Configuresoft
Enterprise Configuration Manager 4.10
Security Target – EAL 3

Release Date:	June 27, 2008
Document ID:	06-955-R-0027
Version:	1.1

Prepared By: InfoGard Laboratories, Inc.

Prepared For: Configuresoft
4390 Arrowswest
Colorado Springs, CO 80907

Table of Contents

DOCUMENT HISTORY 5

1 INTRODUCTION 6

1.1 IDENTIFICATION 6
1.2 CC CONFORMANCE CLAIM 6
1.3 OVERVIEW 6
1.4 ORGANIZATION 7
1.5 DOCUMENT CONVENTIONS 8
1.6 DOCUMENT TERMINOLOGY 8
1.6.1 ST Specific Terminology 8
1.6.2 Acronyms 10
1.7 COMMON CRITERIA PRODUCT TYPE 12

2 TOE DESCRIPTION 13

2.1 OVERVIEW 13
2.2 ARCHITECTURE DESCRIPTION 14
2.2.1 CMDB (Configuration Management Database) 14
2.2.2 Collector 15
2.2.3 Collector Machine Web App 16
2.2.4 Agent 17
2.2.5 Statement of Non-Bypassibility of the TSF 18
2.3 IT ENVIRONMENT CRYPTOGRAPHIC SUPPORT 18
2.4 PHYSICAL BOUNDARIES 20
2.4.1 Hardware Components 20
2.4.2 Software Components 22
2.4.3 Guidance Documents 25
2.5 LOGICAL BOUNDARIES 26
2.5.1 ECM Data Access Control 26
2.5.2 Security Audit 26
2.5.3 Secure Communications 27
2.5.4 Data Consolidation 27
2.5.5 Assessment 28
2.5.6 Remediation 28
2.5.7 TOE Protection 28
2.5.8 Identification & Authentication 29
2.5.9 Security Management 29
2.5.10 Session Termination by the IT Environment 30
2.6 ITEMS EXCLUDED FROM THE TOE 30
2.6.1 Exclusions 30

3 TOE SECURITY ENVIRONMENT 33

3.1 ASSUMPTIONS 33
3.1.1 Personnel Assumptions 33
3.1.2 Physical Environment Assumptions 33
3.1.3 Operational Assumptions 33
3.2 THREATS 33
3.3 ORGANIZATIONAL SECURITY POLICIES 34

4 SECURITY OBJECTIVES 35

4.1 SECURITY OBJECTIVES FOR THE TOE 35
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 35

4.3 MAPPING OF SECURITY ENVIRONMENT TO SECURITY OBJECTIVES 37
4.4 RATIONALE FOR THREAT COVERAGE 39
4.5 RATIONALE FOR ORGANIZATIONAL POLICY COVERAGE 40
4.6 RATIONALE FOR ASSUMPTION COVERAGE 40

5 IT SECURITY REQUIREMENTS 42

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 43
5.1.1 Class FAU: Security Audit 43
5.1.2 Class FIA: Identification and authentication 43
5.1.3 Class FMT: Security management 44
5.1.4 Class FPT: Protection of the TSF 46
5.2 EXPLICITLY STATED TOE SECURITY FUNCTIONAL REQUIREMENTS 46
5.2.1 Class FAU: Security Audit (Explicit) 46
5.2.2 Class FDC: Data Collect functions (Explicit Class) 48
5.2.3 Class FPT: Protection of the TSF (Explicit Class) 51
5.3 IT ENVIRONMENT SECURITY FUNCTIONAL REQUIREMENTS 51
5.3.1 Class FAU: Security Audit 52
5.3.2 Class FCS: Cryptographic Support 52
5.3.3 Class FIA: Identification and authentication 53
5.3.4 Class FPT: Protection of the TSF 53
5.3.5 Class FTA: TOE Access 54
5.4 EXPLICITLY STATED IT SECURITY FUNCTIONAL REQUIREMENTS 54
5.4.1 Class FAU: Security Audit (Explicit) 54
5.5 TOE STRENGTH OF FUNCTION CLAIM 55
5.6 TOE SECURITY ASSURANCE REQUIREMENTS 55
5.6.1 ACM_CAP.3 Authorisation controls 56
5.6.2 ACM_SCP.1 TOE CM coverage 57
5.6.3 ADO_DEL.1 Delivery procedures 57
5.6.4 ADO_IGS.1 Installation, generation, and start-up procedures 58
5.6.5 ADV_FSP.1 Informal functional specification 58
5.6.6 ADV_HLD.2 Security enforcing high-level design 58
5.6.7 ADV_RCR.1 Informal correspondence demonstration 59
5.6.8 AGD_ADM.1 Administrator guidance 60
5.6.9 AGD_USR.1 User guidance 60
5.6.10 ALC_DVS.1 Identification of security measures 61
5.6.11 ATE_COV.2 Analysis of coverage 61
5.6.12 ATE_DPT.1 Testing: high-level design 62
5.6.13 ATE_FUN.1 Functional testing 62
5.6.14 ATE_IND.2 Independent testing - sample 63
5.6.15 AVA_MSU.1 Examination of guidance 63
5.6.16 AVA_SOF.1 Strength of TOE security function evaluation 64
5.6.17 AVA_VLA.1 Developer vulnerability analysis 64
5.7 RATIONALE FOR TOE SECURITY REQUIREMENTS 65
5.7.1 TOE Security Functional Requirements 65
5.7.2 TOE Security Assurance Requirements 68
5.8 RATIONALE FOR IT ENVIRONMENT SECURITY REQUIREMENTS 68
5.9 RATIONALE FOR EXPLICITLY STATED SECURITY REQUIREMENTS 70
5.10 RATIONALE FOR IT SECURITY REQUIREMENT DEPENDENCIES 72
5.11 RATIONALE FOR UNSATISFIED DEPENDENCIES 73
5.12 RATIONALE FOR INTERNAL CONSISTENCY AND MUTUALLY SUPPORTIVE 74
5.13 RATIONALE FOR STRENGTH OF FUNCTION CLAIM 74

