Xceedium GateKeeper Version 4.0.0 Security Target

Version 2.0

April 4, 2007

Prepared for:
Xceedium, Inc.
30 Montgomery Street
Jersey City, NJ 07302

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

.

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. Xceedium provides the TOE, which is Xceedium GateKeeper Version 4.0. The TOE is an IT management tool that provides an organization the ability to remotely maintain multiple network devices (servers, routers, and platforms) via any Java enabled browser, SSL transmission, and administrator/user/device profiles and access policies.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by Xceedium and it environment and the organizational policy that the Xceedium must fulfill.
- Section 4 –Security Objectives
  This section details the security objectives of the Xceedium and its environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for Xceedium and IT Environment that supports the TOE, and details the assurance requirements for EAL3.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the Xceedium that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any Protection Profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Xceedium GateKeeper Version 4.0.0 Security Target

ST Version – Version 2.0

ST Date –April 4, 2007

TOE Identification – Xceedium GateKeeper Version 4.0.0

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, ISO/IEC 15408

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005.
  - Part 3 Conformant

.

- Evaluation Assurance Level 3 (EAL3)

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Acronyms

The acronyms used within this Security Target:

ACM	Access Control Management
AGD	Administrator Guidance Document
CC	Common Criteria
CD-ROM	Compact Disk Read Only Memory
CM	Control Management
DAC	Discretionary Access Control
DO	Delivery Operation
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
I/O	Input/Output
NIST	National Institute of Standards and Technology
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
SF	Security Functions

.

SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control

2. TOE Description

The Target of Evaluation (TOE) is the Xceedium appliance Xceedium GateKeeper 4.0.0, hereafter referred to as the TOE. The product is designed by Xceedium, located at, 30 Montgomery Street, Jersey City, NJ 07302.

2.1 Product Type

The TOE is an IT management appliance that provides an organization the ability to remotely maintain multiple network devices (servers, routers, and platforms) via any Java enabled browser, SSL transmission (using OpenSSL 0.9.7j), and administrator/user/device profiles and access policies.

2.2 Product Description

The TOE is a rack mounted network appliance. The TOE provides remote IT support and monitoring to remote sites or local office locations via a Java enabled web browser. Common environments for use are hosting/co-location facilities where network access methods, monitoring, and security are essential. All communications between the web-browser and TOE is via SSL (encrypted).

An administrator configures user access to network devices. The administrator configures custom module permissions per user to the specific network devices. User entity includes both account and contact information. Both an authorized administrator and a user can update the user's account information for First Name, Last Name, Password, Phone number, Beeper number, Email address, and other description such as department, and location… Only the authorized administrator can update the user identifier. The TOE enforces the associations between a user and a device. The attributes assigned to this relationship are the access methods or services available to the user for this device. Every network device can be accessed by various methods that include: VNC, Telnet, and SSH,. Additional optional capabilities include remote power, console, and IP-based KVM access.

Users and administrators access the TOE, but only administrators can access and set TOE security functions. Administrators may view logins, user sessions, and reporting; set configuration parameters and conduct maintenance tasks; create custom access; utilize management features; and set associations between users and devices. All administrative actions are mediated by the TOE using an access control policy.

The evaluated configuration of Gatekeeper does not support the following product features:

1. Fail Over
2. Radius Server
3. Whole Security Scan
4. Modem
5. SNMP
6. NTP communications
7. Active Directory Server

2.3 Product Features

The TOE implements the following features:

- Web-based access to establish VNC, Telnet, SSH, and standard operating system specific GUI sessions to network devices over TCP/IP.
- Optional remote power, console, and/or IP based KVM management. (Users are able to turn attached network devices on or off, console into network devices such as routers and switches, and access servers down to the BIOS level).
- External appliance LCD display for entering initial host connection information or checking on system configuration.
- Browser access to all types of graphical and text based sessions using Windows, Mac, UNIX, Telnet, Secure Shell, 3270, and web-based applications accessed via an SSL tunnel to the network server.
- Supported systems platforms: Intel, Mac, Sun, HP, AIX, and IBM
- Supported network devices: Servers, Desktop PC's, Routers, switches, terminal servers, private branch exchange (PBX), and other network enabled devices.
- Authentication via TOE web server
- Multiple users can have GUI access to the same Windows, Unix, or Mac systems simultaneously to access a network device
- Multiple text based UNIX sessions to access a network device
- SSL user communication – Note the evaluation did not address the correctness of the SSL implementation
- Single Access Port to network devices
- Web interface GUI for administrators and users
- Monitoring, logging, and alert emails for monitored events

