewing of user records including usernames and permissions
- Adding new users to the system including username, reset passwords, grant/deny permissions
- Modification of user records including reset passwords and grant/deny permissions
- Deleting users from the system

Administrators are also permitted to manage the Security Audit Log. If a user has been granted the Administrator permission, that user is allowed to gain access to the Security Audit Log pages which allows:

- The viewing of security related events
- Export and print the Security Audit Log
- Sort and filter the entries of the Security Audit Log
- Purge the entries in the Security Audit Log

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

- FMT_MOF.1, which restricts configuration of the Access Control Security Policy to an Administrator
- FMT_MSA.1, which restricts the ability to modify or delete the security attributes defined in Access Control Security Policy to the Administrator
- FMT_MSA.2, which ensures that only correct authentication credentials are accepted
- FMT_MSA.3, which ensures the TOE provides restrictive default values for the Access Control Security Policy
- FMT_MTD.1, which restricts control of user and TOE data to an Administrator
- FMT_SMF.1, which specifies management functions available in the TOE
- FMT_SMR.1, which specifies roles utilized by TOE Administrators.

7.6 TOE Access

Access to all TOE functionality is accomplished via the Administration Console. The console monitors user activity and makes the console illegible when an inactivity threshold is reached. The default timeout is set to 20 minutes.

When the user completes authentication successfully, the CIRT Web Server creates a unique session for that user. Included in the data associated with the session is a count down timer that is set to the current date and time. Each time the user navigates to a new page or modifies the contents of the existing page, that timer value is reset to the current date and time. Once a minute, the CIRT Web Server checks for user activity by subtracting the sessions date and time from the current date and time. If 20 or more minutes has lapsed, the CIRT Web Server logs the user out and displays the login page for re-authentication.

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

- FTA_SSL.3, which provides session termination after 20 minutes of idle time