6 TOE SUMMARY SPECIFICATION 75

6.1 TOE SECURITY FUNCTIONS 75
6.1.1 ECM Data Access Control 75

6.1.2 Security Audit *76*
6.1.3 Secure Communications *77*
6.1.4 Data Consolidation *79*
6.1.5 Assessment *84*
6.1.6 Remediation *85*
6.1.7 TOE Protection *86*
6.1.8 ID & Authentication *86*
6.1.9 Security Management *87*
6.2 SECURITY ASSURANCE MEASURES 89
6.3 RATIONALE FOR TOE SECURITY FUNCTIONS 90
6.4 APPROPRIATE STRENGTH OF FUNCTION CLAIM 91
6.5 RATIONALE FOR SECURITY ASSURANCE MEASURES 92

7 PROTECTION PROFILE CLAIMS 95

8 RATIONALE 96

8.1 SECURITY OBJECTIVES RATIONALE 96
8.2 SECURITY REQUIREMENTS RATIONALE 96
8.3 TOE SUMMARY SPECIFICATION RATIONALE 96
8.4 PROTECTION PROFILE CLAIMS RATIONALE 96

List of Tables

Table 1: ST Organization and Description 7
Table 2: Console Machine Hardware Component 20
Table 3: Collector Hardware Component 21
Table 4: Windows Agent Hardware Component 21
Table 5: UNIX Agent Hardware Component 21
Table 6: Linux Agent Hardware Component 22
Table 7: Active Directory Server Agent Hardware Component 22
Table 8: Console Machine Software Components 22
Table 9: Collector Software Components 23
Table 10: Windows Agent Software Components 24
Table 11: UNIX Agent Software Components 24
Table 12: Linux Agent Software Components 25
Table 13: Active Directory Server Agent Software Components 25
Table 14: Threats & IT Security Objectives Mappings 39

Table 15: Functional Requirements 43
Table 16: Audited Events 47
Table 17: IT Environment SFRs 52
Table 18: Assurance Requirements: EAL3 56
Table 19: SFR and Security Objectives Mapping 66
Table 20: SFR and Security Objectives Mapping 69
Table 21: Explicitly Stated SFR Rationale 71
Table 22: SFR Dependencies 73
Table 23: Rationale for unsatisfied dependencies 73
Table 24: Collected data types (default) for Windows based Clients 82
Table 25: Collected data types (default) for UNIX/Linux based Clients 83
Table 26: Collected data types (default) for Active Directory based Clients 84
Table 27: Assurance Requirements: EAL3 90
Table 28: TOE Security Function to SFR Mapping 91
Table 29: Rationale for Security Assurance Measures 94

List of Figures

Figure 1: ECM Collection Concept 13
Figure 2: TOE Architecture 14
Figure 3: TOE Physical Boundaries 20

Document History

Document Version	Date	Author	Comments
1.0	04/28/08	M. McAlister	Final Release
1.1	6/27/08	M. McAlister	Updated based on FVOR verdicts

1 Introduction

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

1.1 Identification

TOE Identification:	Configuresoft Enterprise Configuration Manager 4.10 for Windows, UNIX and Active Directory
ST Identification:	Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3
ST Version:	1.1
ST Publish Date:	June 27, 2008
ST Authors:	Mike McAlister (InfoGard)
PP Identification:	N/A

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.2[1] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.2 Part 3 conformant at EAL3

The TOE is also compliant with International interpretations with effective dates on or before 6/12/06.

This TOE is not conformant to any Protection Profiles (PPs).

1.3 Overview

The Configuresoft Enterprise Configuration Manager (ECM) is a network software product that allows administrators to manage configuration control over Enterprise network resources. ECM offers a scalable, cross platform solution to help customers effectively manage and control the configuration of Network resources from a centralized Administrator workstation.

ECM collects security and configuration data settings across the IT enterprise through an Agent software component. Agents are available for multiple Operating Systems including Windows, UNIX, Linux, and Active Directory Servers. The agent is in the form of a quiescent executable which wakes up when it receives a call for a desired collection or change. The data and configuration settings are collected from the targeted machines which ECM stores in a

[1] Common Criteria (CC) for Information Technology Security Evaluation – January 2004, Version 2.2.

comprehensive Configuration Management Database (CMDB). Data transfer is secured through the Microsoft cryptographic API installed on the Collector and on Window's based agent machines that supports secure session establishment. UNIX sessions are secured through an OpenSSL object module. By leveraging the information stored in the CMDB, IT administrators can assure that the policies they develop are in effect and institute actions through ECM to support IT infrastructure policies.

In the event an Agent is not available, due to a disconnected IT resource, the Agent machine is marked within ECM as "Failed" and logs the event. The "Failed" status applies to a given Collection attempt. When a new Collection request is initiated, connection attempts resume and upon successful connection, the status of the "Failed" machine is then reported as "Succeeded".

Configuresoft ECM's CMDB based approach allows IT administrators to run enterprise compliance reports and policies against the centralized CMDB, not each remote machine across the network. Traditional issues such as data gaps due to un-powered and disconnected machines and impacts to client performance are eliminated using this CMDB based approach. ECM combines the power of distributed computing with minimal resource consumption. This low impact approach provides secure data collection, remediation and continuous compliance monitoring capabilities.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1: ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***additions indicated with bold text and italics***

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

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

The explicitly stated requirements claimed in this ST are denoted by the ".EXP" extension in the unique short name for the explicit security requirement.

1.6 Document Terminology

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

1.6.1 ST Specific Terminology

Administrative Users

Refers to users of the Configuresoft ECM (TOE) application holding one of the following roles: Configuresoft ECM administrator, ECM read-only, Windows ECM administrator, Active Directory ECM administrator, UNIX ECM Administrator, (includes Linux agent machines).

Agent

The software installed on monitored Machines that accepts requests from the Collector and coordinates interactions with system APIs to collect data and implement actions.

AIX

IBM's UNIX implementation

Alert

A message issued by the Collector to notify the Administrator when a Rule has been matched indicating a potential TSF violation.

Collector

The software that coordinates collection activities installed on a central server. The Collector includes the Configuration Management Database.

Collection

The process used by the Collector to acquire configuration data from Machines within the network environment.