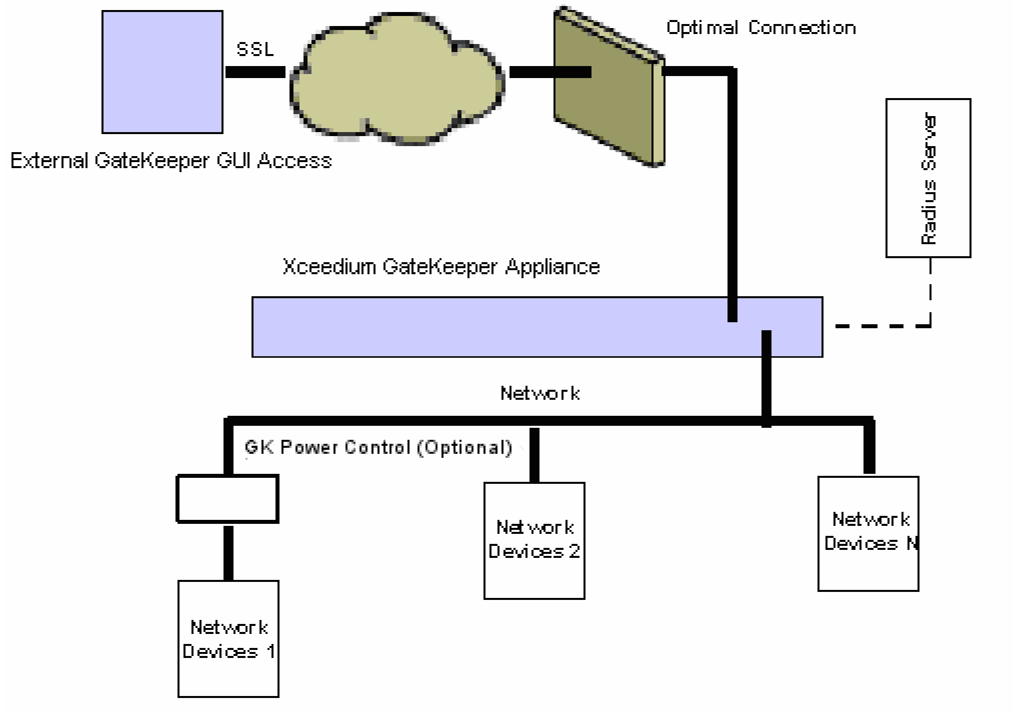
2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The TOE is an appliance and as such, its ports are its interfaces. The majority of the TOE's functioning is performed via its network port. The network port is used by both administrators and users to access the IT network environment. This interface is provided by the TOE through a SSL connection. A custom internal TOE web server provides an administrative interface for all TOE management functions called the Administrative Modules. From this GUI interface, the administrator manages user access. The actual browser is not part of TOE. The following diagram depicts the GUI in purple as it is how the administrator actually enters data to create a request to the TOE.

A second physical boundary is its LCD Panel and four configuration buttons on the front of the TOE. This external interface allows for basic network configuration of the device out of the box. Once the TOE basic network configuration has been completed via the LCD Panel and buttons that interface with the configuration firmware, the device is rebooted, and the web-based configuration of network parameters are completed via an Internet Browser (any Java-enabled web browser). Once in the evaluated configuration the TOE is assumed to be in a protected environment and the LCD Panel and buttons are not used and do not need any further description.



Xceedium GateKeeper TOE in its environment

2.4.2 Hardware Specifications

The following is a list of hardware used within the TOE.

Chassis	1U IPC Chassis
Power Supply	200W Power Supply Unit (PSU)
System Board	Single Board Computer (SBC) with socket 478
CPU (Model Specific)	Intel Celeron, Pentium 4
Memory (Model Specific)	512 MB DDR
Disk (Model Specific)	128MB Disk-on-Module / Solid-State
Additional Storage	128MB CompactFlash
Display	LCD Display

2.4.3 Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces.

2.4.3.1 Security Audit

The internal TOE Web Server generates audit records related to the authentication and management of the TOE that are stored and protected in an internal database. The function records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by the user once authenticated. All auditable actions can be found in Active Logins, Sessions, Logs and Report interface. The Logs Report Parameters screen allows administrator selection of the specific report information to be generated.

2.4.3.2 User Data Protection

The TOE enforces user access policies by restricting what management functions an authorized administrator may perform on the TOE. Access is restricted based on the user identifier and privileges associated with the requestor. The TOE also supports a separate access control policy that controls access between users and devices. Access to devices is limited based upon the user identifier associated with the requestor and device service access list. A user

.

can access a given service on a given device if the device service access control list specifically allows access to the requested service for the device..

2.4.3.3 Identification and Authentication

The TOE requires users to provide unique identification and authentication data (User ID and Password) before any access to the system is granted. The TOE provides authorized administrator's the ability to define user device access.

2.4.3.4 Security Management

An authorized administrator is any user that has an administrative privilege. Users with no administrative privileges are simply called users. The TOE is managed through the Administrative modules (Config, Services, Sessions, Users, Devices, Associations), a SSL virtual desktop web-based interface. Through this interface all TOE management can be performed, including user management and the configuration of IT devices access functions. This interface is restricted to authorized administrators, which provides the administrator the ability to set user attributes and privileges, as well as assign privileges for different levels of administrative access.

Administration functions and programming tasks are done using PERL scripts. A Spadmin daemon accepts input from specific functions on the web sever and LCD to control system configuration parameters. Scripts operate the features of the optional TOE power, console, and IP based KVM device components.

2.4.3.5 Protection of Security Functions

The TOE protects itself by providing a custom OS in firmware and only permitting trusted processes to run on the TOE. Furthermore, Gatekeeper interacts with users through well-defined interfaces designed to ensure that its security policies are always enforced. The TOE also generates timestamps for use within the audit trail.

3. Security Environment

The security environment for the functions addressed by this specification includes threats, security policies, and usage assumptions, as discussed below.

3.1 Threats to Security

3.1.1 TOE Threats

T.AUDIT_COMPROMISE A process or user may cause audit data to be inappropriately accessed (viewed, modified or deleted),

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.TSF_COMPROMISE A malicious user or process may cause the TOE, configuration data, or sensitive user data to be inappropriately accessed (viewed, modified or deleted) allowing a breach in the TSF security policies.

T.UNAUTH_ACCESS A user may gain unauthorized access (view, modify, delete) to devices

3.2 Organization Security Policies

P.MANAGE The system must provide authorized administrators with utilities to effectively manage the security functions of the TOE

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

P.AUDIT Users of the system shall be held accountable for their security relevant actions within the system.

3.3 Secure Usage Assumptions

3.3.1 Physical Assumptions

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

3.3.2 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.

