AssetCentral Security Target

Common Criteria: EAL1

Version 1.1

14-NOV-11

Document management

Document identification

Document ID	AUV_ST_EAL1
Document title	AssetCentral Security Target
Product version	AssetCentral 4.0.0 consist of: - AssetXplorer (Version 5.0) - AssetCentral Server (Version 4.0)

Document history

Version	Date	Description
0.1	06-AUG-10	Release for internal review.
0.2	09-DEC-10	Addressed EORs
0.3	08-APR-11	Updated to address minor changes for Product Version.
0.4	14-SEP-11	Updated to address minor changes for SFR FTP_ITT.1 (Basic internal TSF data transfer protection)
0.5	14-OCT-11	Updated to address minor changes for the inconsistency in Net framework which is regarding the version
1.0	21-OCT-11	Initial Released
1.1	14-NOV-11	Updated from certifier, refer to section 3.2. Address minor changes to OE.COMMUNICATION, replace SSL with passkey.

Table of Contents

1 Security Target introduction (ASE_INT) 4

1.1 ST and TOE identification 4

1.2 Document organization 4

1.3 TOE Overview 5

1.4 TOE Description 6

2 Conformance Claim (ASE_CCL) 8

3 Security objectives (ASE_OBJ) 9

3.1 Overview 9

3.2 Security objectives for the environment 9

4 Security requirements (ASE_REQ) 11

4.1 Overview 11

4.2 SFR conventions 11

4.3 Security functional requirements 12

4.4 Dependency analysis 20

4.5 TOE security assurance requirements 22

4.6 Assurance measures 23

5 TOE summary specification (ASE_TSS) 25

5.1 Overview 25

5.2 User Data Protection 25

5.3 Identification and Authentication 25

5.4 Security Management 26

5.5 Auditing 26

5.6 Secure Communication 26

6 Glossary 27

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	Authentic Venture AssetCentral Security Target
ST Version	1.1, 14-NOV-11
TOE Reference	AssetCentral 4.0.0 consist of: - AssetXplorer (Version 5.0) - AssetCentral Server (Version 4.0)
TOE Version	Version 4.0.0
Assurance Level	EAL1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009.

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 defines the security objectives for the environment.
- Section 4 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

- Section 5 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE
- Section 6 provides the glossary for the ST.

1.3 TOE Overview

1.3.1 TOE type and usage

The TOE is an automated asset management system. **AssetCentral** automates the protection of managed systems against unauthorized software or hardware installations and removal and having unlicensed software-related vulnerabilities. The TOE allows users to monitor compliance throughout an organization for their IT asset.

AssetCentral is an asset management system and comprises a server component and agents, known as AssetXplorer agents, which are deployed on computers throughout the enterprise. AssetXplorer agents send information about each computer to AssetCentral Server. AssetCentral Server consolidates all the information and allows administrators and custom-role users to view them through a web interface. AssetXplorer is part of the TOE.

1.3.2 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Auditing	The TOE provides auditing capabilities.
Identification and Authentication	The TOE provides identification and authentication of human users of the TOE and identification of AssetXplorer. The TOE also provides identification of AssetXplorer that are installed in managed devices.
Security Management	The TOE provides security management through the use of the Web Administration Interface. Through the enforcement of the AssetCentral Access Control Policy, the ability to manage various security attributes is controlled.
User Data Protection	The TOE provides its own access control between subjects and objects covered by the AssetCentral Access Control SFP.

Security function	Description
Secure Communication	The TOE is able to protect the scanned data from disclosure and modification when the scanned data is sent from AssetXplorer to AssetCentral Server.

1.4 TOE Description

1.4.1 Physical scope of the TOE

The TOE comprises the AssetCentral Server (Version 4.0) with a web Interface. Data is stored in a third party database AssetXplorer agents (Version 5.0) are part of the TOE.

- **AssetCentral Server.** AssetCentral Server is a collection of web components on a web server. All computer inventory retrieved from AssetXplorer Agents is sent to AssetCentral Server and stored in the third party database. The Web Interface ties all these components together to provide a system-wide view of all the computers on your network.

  The Web Interface allows an authorized user to view information about the managed devices assigned to them.

  Through the web based interface, AssetCentral Server includes customizable account creation with modifiable role-based policy capabilities that can be configured by administrators.

- **AssetXplorer Agents.** AssetXplorer Agents are installed on every computer that is to be managed under AssetCentral Server. AssetXplorer scans the local host computer and compiles a full computer inventory (hardware and software). The information is sent from the agent to AssetCentral Server through a secure channel.