Compliance

A collector process that compares a Machines collected configuration information with: Accepted IT Industry Best Practices, Governmental Standards (Regulatory Guidelines) or established enterprise standards.

Console

The browser hosted TOE user interface.

Configuration Management Database

A centrally located database within the Collector Machine that is used to store detailed configuration information from Machines.

Dashboard

A summary presentation of configuration data collected from Machines.

Data Grid

A column based GUI to view collected data presented from the CMDB.

Discovery

The scanning process by which the Collector searches the Network for available Machines or alternatively a list of network machines is uploaded to the application. This is a prerequisite to Collection.

ECM Users

ECM Users within this ST refers to any user of the ECM Application in any role, by definition these users are Administrators as the application is not intended for non-administrative users.

Enterprise Configuration Manager

The descriptive name of the TOE application.

inetd This is a super-server daemon on many Unix systems that manages Internet services.

Machine

Any Enterprise Network Resource such as a computer workstation or server that is identified in the discovery processes from which configuration information is to be collected (managed). Installation of an Agent is required.

Machine Group

Machine Groups are used to organize the machines into logical groups. This includes static groups where the members are selected by hand, or dynamic groups where filters determine membership. For the CC Evaluated Configuration Machine Group may not be edited.

Network Authority Accounts

Refers to an ECM account, created and managed on the Collector machine, which has domain administrator rights to Agent machines in the network. Once these accounts have been added, they are assigned by Domains and/or machine groups to allow the Collector to access Agent machines for Data Consolidation and/or Remediation as applicable.

Role

An ECM defined set of access rules that can be allocated to a user. The individual access rules determine what functions a user can perform within ECM.

Security Identifier

"Within the context of Windows Operating Systems, a Security Identifier is a unique alphanumeric character string assigned by a Windows Domain controller during the log on process that is used to identify an object, such as a user or a group of users in a network of NT/2000 systems."

Users

Within this ST, this term refers in a general sense to users of the Configuresoft ECM application. These users hold one or more of the following roles within the TOE: Configuresoft ECM Administrator, ECM Read-Only, Windows ECM Administrator, Active Directory ECM Administrator, Unix ECM Administrator (Linux included in UNIX administrator role). These users must also be valid users of the underlying Collector Machine Operating System.

1.6.2 Acronyms

CC Common Criteria

CMDB	Configuration Management Database
DCOM	Distributed Component Object Model
DSSBASE	Microsoft Base Diffie-Hellman cryptographic module (FIPS 140-1 cert #103)
DSSENH	Microsoft Enhanced Diffie-Hellman cryptographic module (FIPS 140-2 cert #381)
ECM	Enterprise Configuration Manager
FIPS	Federal Information Processing Standard
HTTP	Hyper Text Transfer Protocol
HTTPs	HTTP over SSL
HP	Hewlett Packard
IBM	International Business Machines
IIS	Microsoft Internet Information Services (Windows Web Server feature)
IP	Internet Protocol
OpenSSL	OpenSSL FIPS Object Module
RSABASE	Windows Base Cryptographic Module
RSAENH	Windows Enhanced Cryptographic Module
SFP	Security Function Policy
SID	Security Identifier (Windows authentication reference)
SOF	Strength of Function
SQL	Structured Query Language
SUM	Security Update Manager
SSL	Secure Sockets Layer
TLS	Transport Level Security (SSL v3.1)
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSC	TOE Scope of Control

1.7 Common Criteria Product type

The TOE is a **Network Management** software product that manages configuration information for network resources, provides security auditing, compliance assessment, and facilitates configuration control for network resources.

2 TOE Description

2.1 Overview

The Configuresoft Enterprise Configuration Manager provides a scalable, cross platform software solution to help customers effectively manage and control IT network enterprises.

For Common Criteria classification purposes, the Configuresoft ECM is classified as a Network Management Software product.

ECM collects asset, security and configuration data settings from IT resources with ECM Agent component installed, across the IT enterprise and stores them in a comprehensive Configuration Management Database (CMDB). Through the acquisition and storage of this configuration data in the database, administrators can evaluate the configuration status of resources throughout the network and apply configuration changes to specific IT resources in the network, without requiring real-time network access to workstations. Evaluations are executed against the CMDB database as a proxy of the actual Agent machine and changes can be manually made against this data and are then pushed out to IT resources by the ECM application.

The Common Criteria ECM release features a modified GUI, which presents the feature set and options supported by the Common Criteria Evaluated configuration.

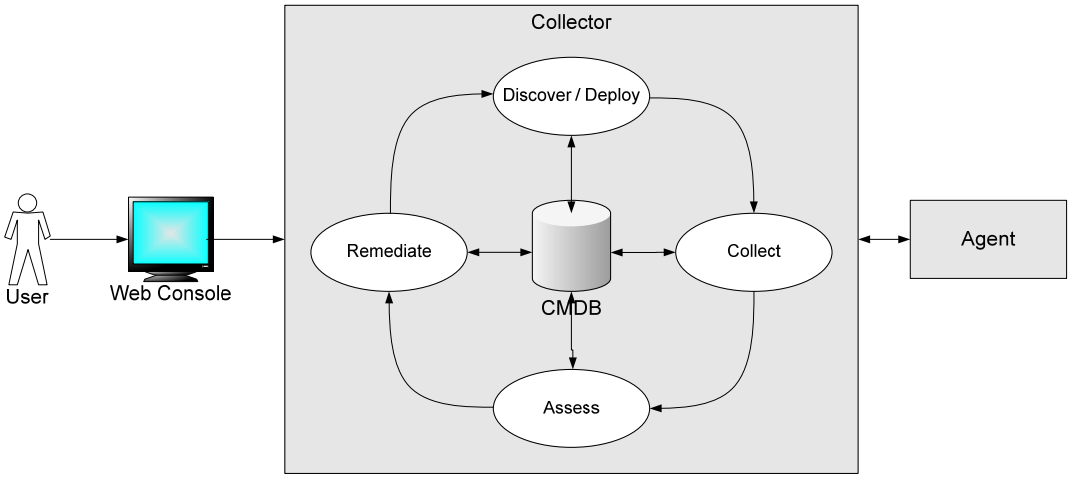

Figure 1: ECM Collection Concept

2.2 Architecture Description

The follow section describes the TOE software architecture through a series of subsystems.