4. Security Objectives

This section defines the security objectives for the TOE and its environment. These objectives are suitable to counter all identified threats and cover all identified organizational security policies and assumptions. The TOE security objectives are identified with 'O.' inserted at the beginning of the name and the environment objectives are identified with 'OE.' inserted at the beginning of the name.

4.1 IT Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data as defined by the administrator.

O.AUDIT The TSF must record the security relevant actions of users of the TOE. The TSF must present this information in a readable format to authorized administrators and ensure that only authorized users are able to access this information.

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

O.DEVICE_ACCESS The TOE will control access to devices based upon the identity of users.

O.MANAGE The TOE must provide services that allow effective management of its functions and data.

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

O.TIME The TOE provides adequate time stamps for audit records.

O.TOE_PROTECTION The TOE will protect itself and its assets from external access, interference and tampering.

4.2 Non-IT Security Objectives for the Environment

OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

OE.PERSON Authorized users of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.

.

OE.PHYCAL Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from physical attack that might compromise the TOE security objectives.

5. IT Security Requirements

This section provides a list of all security functional requirements for the TOE.

5.1 TOE Security Functional Requirements

The following table lists the SFRs.

Security Functional Class	Security Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit Data Generation
	FAU_SAR.1 Audit Review
	FAU_STG.1 Protected audit trail storage
User Data Protection (FDP)	FDP_ACC.1(a and b) Subset Access Control
	FDP_ACF.1(a and b) Security attribute based access control
Identification and authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UAU.7 Protected authentication feedback
	FIA_UID.2 User identification before any action
Security management (FMT)	FMT_MOF.1 Management of security functions behavior
	Management of security attributes – authentication data (FMT_MSA.1a)
	Management of security attributes – user identity (FMT_MSA.1b)
	Management of security attributes – service associations (FMT_MSA.1c)
	FMT_MSA.3(a and b) Static attribute initialization
	FMT_MTD.1(a)Management of TSF data (security-relevant privileges)
	FMT_MTD.1(b) Management of TSF data (audit data)
	FMT_MTD.1(c) Management of TSF data (timestamp)
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1 Reliable time stamps

Table 1 Security Functional Components

.

5.1.1 Audit Requirements

5.1.1.1 Audit Data Generation (FAU_GEN.1)

5.1.1.1.1 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) **[All authentication attempts to the TOE**

d) **Adding and Removing user accounts**

e) **Changes to authentication data (passwords)**

f) **Access Control descisions**

g) **Changes to user attributes and privileges]**.

5.1.1.1.2 FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[no other additional information]**

5.1.1.2 Audit Review (FAU_SAR.1)

5.1.1.2.1 FAU_SAR.1.1

The TSF shall provide **[authorized administrators]** with the capability to read **[all audit information]** from the audit records.

5.1.1.2.2 FAU_SAR.1.2

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

5.1.1.3 Protected audit trail storage (FAU_STG.1)

5.1.1.3.1 FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised deletion.

5.1.1.3.2 FAU_STG.1.2

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

5.1.2 User Data Protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1(a))

5.1.2.1.1 FDP_ACC.1a.1

The TSF shall enforce the **[Management Access Control SFP]** on **[subjects: authorized administrators, objects: the Administrative Modules, operations: access to Administrative Modules]**.

5.1.2.2 Subset access control (FDP_ACC.1(b))

5.1.2.2.1 FDP_ACC.1b.1

The TSF shall enforce the **[Device Access Control SFP]** on **[subjects: users, objects: devices, operations: access to devices]**.

5.1.2.3 Security attribute based access control (FDP_ACF.1(a))

5.1.2.3.1 FDP_ACF.1a.1

The TSF shall enforce the **[Management Access Control SFP]** to objects based on the following;

[Subject (authorized administrators): user identity and

Object (Administrative Modules): security privileges].

5.1.2.3.2 FDP_ACF.1a.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[An authorized user will be granted access to the Administrative Modules if their user identity is assigned the appropriate privilege(s)]**.

5.1.2.3.3 FDP_ACF.1a.3

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

5.1.2.3.4 FDP_ACF.1a.4

The TSF shall explicitly deny access of subjects to objects based on the **[no additional explicit denial rules]**.

5.1.2.4 Security attribute based access control (FDP_ACF.1(b))

5.1.2.4.1 FDP_ACF.1b.1

The TSF shall enforce the **[Device Access Control SFP]** to objects based on the following;

[Subject (users): user identity and

Object (devices): service access control list].

5.1.2.4.2 FDP_ACF.1b.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[A user can access a given service on a given device if the device service access control list specifically allows access to the requested service]**.

.

5.1.2.4.3 FDP_ACF.1b.3

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

5.1.2.4.4 FDP_ACF.1b.4

The TSF shall explicitly deny access of subjects to objects based on the **[no additional explicit denial rules]**.

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

5.1.3.1.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: **[user identity, authentication data, device associations, and security privileges]**.

5.1.3.2 User authentication before any action (FIA_UAU.2)

5.1.3.2.1 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.

5.1.3.3 Protected authentication feedback (FIA_UAU.7)

5.1.3.3.1 FIA_UAU.7.1

The TSF shall provide only **[obscured feedback]** to the user while the authentication is in progress.

5.1.3.4 User identification before any action (FIA_UID.2)

5.1.3.4.1 FIA_UID.2.1

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behavior (FMT_MOF.1)

5.1.4.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to **[*disable, enable, modify the behavior of*]** the functions **[access control]** to **[authorized administrators]**.