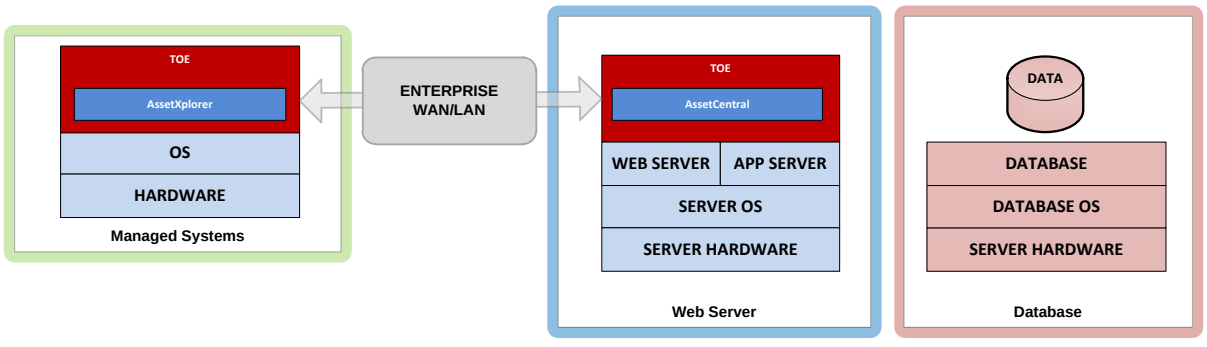

Figure 1 – AssetCentral architecture

The TOE configuration will include the following:

- AssetCentral Server running on a Windows based Server
- AsseExplorer Agent running on windows-based system with .Net Framework installed.

The TOE does not include the third party relational database.

Before the installation of the TOE (AssetCentral), the operating system has to be installed on the web server with the following software:

- Windows 2003 with IIS
- SQL Server 2005
- Microsoft .NET Framework Version 2. 0

1.4.2 Logical scope of the TOE

The TOE provides the following security features:

- **Auditing:** The TOE provides auditing capabilities. Identification and authentication of users, when the scanning of the managed devices is done, when a new managed device is added/deleted are all logged by the TOE.
- **User data protection:** The TOE provides its own access control between subjects and objects covered by the AssetCentral Access Control SFP. Different roles will have different privileges as enforced by the SFP.
- **Identification and Authentication:** The TOE provides identification and authentication of users before allowing any TSF mediated actions
- **Security Managementt:** The TOE provides security management through the use of the Web Interface. Through the enforcement of the AssetCentral Access Control Policy, the ability to manage various security attributes is controlled.
- **Secure Communication:** The TOE provides a secure communication channel between AssetXplorer and AssetCentral Server when scanned data is sent from the AssetXplorer.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3.
- Part 3 conformant, EAL1 Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3. Evaluation is EAL1.

3 Security objectives (ASE_OBJ)

3.1 Overview

The security objectives at an EAL1 level of assurance include concise statements of the objectives to be achieved by the supporting environment.

3.2 Security objectives for the environment

Identifier	Objective statements
OE.TIMESTAMP	The IT environment must provide reliable time stamps.
OE.INSTALL	The TOE shall be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures and only by trustworthy staff. The administrator must ensure that the TOE is delivered, installed, configured, managed and operated in a manner that is consistent with IT security. Beside the software necessary for the management and operation of the TOE (e.g. management tools) no untrusted software shall be installed on the machines the TOE is installed on. The administrator(s) shall ensure – during TOE installation and operation - that the platform the TOE is running on allows the secure operation of the TOE.
OE.PHYSICAL	The administrators shall ensure the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non-shared hardware.
OE.ADMIN	Administrators shall be carefully selected and trained for proper operation of the system.
OE.LOCAL	The operating system of managed systems will provide a suitable access control environment so that the AssetXplorer agents can operate effectively and without being tampered with by local users.
OE.NETWORK	Those responsible for the TOE must ensure that appropriate network layer protection, that there is a firewall in place that only permits access through

	required ports for external users to access the web-server.
OE.PATCH	Those responsible for the TOE must ensure that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.
OE.COMMUNICATION	Those responsible for the TOE must ensure that the communication between AssetXplorer and AssetCentral Server is secured using passkey. The communication channel establishment and passkey generation is using Authentic Venture's proprietary algorithm

4 Security requirements (ASE_REQ)

4.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

4.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.3 Security functional requirements

4.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 4.2 and summarized in the table below.