The TOE architecture is divided into 4 subsystems:

- Configuration Management Database (CMDB)
- Collector
- Collector Machine Web App
- Agent

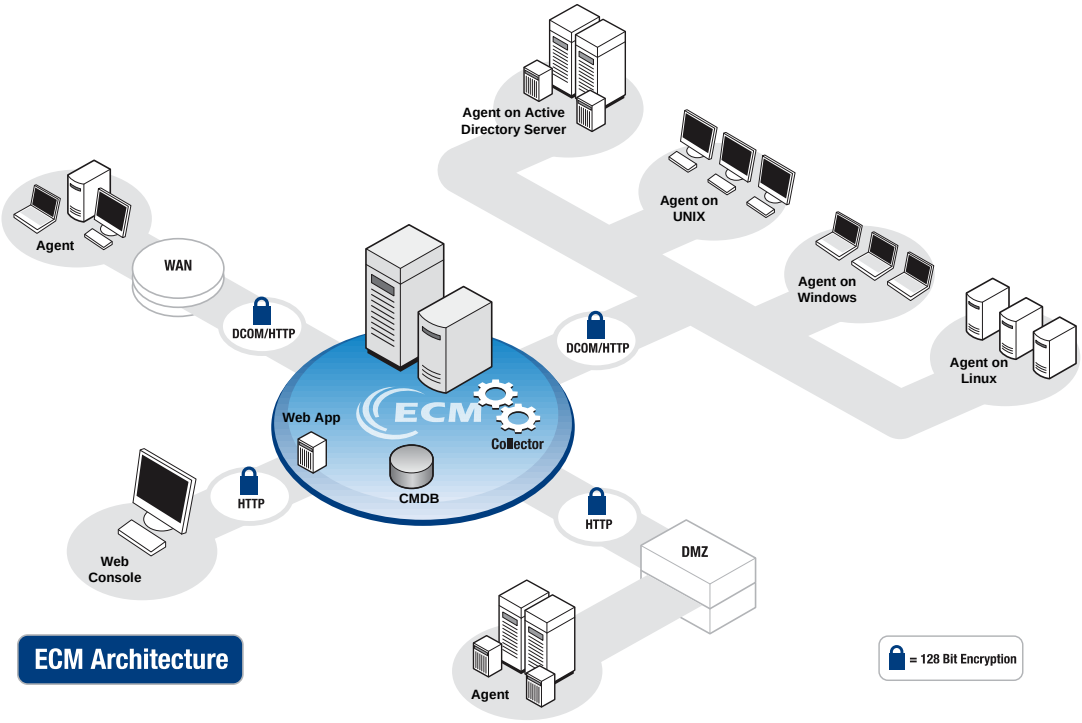

Figure 2: TOE Architecture

2.2.1 CMDB (Configuration Management Database)

The CMDB is a series of custom databases hosted by Microsoft SQL server. The CMDB maintains the list of Machines and data used by ECM for configuration management and reporting activities within the network. The Discovery process first populates the CMDB by identifying machines within the network that may be included for data collection. The Common Criteria Evaluated Configuration supports the File Upload method of importing Discovery data into the TOE. Through the File Upload Filter, important files can be imported from selected machine agents within the network and imported into the CMDB by selected file type during the ECM Collection process. Based on machine group and Collection selections made by the

Configuresoft ECM Administrator, ECM collects detailed data from the Agent Machines.

By storing configuration information in the CMDB ECM users may assess the data locally without affecting the network or the machines and then implement changes or policies during ad-hoc or scheduled ECM sessions.

The CMDB database subsystem includes the schema, stored procedures and support modules that accept collected data, support queries and reports, and handle appropriate actions across monitored systems within the enterprise.

Windows Authentication is used when connecting to the CMDB (SQL server). The User logs onto the OS and the SQL server uses the established token for its sign-on process. Both the Web App and the Collector service connect to the CMDB and make this connection using their own user credentials. For example, the Web App will connect to the CMDB as the User that ran the Web App to execute the command.

2.2.2 Collector

The Collector subsystem identifies the Agent Machines through uploading a Discovery list of machines that are available for Collection and then, upon Administrator request, gathers information through the Collection process from the Agent Machines. This data is imported into the CMDB following Collection, to allow for network security auditing, compliance assessment, configuration control and remediation management. Access to the ECM application is not performed directly through the Collector machine, Administrators access ECM using a browser through the Web Console machine in the IT Environment. When initiating a session, the Administrative user is presented with a login screen to enter the applicable username and password credentials. These credentials are passed to the Collector machine from the Web Console over an SSL/TLS secured session. The Web App subsystem passes the username/password data to the underlying Operating System (OS) for validation. The Operating System verifies that the credentials reflect a valid Collector machine OS account, accesses the associated token and verifies, through the token Security Identifier (SID) that the user also holds a valid ECM Administrative User account. The User is then logged into ECM under the role associated with the access credentials used during login. This is further described below under Section 2.2.3 Collector Machine Web App.

The Collector subsystem component also includes a Windows Agent as part of its installation package that allows the Collector to execute collection activities against its installed platform. The composition of this Agent is as described in Section 2.2.4 below.

The Collector Service executes jobs that dispatch requests to agents, retrieve the results and insert the results in the CMDB. The request contains three primary types of information. The first type is a description of the work, called Jobs. The second type is a list of the machines to do the work on. The third type is the configuration information that describes specifically how to do the work on the machines. The Collector Service is controlled via the Windows Service Control Manager.

The ECM Collector application runs as a service. The Collector is a stand-alone application that can run even when no other ECM components are active. The executable is structured into a

Request Processing component, which processes Agent and CMDB bound jobs, and generates audit events based on Collector service activities; an Agent Communication component that executes the instructions submitted form the request processing component into specific actions such as submittal of requests, status verifications, transfer results and data exchange acknowledgement. A Database Communications component of the Collector Service executable, executes operations against the CMDB to pre-process collected data and perform transform operations on collected data.