5.1.4.2 Management of security attributes – authentication data (FMT_MSA.1(a))

5.1.4.2.1 FMT_MSA.1a.1

The TSF shall enforce the **[Management Access Control SFP]** to restrict the ability to **[*modify, delete*]** the security attributes **[authentication data]** to **[authorized administrators and users authorized to modify their own authentication data]**.

5.1.4.3 Management of security attributes – user identity (FMT_MSA.1(b))

5.1.4.3.1 FMT_MSA.1b.1

The TSF shall enforce the **[Management Access Control SFP]** to restrict the ability to **[create]** the security attributes **[user identity]** to **[authorized administrators]**.

5.1.4.4 Management of security attributes – service associations (FMT_MSA.1(c))

5.1.4.4.1 FMT_MSA.1c.1

The TSF shall enforce the **[Device Access Control SFP]** to restrict the ability to **[create, *modify, delete*]** the security attributes **[service access control list]** to **[authorized administrators]**.

5.1.4.5 Static attribute initialization (FMT_MSA.3(a))

5.1.4.5.1 FMT_MSA.3a.1

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

5.1.4.5.2 FMT_MSA.3a.2

The TSF shall allow the **[authorized administrators]** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.6 Static attribute initialization (FMT_MSA.3(b))

5.1.4.6.1 FMT_MSA.3b.1

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

5.1.4.6.2 FMT_MSA.3b.2

The TSF shall allow the **[authorized administrators]** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.7 Management of TSF data (FMT_MTD.1(a)) (Security-Relevant Privileges)

5.1.4.7.1 FMT_MTD.1.1(a)

The TSF shall restrict the ability to **[*modify, delete/ clear*]** the **[security-relevant privileges for users]** to **[authorized administrators]**.

5.1.4.8 Management of TSF data (FMT_MTD.1(b)) (Audit data)

5.1.4.8.1 FMT_MTD.1.1(b)

The TSF shall restrict the ability to **[*query*]** the **[audit data]** to **[authorized administrators]**.

5.1.4.9 Management of TSF data (FMT_MTD.1(c)) (Timestamp)

5.1.4.9.1 FMT_MTD.1.1(c)

The TSF shall restrict the ability to **[*modify*]** the **[timestamp]** to **[authorized administrators]**.

5.1.4.10 Specification of Management Functions (FMT_SMF.1)

5.1.4.10.1 FMT_SMF.1.1

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

a) **Management of access control (both Management and Device access control polices)**

b) **Management of audit functions**

c) **Management of the timestamp].**

5.1.4.11 Security roles (FMT_SMR.1)

5.1.4.11.1 FMT_SMR.1.1

The TSF shall maintain the roles **[authorized administrators and users authorized to update authentication data]**.

5.1.4.11.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.5 Protection of the TOE security functions (FPT)

5.1.5.1 Non-bypassability of the TSP (FPT_RVM.1)

5.1.5.1.1 FPT_RVM.1.1

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

5.1.5.2 TSF domain separation (FPT_SEP.1)

5.1.5.2.1 FPT_SEP.1.1

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

5.1.5.2.2 FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.3 Reliable time stamps (FPT_STM.1)

5.1.5.3.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.2 IT Requirements for the Environment

There are no IT requirements for the environment.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3: Authorization Controls
	ACM_SCP.1: TOE CM Coverage
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2: Security Enforcing High Level Design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life Cycle Support	ALC_DVS.1: Identification of security measures
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 2 EAL3 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Authorization controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.

.

ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.
ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.

ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

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

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.

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

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1c The presentation of the high-level design shall be informal.

ADV_HLD.2.2c The high-level design shall be internally consistent.

ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

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

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

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

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

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

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

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

5.3.5 Life Cycle (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

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

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.

ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

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

5.3.6.2 Functional testing (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

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

5.3.6.3 Functional testing (ATE_FUN.1)

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

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

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

5.3.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

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

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.

AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

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

AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

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

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

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

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

FAU_GEN.1 Audit Data Generation, FAU_STG.1 Audit storage protection

The TOE can generate audit records of all the events listed in section 5.1.1.1 as part of the definition of FAU_GEN.1.1 with the exception of the event for audit startup and shutdown as auditing is always on. Audit records include at least event time and date, event type, subject identity and outcome (success or failure) as well as other data specific to the report type such as port, status, address etc.. The audit trail is protected so that only an authorized administrator can read the audit records. All audit trail records are stored in the TOE internal database. The Administration Modules are the only interface to the audit trail and its access is restricted. Only authorized administrators are able to view these audit records through the Administration Modules using the Sessions (Sessions -> logs) module. No user is permitted to alter the audit trail.

The TOE generates audit data for all authentication attempts to the TOE, including successful and unsuccessful attempts. The audit function also generates records for the creation, removal and modification of user accounts, network device access attempts, as well as the security-relevant privileges assigned to the accounts. The TOE also records all changes to authentication data, whether changed by an administrator or the user.

Administrators have access to a sessions screen portion of the Administrative Modules from which three types of reports can be –Active Logins, Sessions, or Logs.

- Active Logins (under Sessions-> Manage Sessions link)– lists the users that are presently logged in to the TOE
- Sessions (under Sessions ->Overview link)– lists the sessions that are presently in use to manage devices from the TOE
- Logs (under Sessions -> Logs link) – lists the logs of previous transaction made to and/or from the TOE.

FAU_SAR.1 Audit Review

The TOE presents the audit data in a format viewable by authorized administrators for review. The Report screen displays the generated report.

6.1.2 User Data Protection

FDP_ACC.1a Subset Access Control (Management Access Control)

The TOE controls access to the Administrative Modules by limiting access to authorized administrators for all requests made to the Administrative Modules.