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTP_ITT.1	Basic internal TSF data transfer protection

4.3.2 FAU_GEN.1 Audit Data Generation

Hierarchical to:	No other components.
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 following auditable events:** • **Identification and authentication of users** • **AssetXplorer deployment on managed devices** • **Scan data**]**.**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: **[no other information].**
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	None.

4.3.3 FAU_GEN.2 User Identity Association

Hierarchical to:	No other components.
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
Notes:	None.

4.3.4 FAU_SAR.1 Audit Review

Hierarchical to:	No other components.

FAU_SAR.1.1	The TSF shall provide [**the AssetCentral administrator and authorized custom user role**] 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.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

4.3.5 FAU_SAR.2 Restricted Audit Review

Hierarchical to:	No other components.
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.
Dependencies:	FAU_SAR.1 Audit review
Notes:	None.

4.3.6 FDP_ACC.1 Subset Access Control

Hierarchical to:	No other components.
FDP_ACC.1b.1	The TSF shall enforce the [**AssetCentral Access Control SFP**] on [**Subjects:** **a) Administrator** **b) Custom roles defined by AssetCentral administrator** **Objects:** **a) scan reports of individual managed devices** **Operations:** **a) Reading scan reports of individual managed devices**]**.**
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	None.

4.3.7 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**AssetCentral Access Control SFP**] to objects based on the following: [**Objects:** **a) scan reports of individual managed devices** **Object attributes:** **a) None** **Subjects:** **a) Administrator** **b) Custom roles defined by AssetCentral administrator** **Subject attribute:** **a) Access rights** **b) Assigned managed device** **c) Assigned groups**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) The administrator may view pages, features, and functions through the Administrator Interface and perform actions associated with administrator rights** **b) If a user logs in and has been assigned a custom user role by the administrator, the user has the access rights, assigned computers, and assigned groups associated with that user role**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**None**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

4.3.8 FIA_ATD.1 User Attribute Definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a) User Identity** **b) Roles (Administrator and Custom (role defined by AssetCentral administrator))** **c) Assigned Access Rights** **d) Assigned Groups** **e) Assigned managed devices**].
Dependencies:	No dependencies.
Notes:	None.

4.3.9 FIA_UAU.2User Authentication before any Action

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.10 FIA_UID.2User Identification before any Action

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies:	No dependencies.
Notes:	None.

4.3.11 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [***determine the behaviour of, disable, enable, and modify the behaviour of***] the functions [**audit (see FAU_GEN.1.1)**] to [**Authorized Administrators**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.12 FMT_MSA.1 Management of Security Attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**AssetCentral Access Control SFP**] to restrict the ability to [***query, modify, delete,*** **create**] the security attributes [**a) Access rights** **b) Assigned managed device** **c) Assigned groups**] to [**Authorized Administrators and Custom (role defined by administrator)**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.13 FMT_MSA.3 Static Attribute Initialization

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**AssetCentral Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the-[**AssetCentral administrator and authorized custom user role**] to specify alternative initial values to override the default values when an object or information is created.

Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	The restrictive values are: • When a computer is added to the system, it is not assigned to any non-default groups. • When a user is added to the system, the user only assumes the chosen user role as customized by the administrator • When a group is created, no policy set or member computers are assigned by default

4.3.14 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) determine the behaviour of, disable, enable, and modify the behavior of the functions audit (FAU_GEN.1.1) (FMT_MOF.1)** **b) query, modify, delete, and create the security attributes (FMT_MSA.1)** **c) mapping user IDs to roles** **d) mapping of user IDs to groups** **e) creation of users with default passwords** **f) deletion of users** **g) changing of passwords**].
Dependencies:	No dependencies.
Notes:	None.

4.3.15 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles **[Administrator and Custom (role defined by AssetCentral administrator)].**
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.16 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from [***disclosure*** **and** ***modification***] when it is transmitted between separate parts of the TOE.
Dependencies:	No dependencies.
Notes:	Communication between AssetXplorer and AssetCentral Server is always initiated by AssetXplorer.

4.4 Dependency analysis

SFR	Dependency	Inclusion
FAU_GEN.1	FPT_STM.1 Reliable time stamps	The TOE relies on the underlying operating system and hardware for the both the server and the managed devices to provide a reliable time stamp for the TOE to capture timestamps with audit records.
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1 Audit review	FAU_SAR.1
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1, FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A

SFR	Dependency	Inclusion
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FDP_ACF.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FPT_ITT.1	No dependencies	N/A

4.5 TOE security assurance requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1).

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behavior.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents. This EAL provides a meaningful increase in assurance over unevaluated IT.