2.2.3 Collector Machine Web App

The Web App subsystem is installed in the Collector Machine and accepts browser-based connections from the Web Console Machine. To access ECM from the Web Console Machine the User navigates to the applicable URL where ECM is hosted on the Collector Machine, the user enters Username and Password credentials that are passed to the Collector machine Operating System for validation. Authentication to the ECM application is a two stage process: First, the Windows Operating System verifies that the entered credentials belong to an authorized account and creates a token. The token is a data structure, created for the user that contains the User's Security Identifier (SID) and list of privileges held by that user. The SID is a unique alphanumeric character string assigned by a Windows domain controller during logon. The token is applied to every process and thread within each process that the particular user starts up.

Following this initial OS validation step, the Web App accesses the token held within the OS in protected address space, and compares the SID information to the authorized SIDs in the ECM CMDB (database). This validation step assures the User represented by the token SID has a valid ECM role and then establishes the ECM session using those attributes under the appropriate role.

User commands to the Collector and Database subsystems are executed from the GUI and provide the essential web server support for the ECM Collector to execute. The Web App provides access to ECM through HTTPs using a standard Microsoft® Internet Explorer browser based interface. The Web Console Machine browser based interface represents the Administrator interface to the ECM Collector. All administrator functions are accessed through this interface based on Administrator Roles within ECM. The Configuresoft ECM TOE supports the following roles: ECM Administrator, ECM Read-only, Active Directory ECM Administrator, Windows ECM Administrator, UNIX ECM Administrator (includes Linux),.

The Web App provides two basic functions:

1. Access to and presentation of all data collected from monitored Machines.
   The Web App provides administrators with tools such as the Data Grid and customized Dashboards, to review and evaluate information collected from the monitored Machines.
2. The Web App provides the interface that allows users to perform the following security functions:

- Manage User Access: The Administrator can control who has access and what areas they have access to via the TOE assigned user Role.
- Review Audit logs
- Evaluation of Collected Data
- Remediation/update of Agent Machine data based on evaluation

The Web App is a server side IIS application that generates Web Console content via interactions with the CMDB and IIS. The Web Console is a term used to connote the Internet Explorer side rendering of all ECM content. The ECM Portal is the main Active Server Page (ASP) page or GUI used to interact with the ECM product. ASP is the server side code that sends HTML back to the client with Java-script embedded in it. ASP does not generate the Java-script code. Configuresoft developers write the Java-script. Java-script runs only on the web console client and not on the Collector machine.

2.2.4 Agent

The Configuresoft ECM Administrator or local Agent machine administrator installs Agent software manually on network resources that are selected as candidates for Collection during deployment. Once installed, the Collector can contact the Agent, establish a secure connection, initiate a Collection session and institute Remediation activities on Agent machines. The Agent in operation is quiescent until an appropriate request is received from the Collector to execute a Collection or Remediation. The Agent also includes a mechanism to restrict collections to the delta or differences since the last collection. Both mechanisms ensure that there is minimal impact to the monitored Agent Machine and network.

The Collector subsystem also includes a Windows Agent as part of the installation package. This allows the Collector to execute Collection against it own platform (Collector Machine).

The Agent is an executable set of code installed on agent machines included in the file list (and thereby eligible for collection). The Agent provides the primary vehicle to execute instructions for configuration verification or collection activities on installed machines. The Agent executable includes constructs which contains the code set utilized to access the selected data types for the particular Operating System type of the Agent Machine (Windows, Active Directory, UNIX or Linux).

The Microsoft Windows based agent consists of the following:

- Windows Agent Software Component: Standard agent for Windows based systems

The UNIX based Agent consists of the following:

- UNIX Agent Software Component: Standard agent for UNIX based systems.

The Linux based Agent consists of the following:

- Linux Agent Software Component: Standard agent for Linux based systems.

The Active Directory based Agent consists of the following:

- The Active Directory Agent Software Component: Standard agent for Active Directory Server based systems.

2.2.5 Statement of Non-Bypassibility of the TSF

TOE security functions cannot be bypassed. All access to ECM security functions requires Administrator level access and no direct interface is available to underlying subsystems (CMDB, Agents, Collector, Web App) without going through the GUI interfaces accessible only through the Web Console machine (CC configuration requirement). The ECM Collector identification process verifies that Administrator users are successfully identified and authenticated by the Collector IT Environment and subsequently identified with a valid ECM Administrator Role within the TSF prior to allowing any access to TSF settings.

The only Human Accessible interface provided is through the Web Console machine in the IT Environment using a browser. The Collector machine and Agents deployed within the network do not provide alternate interfaces into the TOE.

Agents reside on the applicable workstations/servers in the network environment but do not contain an interface for direct access to the Agent software (the Agent and its operation is transparent on installed machines). The Agents are only capable of transmitting configuration status to the Collector, when requested by the Collector. The Agent cannot initiate any communication and can only respond to requests for communication from the Collector by design. The underlying Agent machine Operating System provides protection to installed ECM code on the platform through access control mechanisms.

2.3 IT Environment Cryptographic support

Cryptographic functionality provided by the IT Environment invoked by the TOE:

DSSBASE and DSSENH are the default cryptographic modules provided by Microsoft®, RSAEHN and RSABASE are modules that implement the Microsoft® enhanced cryptographic service.

Microsoft® Cryptographic Modules:

ECM Console machine – RSAENH, DSSENH

The ECM Console machine running Microsoft® Internet Explorer utilizes Microsoft® cryptographic modules to secure connections to the Collector Machine using SSL/TLS. These modules are part of the SChannel security package provided by Microsoft®. These ECM Console sessions are used by authorized ECM Administrative users to access the ECM application security management interface. These sessions may use the AES algorithm with a 128 bit key size or two key 3DES. Cryptographic hash functions for these sessions utilize either

HMAC-MD5 or HMAC–SHA1. Session keys are established between the parties using RSA key exchange. The usage of these modules is in the non-FIPS mode.

The SSL/TLS cipher suites for the above are:

TLS_RSA_WITH_3DES_EDE*_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

*The 'EDE' in the 3DES string indicates the '2-key' mode.