FDP_ACF.1a Security Attribute based access control (Management Access Control)

The TOE maintains a list of users (authorized users and administrators), authentication data and associated security privileges. A user must successfully authenticate with a valid username and password before any access will be granted to the administration modules or devices. Based upon the user’s identity, the user is assigned association privileges, which are then used to provide access to specific management functions controlled by the TOE.

The TOE controls security policies that grant access to administrative functions based upon if a user identify has the privilege associated with the specific management function. If a user has the correct privilege, access is granted. If not, access is denied.

FDP_ACC.1b Subset Access Control (Device Access Control)

The TOE controls access to the devices by limiting access to users for all requests made to devices.

FDP_ACF.1b Security Attribute based access control (Device Access Control)

The TOE protects devices that are logically located behind it on a network. The TOE maintains an association between users and devices, called a device association. Users are associated with particular devices and for particular services on those devices; this association is maintained in a service access control list. The TOE grants access to a device based upon if a user identity has the device associated with the specific service request. If a user has the correct service association, access is granted. If not, access is denied.

The possible set of services that can be associated with a user is:

- ***VNC*** **(options: Standard, Linux, Web version)**– graphical access to a device (requires the VNC service to be installed and running on the device)
- ***Telnet*** – standard, unsecured Telnet access to a device
- ***SSH*** **–** secured, in-band console access to a device (requires SSH v1 or v2 to be installed and running on the device)
- ***SSH2Telnet*** **–** allows secured access to a Telnet-enabled device by using the secure shell protocol
- ***R DP*** **–** Remote desktop connection (required the remote desktop connection enabled)
- ***Out-of-Band*** – serial (RS-232) console access of a device.
- ***Power*** – remote boot (power on/off/reboot) of a device.
- ***Service*** – Other services defined by the authorized administrator (e.g. remote desktop)

6.1.3 Identification and Authentication

FIA_ATD.1 User Attribute Definition

Authorized administrator and user accounts in the TOE have the following attributes: user name, userID, authentication data (password), device associations, and their assigned privileges. The authentication data can be set to required levels using additive hierarchal strength as defined by the administrator including the following: 0-Require New Password, 0+1-Require length of X to Y as set by administrator, 1+2-Require Alpha-Numeric, 2+3-Require Upper and Lower Case, 3+4-Require Special Characters. The evaluated configuration requires level 2 and the minimum password length is six characters.. The authentication data is encrypted and stored inside the TOE.

SSL is used to ensure secure access to the login interface. The TOE controls security policies that grant access to operations, users, and objects. The TOE makes use of the three types of data entities. User entities relate to the user accounts, Device entities relate to the devices configured for access or monitoring, and associations are the relationship entities between users and devices.

A TOE administrator configures custom module permissions per user (a person configured for access to the TOE). The user entity includes both account (UserId and password) and contact information (First name, Last Name, Phone number, Beeper number, Email address, other description such as department, location, etc) for a user. Both an administrator and a user can update the user's entity information (Username, Password, First Name, Last Name, Phone number, Beeper number, Email address, other description such as department, location, etc.)

Module permissions determine the features that the user will have access to, and type of user (access and/or monitor). Typically users have access and monitoring permissions, and administrators have all permissions.

FIA_UAU.2 User Authentication before Any Action and **FIA_UID.2 User identification before any action**

The Identification and Authentication security function provides for user logon (authorized administrators and users), and management of user profiles.

The administrative log-in and administration configuration modules allow for Configuration and Administration of the TOE itself, as well as the permission to create/update/delete Users, Devices, and Associations. Access is restricted to an administrator. Once authenticated, the administrator creates associations between a specific User and a specific Device Associations are enforced by the TOE. This includes what devices each user is allowed to access and/or manage. The association also controls what type of access the user will have to each Device.

The TOE requires users (authorized administrators and users) to provide unique identification and authentication data (UserId and passwords) before any access to the system is granted. If the password comparison is the same between the user and TOE stored password, the user is granted access. No administrative or user actions are allowed until successful authentication as an authorized administrator or user

FIA_UAU.7 Protected authentication feedback

The TOE GUI Gateway interface uses a standard user name and password command line where the password is obscured. If the UserId or Password is entered incorrectly, the TOE GUI will display a message stating “Bad User Id or Password” on the login page allowing the user to make an additional attempt to authenticate. An administrator can set a parameter in the TOE to allow only X number of “failed login attempts”. If that number is reached, the user’s ID is disabled and prompts them to contact an administrator. An administrator can also set the TOE to notify an administrator via email of the event.

6.1.4 Security Management

FMT_SMR.1 Security Roles

The ST identifies two roles upon which the SFRs are defined – authorized administrators and users authorized to update their authentication data. The TOE realizes the authorized administrator with two pre-defined roles, Administrator and Configurator. Administrators can define other users each with its own set of privileges. The Configurator is able to access configuration pages (https://TOEip/config/) to configure addition network information, monitor settings, and purge logs. When a new user account is created, it can be assigned one or more privileges. User accounts with no administrative privileges are called users. Users and Administrators are able to view/modify authentication data) and contact information.

FMT_MOF.1 Management of security functions behavior

There are two pre-defined administrators in the TOE - Administrator and Configurator. Different types of administrators can be created but all users with any ability to manage TOE data are administrators in CC terminology. The TOE restricts the management of access control to authorized administrators. Only authorized administrators are able to enable, disable or modify the behavior of administrator accounts.

Authorized administrators control the TSF. A TOE administrator configures custom permissions per user (a person configured for access to the TOE). The TOE consists of a number of administrative modules, which is a set of button selections available at the top of the screen on the user’s web browser window each with its own set of features. A user’s permissions are controlled by their access to the modules. Administrative module permissions determine the features and devices that the user will have access to by limiting the features a user can access.