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labelling of the TOE
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

4.6 Assurance measures

Assurance requirement	Assurance measures	Demonstration
ADV_FSP.1 Basic functional specification	Development	The development assurance measure provides all the necessary design documentation to support the analysis of the TOE for an evaluation at EAL1. The functional specification provides a detailed description of the security functions of the TOE.
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will utilise the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.1 Labelling of the TOE	Life cycle support	Configuration management measures provide the assurance that the TOE and supporting evidence can be uniquely identified.
ALC_CMS.1 TOE CM coverage		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL1 can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.1 Security objectives for the operational environment		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.1 Stated security requirements		
ASE_TSS.1 TOE summary specification		
ATE_IND.1 Independent testing - conformance	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
AVA_VAN.1 Vulnerability survey	Vulnerability assessment	The TOE will be made available for vulnerability analysis and penetration testing.

5 TOE summary specification (ASE_TSS)

5.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The TOE security functions include the following:

- User Data Protection
- Identification and Authentication
- Security Management
- Auditing
- Secure Communication

5.2 User Data Protection

The TOE enforces an access control policy on the features, functions and pages to the scan data of the managed devices. After a user identifies and authenticates to the TOE, The TOE will permit a user to access the features, function and pages if the user role and group has permission to perform the requested action on the scan data (**FDP_ACC.1, FDP_ACF.1, FIA_ATD.1**).

There are 2 users maintained by the TOE. They are administrator and custom-role (**FMT_SMR.1**). Each type of user will have different access rights and privileges to features, functions and pages on the scan data of the managed devices.

5.3 Identification and Authentication

The TOE requires that all users (being a administrator or a custom-role user) identify and authenticate themselves before performing any TSF mediated action on behalf of the user (**FIA_UID.2, FIA_UAU.2, FIA_ATD.1**). The TOE checks the credentials presented by the user through the web interface against the authentication information in the database. After a successful identification and authentication, they are assigned a role in the database.

5.4 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1**):

- User management;
- Permission management to scan data;

Administrator and custom- role (given admin function) can modify the access control list, mapping of users to roles, groups as well as modifying the user accounts (**FMT_MSA.1**).

The TOE maintains 2 roles (**FMT_SMR.1**) within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: Administrator and custom roles. Custom roles can be created and the privileges set by the administrator

The TOE allows Administrator and custom- role (given admin function) to change the default values of the TSF data and security attributes of the TOE (**FMT_MSA.3**).

5.5 Auditing

The TOE provides auditing capabilities on the success/failure of the identification and authentication of users, a managed device added/removed to the system and when the scanned data is sent from the AssetXplorer to the TOE. (**FAU_GEN.1**)

The TOE relies on the underlying operation system for reliable time stamps. It is able to associate each event to the user or managed devices. (**FAU_GEN.2**)

The TOE also provides the capabilities for administrators and authorized custom role users to view the audit records on the web interface. (**FAU_SAR.1, FAU_SAR.2**) Only administrators can enable/disable auditing function (**FMT_MOF.1**).

5.6 Secure Communication

The TOE uses encryption to protect scanned data flowing among the TOE components (AssetXplorer and AssetCentral Server) from disclosure (**FPT_ITT.1**).

6 Glossary

Term	Description
AssetCentral Server	The server component of the TOE that provides the central collection capability for the TOE and also provides the administrator with the ability to manage and administer the TOE.
AssetXplorer	The client or agent component of the TOE that collects data on the managed system for transfer back to the AssetCentral Server.
Scan Data	Data collected by AssetXplorer relating to the configuration of the managed device on which the agent is installed.
Scan Report	A human readable output of the scan data presented for the Administrator to view the results and current status of managed devices.
Administrator	The system administrator with privileged system access. This role can control the deployment and operation of the AssetCentral capability within an organisation.
Custom Role	The Administrator can define one or more additional controlling roles with varying levels of privilege and access to the system.
Access Rights	The suite of privileges that can be assigned to custom roles or groups.
Assigned Managed Devices	An administrator or custom role can have any number of managed devices assigned to them for administration.
Group	A grouping of managed devices.
Managed Device	Any device or system that has the AssetXplorer agent installed and operating on it.