As with collector-agent communication, ECM web console-web application (webapp) subsystem communication via SSL/TLS involves a cipher negotiation between the console and webapp.

The strongest cipher supported by both will be chosen. This is a configuration setting on each side.

Microsoft® Cryptographic Modules:

ECM Collector Machine– RSAENH, DSSENH

The ECM Collector machine utilizing these modules for cryptographic key generation, key exchange and session in the same manner as described for the ECM Console machine above.

NOTE: RSAENH, DSSENH are part of the underlying Microsoft Operating System in the IT Environment and are shown here to illustrate where cryptographic functions are accessed by the TOE. FIPS validated modules included in this listing may be assumed to be operating in non-FIPS modes.

OpenSSL Cryptographic Module:

The OpenSSL module is used by the ECM application, UNIX or Linux Agent Component for the purpose of establishing secure sessions (HTTP over SSL/TLS) with the Collector machine.

OpenSSL – used for session encryption over TLS – provides AES (128), 3DES (112), SHA1, MD5, key generation (RNG), RSA based key exchange via TLS

The specific OpenSSL module used by ECM is as follows:

OpenSSL FIPS Object Module (Source Content Version: OpenSSLfips1.0.tar.gz; Resultant Compiled Software Version: 1.0) (FIPS 140-2 #642)

The FIPS certificate for this module can be found here:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2006.htm

This module is FIPS validated, however, it is used by ECM in non-FIPS mode.

2.4 Physical Boundaries

This section lists the hardware and software components of the product and denotes which are in the TOE and which are in the IT Environment.

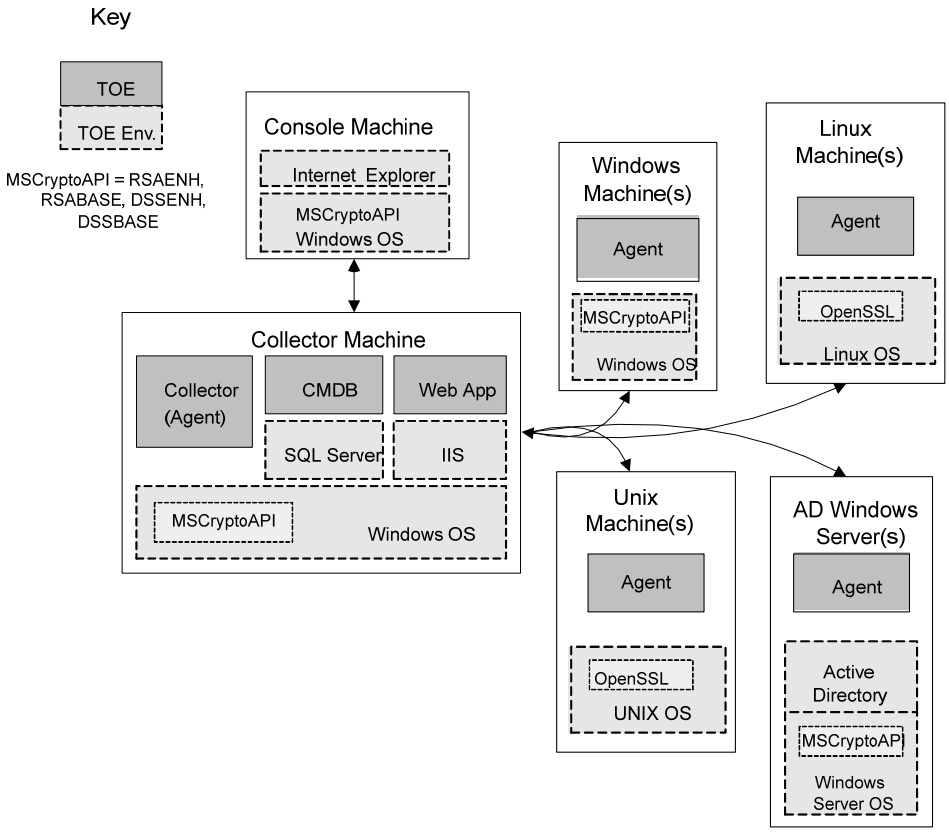

Figure 3: TOE Physical Boundaries

* MSCryptoAPI indicated in the above diagram refers to RSAENH, DSSENH for Windows & Active Directory

2.4.1 Hardware Components

These tables identify hardware components required by the TOE which are part of the IT Environment (ENV).

Console Machine

TOE or Env	Component Name	Description of Component
Environment	Console Workstation	General purpose computer capable of supporting Microsoft® Windows XP SP2 and Microsoft® Internet Explorer 6.0 or higher

Table 2: Console Machine Hardware Component

Collector Machine

TOE or Env	Component Name	Description of Component
Environment	Collector Server	General purpose computer capable of supporting Microsoft® Windows Server 2003 SP2

Table 3: Collector Hardware Component

Windows Agent

TOE or Env	Component Name	Description of Component
Environment	Windows Agent Workstation or Server	General purpose computer capable of supporting Microsoft® Windows Server 2003 SP2, Microsoft Windows XP professional SP2

Table 4: Windows Agent Hardware Component

UNIX Agent

TOE or Env	Component Name	Description of Component
Environment	UNIX Workstation or Server (AIX)	Any Hardware capable of supporting AIX UNIX Operating System
Environment	UNIX Workstation or Server (HP)	Any Hardware capable of supporting HP UNIX Operating System
Environment	UNIX Workstation or Server (Sparc)	Solaris 10 (SunOS 5.10) – Sparc platform only

Table 5: UNIX Agent Hardware Component

Linux Agent

TOE or Env	Component Name	Description of Component
Environment	Linux Workstation or Server	General purpose computer capable of supporting RedHat 4.0 Enterprise Server – x86 platform only , Novell SUSE v 10 Enterprise

		Linux Server

Table 6: Linux Agent Hardware Component

Active Directory Server Agent

TOE or Env	Component Name	Description of Component
Environment	Active Directory Server	General purpose computer capable of supporting Microsoft® Windows Server 2003 SP2

Table 7: Active Directory Server Agent Hardware Component

2.4.2 Software Components

These tables identify software components by applicable subsystem and indicate whether or not each component is in the TOE or IT Environment (ENV).