The user entity includes both account and contact information for a user. Both an administrator and a user can update the user’s entity information with the exception of the userid – only an administrator can create userid.

Below is a summary of the Administration Modules:

- Sessions – a setting used to manage active logins, to view logs and view/create audit reports. This privilege is assigned to the GateKeeper administrators
- Config – a setting allowing this user to utilize the Configuration module features (setting Login, Session timeouts, Password security level, Password failure limit and Password Change interval), assigned to the TOE administrators
- Services – a setting allowing this user to utilize the Services module features which includes creating custom access methods to run either their own local clients or launch a URL , assigned to the TOE administrators

- Users – a setting allowing this user to utilize the Users module features which includes create, update and delete user account and privileges, assigned to the TOE operation administrators
- Devices – a setting allowing this user to utilize the Devices module features which includes create, update and delete devices, assigned to the TOE operation administrators
- Associations – a setting allowing this user to utilize the Associations module features which includes create, update and delete association between users and devices, assigned to the TOE administrators

FMT_MSA.1a,b, and c Management of security attributes

The TOE enforces the Management Access Control SFP in allowing that only authorized administrators to create, modify, and delete user accounts and authentication data. Users have the ability to change and modify their authentication data. Likewise, the TOE enforces the Device Access Control SFP in limiting only authorized administrators the ability to create, modify, and delete device associations.

FMT_MSA.3a and b Static attribute initialization

The TOE provides restrictive default values to provide enforcement of the Management Access Control SFP and Device Access Control SFP, which can be overridden by authorized administrators when creating new accounts and device associations.

FMT_SMF.1 Specification of management functions

The TOE provides the ability to manage user accounts, including the ability to create, delete and modify existing accounts, to authorized administrators.

The TOE provides an authorized administrator the ability to manage audit and log functions by providing an audit review capability in the reporting menu. The administrator is also permitted to purge the audit logs.

FMT_MTD.1a Management of TSF Data (Access Control)

The TOE restricts the ability to administer the security-relevant privileges for users to only authorized administrators.

The TOE restricts the ability to assign modules to users through authorized administrators. All users must change their default authentication information when they try to access TOE first time. User and administrator can able to update authentication information. Successful authentication provides administrators to create/modify/delete services, users, devices and associations. In Create User GUI, administrators are able to define a userid and define or modify module privileges for user. The Create User interface also provides the authorized administrator the ability to configure authentication as local.

FMT_MTD.1b Management of TSF Data (Audit Data)

The administrative module provides the abilities for only authorized administrators to perform the following tasks:

To view and query the audit logs

To purge audit logs

FMT_MTD.1c Management of TSF Data (Timestamp)

The administrative module provides the abilities for only authorized administrators to set the hardware clock supplied with the device. This function is restricted to the Configurator by default.

6.1.5 Protection of Security Functions

FPT_RVM.1 and FPT_SEP.1 Non-bypassability and Process Isolation

The TOE is a hardware appliance that contains a custom operating system that runs in firmware, and supports only trusted processes. The Gatekeeper appliance provides no file abstractions or permanent storage for “executables” to remain for further execution. Furthermore, the TOE has been carefully designed to offer well-defined interfaces that ensure that access to protected resources is subject to the applicable Gatekeeper security policies.

FPT_STM.1 Reliable timestamp

The TOE includes a hardware time clock within the appliance which is used to stamp all records generated by the TOE.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL3 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by Xceedium ensure that the TOE and its configuration items are uniquely identified. Xceedium uses a CM system that ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. Xceedium performs configuration management on the TOE implementation representation, design, tests, vulnerability, delivery, user and administrator guidance, life cycle documentation, and the CM documentation. These activities are documented in:

- Xceedium Configuration Management Plan

The Configuration Management assurance measure satisfies the following Assurance requirements:

- ACM_CAP.2
- ACM_SCP.1

6.2.1.2 Life Cycle Support

Xceedium ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive security plan. The security plan includes controls that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure development of the TOE.

- Xceedium Life Cycle Document

The Life Cycle Support assurance measure satisfies the following Assurance requirement:

- ALC_DVS.1

6.2.2 Delivery and Guidance

Xceedium provides delivery documentation that explains how the TOE is delivered and procedures to identify the TOE. These procedures are documented in:

- Xceedium Product Delivery Process
- Xceedium GateKeeper v4.0 Series Installation Guide, v4.2, February 23, 2007

Xceedium provides administrator guidance in the installation and initialization procedures. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install Xceedium products in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration.

The administrator guidance is documented in:

- Xceedium GateKeeper v4.0 Series Administration Guide v4.1, February, 2007
- Xceedium GateKeeper v4.0 Series Installation Guide, v4.2, February 23, 2007
- Xceedium GateKeeper v4.0 Series User's Guide, v4.1, February 2007

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1;
- ADO_IGS.1;
- AGD_ADM.1; and,
- AGD_USR.1.

6.2.3 Development

The Design Documentation provided for the TOE is provided in these documents:

- Xceedium GateKeeper v4.0 Series Administration Guide v4.1, February, 2007
- Xceedium GateKeeper v4.0 Series Installation Guide, v4.2, February 23, 2007
- Xceedium GateKeeper v4.0 Series User's Guide, v4.1, February 2007
- Xceedium GateKeeper Implementation
- Xceedium GateKeeper System Design

These documents serve to describe the security functions of the TOE to include a description of the TOE TSF in terms of (including which of the subsystems are security enforcing), a functional specification of all interfaces and behavior, and the TOE external interfaces. The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.1;
- ADV_HLD.2; and,
- ADV_RCR.1.

6.2.4 Tests

The Test Documentation is found in the following documents:

- Test Plan Document For Xceedium GateKeeper Version 4.0 Security Functions
- Test Coverage Document For Xceedium GateKeeper Version 4.0
- Test Procedure Document For Xceedium GateKeeper Version 4.0

These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents provide an analysis that demonstrates the functional specification has been appropriately tested.

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2;
- ATE_DPT.1
- ATE_FUN.1; and,
- ATE_IND.2.

6.2.5 Vulnerability Assessment

Xceedium provides guidance documentation that is complete, clear and concise. The guidance documentation provides the requirements for the intended deployment environment, including procedural, physical, and personnel controls. The guidance documentation ensures that the TOE can be configured in a secure manner.

Each probabilistic or permutational mechanism used by the TOE must satisfy the SOF-Basic requirements. The only probabilistic or permutational mechanism used in the TOE is the authentication mechanism (FIA_UAU). Xceedium has performed a strength of function analysis that indicates that the authentication mechanism fulfills at least SOF-basic. Similarly, Xceedium performed a vulnerability analysis of the TOE to identify weaknesses that can be exploited in the TOE. Both the strength of function analysis and the vulnerability analysis are documented in:

- Xceedium GateKeeper Vulnerability Analysis
- Xceedium Strength of Function Analysis

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_MSU.1
- AVA_SOF.1; and,
- AVA_VLA.1.

7. Protection Profile Claims

There are no PP claims for this evaluation.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	O.PROTECT	O.ACCESS	O.AUDIT	O.TIME	O.DEVICE_ACCESS	O.AUDIT_PROTECTION	O.MANAGE	O.TOE_PROTECTION
T.AUDIT_COMPROMISE						X		
T.PRIVIL	X	X						
T.TSF_COMPROMISE					X			X
T.UNAUTH_ACCESS								X
P.MANAGE		X					X	
P.PROTECT	X	X						
P.AUDIT			X	X				

Table 3 Environment to Objective Correspondence

8.1.1.1 T.AUDIT_COMPROMISE

A process or user may cause audit data to be inappropriately accessed (viewed, modified or deleted), or prevent future records from being recorded, thus masking an attacker's actions.

This threat is countered by ensuring that the TOE must provide protection for its audit data (O.AUDIT_PROTECTION).

8.1.1.2 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.ACCESS objective provides for authentication of users prior to any TOE function access thus preventing unauthorized access. The O.PROTECT objective addresses this threat by providing TOE self-protection.

8.1.1.3 T.TSF_COMPROMISE

A malicious user or process may cause the TOE, configuration data, or sensitive user data to be inappropriately accessed (viewed, modified or deleted) allowing a breach in the TSF security policies

This threat is countered by ensuring that the TSF is protected under the TOE objective for TOE protection (O.TOE_PROTECTION). The environment will also protect the TSF from a compromise through physical means (OE.PHYCAL).

8.1.1.4 T.UNAUTH_ACCESS

A user may gain unauthorized access (view, modify, delete) to devices.

This Threat is countered by ensuring access to devices is controlled by a discretionary policy (O.DEVICE_ACCESS). Additionally the TOE ensures its access polices are always invoked (O.TOE_PROTECTION)

8.1.1.5 P.MANAGE

The system must provide authorized administrators with utilities to effectively manage the security functions of the TOE.

The O.MANAGE security objective supports this policy by ensuring that the TOE provides management functions for the authorized administrators use. The O.ACCESS security objective support this objective by allowing only authorized users to access the TOE resources. The O.ACCESS supports this policy by only allowing authorized users to access only appropriate TOE functions and data as defined by the administrator.

8.1.1.6 P. PROTECT

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

The O.ACCESS objective supports this policy by requiring authentication prior to all access to any data, only allowing authenticated and authorized users access to the TOE. The O.PROTECT objective addresses this policy by providing TOE self-protection.

8.1.1.7 P. AUDIT

Users of the system shall be held accountable for their security relevant actions within the system..

The O.AUDIT objective supports this policy by requiring that all security relevant actions are recorded and can be reviewed by authorized administrators. The O.TIME objective supports this policy by providing a reliable timestamp that is used in the audit records.

.

8.1.1.8 Security Objectives for the Non-IT Environment Rationale

Table 4: Security objectives for the non-IT environment mapped to assumptions identifies security objectives for the non-IT environment in which the TOE is designed to operate and provides a mapping to assumptions that are made about that environment.

Security Objectives for the Non-IT Environment	Assumptions
OE.INSTALL	A.MANAGE
OE.PERSON	A.NOEVIL
OE.PHYCAL	A.LOCATE

Table 4: Security objectives for the non-IT environment mapped to assumptions

OE.INSTALL - Ensuring proper installation, management, and operation of the TOE to protect both itself and its resources addresses the assumption A.MANAGE.

OE.PERSON - This objective ensures that the TOE is operated in a secure manner by competent, non-hostile, trained personnel, which addresses A.NOEVIL assumption.

OE.PHYCAL - This objective ensures that the TOE is operated in an environment that will protect it from physical threats and attacks that can disturb and corrupt the information generated. This objective addresses A.LOCATE.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 5** indicates the requirements that effectively satisfy the individual objectives.

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

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.PROTECT	O.ACCESS	O.AUDIT	OAUDIT_PROTECTION	O.DEVICE_ACCESS	O.TIME	O.MANAGE	O.TOE_PROTECTION
FAU_GEN.1			X					
FAU_SAR.1			X	X				
FAU_STG.1				X				
FDP_ACC.1a		X						
FDP_ACC.1b					X			

.