Console Machine

TOE or Env	Component Name	Description of Component
Environment	Internet Explorer	Microsoft® Internet Explorer 6.0 or higher
Environment	Microsoft Windows OS	Microsoft XP professional SP2
Environment	Microsoft Enhanced RSA Cryptographic Module (Cert #238) RSAENH Microsoft Enhanced Diffie-Hellman cryptographic module (Cert #240) DSSENH	Provides cryptographic services for securing console sessions. (operating non-FIPS)

Table 8: Console Machine Software Components

Collector Machine

TOE or Env	Component Name	Description of Component
TOE	Enterprise Configuration Manager Revision 4.10	TOE Software package incl. Windows Agent
Environment	SQL Server	SQL Server 2000 with SP3a

		with Hotfix 904 or SP4
Environment	IIS	Microsoft Internet Information Services(IIS) 6.0
Environment	Windows OS	Microsoft Windows Server 2003 SP2
Environment	Microsoft Enhanced RSA Cryptographic Module (Cert. #868) RSAENH Microsoft Enhanced Diffie-Hellman cryptographic module (Cert #875) DSSENH	Provides cryptographic services (operating non-FIPS)

Table 9: Collector Software Components

Windows Agent

TOE or Env	Component Name	Description of Component
TOE	Enterprise Configuration Manager Revision 4.10: Windows Agent	TOE Agent Software
Environment	Windows OS	Microsoft Windows 2000 Professional, Server, Advanced Server, or Datacenter Edition (or) Windows XP Professional SP2 (or) Windows Server 2003 Standard, Web, Enterprise, or Datacenter Edition SP2
Environment	Microsoft Enhanced RSA Cryptographic Module (FIPS Cert #238) RSAENH (XP), Cert#868 (2003), Cert#382 (2000) Microsoft base Diffie-Hellman cryptographic module (FIPS #240) DSSENH Cert#103 (2000) (selections	Provides cryptographic services for securing Windows based Agent sessions. (operating non-FIPS)

	are OS dependant)	

Table 10: Windows Agent Software Components

UNIX Agent

TOE or Env	Component Name	Description of Component
TOE	Enterprise Configuration Manager Revision 4.10: (UNIX ECM Agent)	TOE Software
Environment	UNIX based OS	Solaris 10 (SunOS 5.10) – Sparc platform only (or) HP-UX 11i v 2 – PA-RISC platform (or) AIX 5L v 5.3 – RS6000 platform only requires Maintenance Level 3
Environment	OpenSSL FIPS Object Module (Source Content Version: OpenSSLfips1.0.tar.gz; Resultant Compiled Software Version: 1.0) (FIPS 140-2 #642)	Provides cryptographic services for the UNIX Agent (operating non-FIPS mode)

Table 11: UNIX Agent Software Components

Linux Agent

TOE or Env	Component Name	Description of Component
TOE	Enterprise Configuration Manager Revision 4.10: (Linux ECM Agent)	TOE Software
Environment	Linux OS	RedHat 4.0 Enterprise Server – x86 platform only (or)

		Novell SUSE v 10 Enterprise Linux Server
Environment	OpenSSL FIPS Object Module (Source Content Version: OpenSSLfips1.0.tar.gz; Resultant Compiled Software Version: 1.0) (FIPS 140-2 #642)	Provides cryptographic services for the Linux Agent (operating non-FIPS mode)

Table 12: Linux Agent Software Components

Active Directory Server Agent

TOE or Env	Component Name	Description of Component
TOE	Enterprise Configuration Manager Revision 4.10: (ECM AD Agent)	TOE Software
Environment	2003 Microsoft Windows Server Operating System SP2	OS platform including Active Directory
Environment	Microsoft Enhanced RSA Cryptographic Module (FIPS Cert #868) RSAENH Microsoft base Diffie-Hellman cryptographic module (FIPS 140-1 #103) DSSENH	Provides cryptographic services for securing Windows Active Directory based Agent sessions. (operating non-FIPS)

Table 13: Active Directory Server Agent Software Components

2.4.3 Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with EAL 3 requirements:

- AGD_ADM - Administrator Guidance –
  - Enterprise Configuration Manager 4.10 Installation and Getting Started Guide
  - Configuresoft© Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3 06-955-R-0088
- ADO_IGS – Installation Guidance –

- Enterprise Configuration Manager 4.10 Installation and Getting Started Guide
- Enterprise Configuration Manager 4.9.0 Hardware and Software Requirements Guide
- Configuresoft© Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3 06-955-R-0088

All documentation delivered with the product is germane to and within the scope of the TOE.

2.5 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

2.5.1 ECM Data Access Control

The ECM Data Access Control security function provides role based access to data collected from Agent Machines and maintained in the CMDB. It includes restrictions on accessing and viewing the Collected Data as well as role based restrictions, on which subsets of data can be analyzed through the Assessment Security Function (See Section 2.5.5) based on ECM Role. This functionality is provided primarily through the CMDB in conjunction with the Collector for access control support.

ECM implements Roles by requiring the user to log into ECM using a browser on the Web Console machine. The TOE passes the credentials to the Collector machine Operating system for validation and subsequently verifies that the user holds a valid OS account on the Collector Machine. Then the User credentials are looked up within the ECM application to determine if the User holds a valid role. The ECM application allows the Configuresoft ECM Administrator to assign users to a selection of Roles based on that account. For example, in order for a User to access collected data for Windows machine they must hold the role of Windows ECM Administrator or Configuresoft ECM Administrator.

The Common Criteria Evaluated configuration includes the following pre-configured roles: Configuresoft ECM Administrator, ECM Read-Only, Windows ECM Administrator, UNIX ECM Administrator (include Linux), and Active Directory ECM Administrator roles.

2.5.2 Security Audit

The Configuresoft ECM TOE generates audit events within the Collector machine to log TSF events by creating Windows Operating System events. These logged events include the time of the event, success or failure of the event and the User Identification associated with the event. The ECM Collector performs a collection against the ECM Collector machine to acquire the ECM related event log entries and import that data into the CMDB as collected data. These collections are performed based on Administrator preference and ECM configuration.