	O.PROTECT	O.ACCESS	O.AUDIT	OAUDIT_PROTECTION	O.DEVICE_ACCESS	O.TIME	O.MANAGE	O.TOE_PROTECTION
FDP_ACF.1a		X						
FDP_ACF.1b					X			
FIA_ATD.1		X			X			
FIA_UAU.2	X							
FIA_UAU.7	X							
FIA_UID.2	X							
FMT_MOF.1							X	
FMT_MSA.1a							X	
FMT_MSA.1b							X	
FMT_MSA.1c							X	
FMT_MSA.3a							X	
FMT_MSA.3b							X	
FMT_SMF.1							X	
FMT_SMR.1	X							
FMT_MTD.1a							X	
FMT_MTD.1b				X			X	
FMT_MTD.1c						X	X	
FPT_RVM.1								X
FPT_SEP.1								X
FPT_STM.1						X		

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.PROTECT

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

The TOE is required to identify and authenticate all users prior to any access and does not provide any authentication data feedback to users. [FIA_UAU.2, FIA_UID.2, FIA_UAU.7] The TOE requires that users be assigned to roles to determine the level of access granted to the TOE. [FMT_SMR.1].

8.2.1.2 O.ACCESS

The TOE must allow authorized users to access only appropriate TOE functions and data as defined by the administrator.

The TOE must prevent unauthorized users from accessing the administrative modules. [FDP_ACC.1a, FDP_ACF.1a]. The TOE requires that all users of the TOE be unique and have unique data. [FIA_ATD.1]

8.2.1.3 O.AUDIT

The TSF must record the security relevant actions of users of the TOE. The TSF must present this information in a readable format to authorized administrators and ensure that only authorized users are able to access this information.

The TOE will record security relevant events that include details about the events themselves in an audit trail that can be reviewed by authorized administrators. [FAU_GEN.1, FAU_SAR.1]

8.2.1.4 O.AUDIT_PROTECTION

The TOE will provide the capability to protect audit information.

The TOE prevents unauthorized deletion or modification of audit records [FAU_STG.1]. The TOE only permits the authorized administrator to access the audit trail [FAU_SAR.1, FMT_MTD.1b].

8.2.1.5 O.DEVICE_ACCESS

The TOE will control access to devices based upon the identity of users

The TOE restricts access to the devices logically behind it. It mediates access based on user identities that it maintains. . [FDP_ACC.1b, FDP_ACF.1b, FIA_ATD.1].

8.2.1.6 O.TIME

The TOE provides adequate time stamps for audit records.

The TSF shall be able to provide reliable time stamps for its own use [FPT_STM.1.1]. The TSF restricts access to the timestamp to the authorized administrator [FMT_MTD.1c].

8.2.1.7 O.MANAGE

The TOE must provide services that allow effective management of its functions and data.

The TOE must provide the authorized administrators the ability to manage the user accounts of the TOE, authentication data, and the timestamp. [FMT_MTD.1a,b,c] The TOE places restrictions on access to the Administrative module. These restrictions include creating new accounts, modifying security roles, device associations, and authentication data. [FMT_MOF.1, FMT_MSA.1a, FMT_MSA.1b, FMT_MSA.1c, FMT_SMF.1] The TOE ensures restrictive default settings for new user accounts and device associations. [FMT_MSA.3a, FMT_MSA.3a].

8.2.1.8 O.TOE_PROTECTION

The TOE will protect itself and its assets from external access, interference and tampering.

This TOE Security Objective is satisfied by ensuring that: the TOE is required to allow access to protected objects only after it makes informed access decisions (FPT_RVM.1). Additionally, the TOE is required to protect itself and separate the contexts of its users (FPT_SEP.1).

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a low level of risk to the assets. The security environment assumes physical protection and the TOE itself offers only a very limited interface and can only be configured during initialization, offering essentially no opportunity for an attacker to subvert the security policies without physical access. As such, it is believed that EAL3 provides an appropriate level of assurance in the security functions offered by the TOE and that SOF-basic is appropriate for an EAL3 TOE.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. Table 6 Requirement Dependency Rationale lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is proved.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1	YES
FIA_UAU.2	FIA_UID.2	YES (FIA_UID.2)
FIA_UAU.7	FIA_UAU.1	YES (FIA_UAU.2)
FMT_MOF.1	FMT_SMF.1	YES
	FMT_SMR.1	Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	YES (FDP_ACC.1)
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.3	FMT_MSA.1	YES
	FMT_SMR.1	YES
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	YES (FIA_UID.2)
FMT_MTD.1	FMT_SMF.1	YES
	FMT_SMR.1	YES
FPT_RVM.1	None	
FPT_SEP.1	None	
FPT_STM.1	None	

Table 6 Requirement Dependency Rationales

8.5 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements.

8.6 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. . **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	AUDITING	**ACCESS CONTROL**	**IDENTIFICATION AND AUTHENTICATION**	**SECURITY MANAGEMENT**	**SELF PROTECTION**
FAU_GEN.1	X				
FAU_SAR.1	X				
FDP_ACC.1a		X			
FDP_ACC.1b		X			
FDP_ACF.1a		X			
FDP_ACF.1b		X			
FIA_ATD.1			X		
FIA_UAU.2			X		
FIA_UAU.7			X		
FIA_UID.2			X		
FMT_MOF.1				X	
FMT_MSA.1a				X	
FMT_MSA.1b				X	
FMT_MSA.3				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FMT_MTD.1a				X	
FMT_MTD.1b				X	
FMT_MTD.1c				X	
FPT_RVM.1					X
FPT_SEP.1					X
FPT_STM.1					X

Table 7 Security Functions vs. Requirements Mapping

8.7 PP Claims Rationale

See section 7, Protection Profile Claims.

.