Audits are generated for login success/failures as well as for application configuration actions, CMDB data consolidation, analysis and remediation actions and security management activities

initiated through the ECM Web Console.

The Collector subsystem provides the Security Audit functionality for Security Audit activities for the ECM TSF activities executed through the Collector.

Agent Machine ECM related actions trigger security-related audit events using the OS-specific Security Logging system (Windows Event log etc). ECM collects the audit events as part of regular data collection routines as established by the applicable ECM Administrative user. This audit data is collected (via the Data Consolidation security function) and stored within the CMDB as TSF data. The Agent subsystem supports the Security Audit security function for Agent Machines. The TOE provides for the viewing of audit records following Collection via the CMDB database in the same manner as other collected data types are viewed. Accessing data in the CMDB database is described in the Assessment security function.

2.5.3 Secure Communications

The ECM TOE secures the communication from the Web Console machine to the Collector's Web App subsystem using the HTTPs protocol and leveraging the Microsoft Cryptographic module in the IT Environment. This assures that Administrator sessions with the ECM application are secured via SSL/TLS utilizing symmetric key cryptography.

Data transfers (i.e.: during the Collection process) between the Agent Machines and the Collector Machine are secured using one of two available methods. For Windows and Active Directory based Agent Machines, DCOM may be used and when used implements the highest possible security setting of Packet Privacy (PKT_PRIVACY) in conjunction with Microsoft cryptographic module support provided in the IT Environment. Alternatively, TLS record protocol over an HTTP transport may be used to secure these data transfers; also utilizing the Microsoft cryptographic module provided in the IT Environment. The Secure Communications security function is supported by the Collector subsystem working with the applicable Agent software.

UNIX/Linux Agent Machines utilize TLS record protocol over an HTTP for securing data transfers to the Collector Machine utilizing an OpenSSL object module in the IT Environment.

Cryptographic support for this security function as noted above is provided in the IT Environment.

2.5.4 Data Consolidation

Through the Data Consolidation Security Function, the TOE utilizes filters to selectively collect data elements from: Windows, UNIX, Linux and Active Directory Agent Machines. The data may then be directly stored in the CMDB or, alternatively if a "Delta" Collection is selected, it compares the newly collected results to a baseline data set stored on the Agent Machine, so that it transmits only the delta information over the network to the Collector and allows the Collector to then store the delta in the CMDB. This minimizes the network traffic and the data insert time into the CMDB. This security function is supported by the Collector subsystem in conjunction with the applicable Agent. Data storage support is provided by the CMDB subsystem.

2.5.5 Assessment

The Assessment Security function provides analysis capabilities through the TSF to evaluate data collected and compare it to compliance matrices. Operational, security and regulatory Compliance templates are available for selection to assess CMDB data and inform administrators of aspects of configuration which are not in compliance with selected criteria.

The Assessment Security function also provides configurable options that use the extensive data stored in the CMDB to display Dashboards and Reports. This functionality allows the user to drill down collected data results from Enterprise to machine-level detail directly from an ECM table or chart.

This security function also allows the user to track changes to configuration information over time based on data collected and a listing maintained within the Agent that is consulted to determine which data has changed since the last collection. The data management aspect of the Assessment Security Function is provided by the Collector subsystem.

The Data Grid provides the primary direct access to the underlying collected information by presenting the data in a columnar format. Options available to the user are indicated by dynamic links, menus and icons that are enabled or disabled based on the role of the user logged into the ECM Web Console. The Graphic User Interfaces and display options are supported by the Web App subsystem.

2.5.6 Remediation

The Remediation Security Function provides the ability for the TSF to initiate changes to the specific Windows configuration through the ECM Web Console:

- Change Agent machine Passwords
- Start/Stop Services (applies to Agent Services configured in the Automatic or Manual Startup mode)
- Apply a registry change (i.e.: change a registry key value)

This may be based on compliance analysis or evaluation of CMDB data and review of Assessment reports. In the Common Criteria certified configuration: remediation does not apply to UNIX and Linux based Agent Machines or any other Windows or Active Directory data other than those specified.

2.5.7 TOE Protection

The Collector requires physical and logical protection to assure that TOE related security functions are not bypassed or altered. The Operating System Environment (TOE Environment), secure communications and access control methods described earlier provide this protection.

The only Human User interface available for login is the browser based GUI session between the Web Console machine and the ECM Web App Subsystem on the Collector machine. Valid credentials must be entered through this interface in order to access the TSF.

Agents installed on machines within the network do not provide any local interfaces allowing access. All communication with the Agent must occur by the Collector subsystem during Collection and Remediation activities. The agent cannot initiate sessions with the Collector or initiate communications within a session and may only respond to specified requests from the Collector.

The Collector and Web App subsystems within the Collector machine support the TOE Protection security function.

2.5.8 Identification & Authentication

The TOE requires that all users are successfully identified and authenticated prior to gaining access to TSF resources. All authorized ECM users are Administrators holding a specific ECM administrator role. Therefore, all references to authorized users within this security target refer to ECM administrators.

Administrative Users access the TOE using a browser on the Web Console machine through an SSL/TLS secured session. The Web App subsystem of the Collector machine passes login credentials to the Collector machine Operating System for validation as described in Section 2.2.3. Following validation of credentials by the underlying Operating System, the ECM application accesses the token and compares the User SID against the SIDs stored in the ECM authorized users list. If the SID matches an ECM authorized user's SID, the User is then logged on to ECM to the applicable role. The Collector machine Operating System provides the initial ID & Authentication, establishing the User as holding a Collector machine account. Secondarily, in order to access ECM resources, the User is verified to have a valid ECM account and is logged in to the role associated to that account. The ID & Authentication Security Function provides the requirement for Administrator Users accessing the TOE from the Web Console to be positively identified to a SID value in the CMDB by the TSF, prior to accessing Collector and CMDB TSF resources. This ID & Authentication functionality is supported by the Collector and CMDB subsystems. Authentication related credentials stored within the Configuresoft CMDB are limited to the SIDs of the User Accounts and Role assignments associated with those SIDs.

2.5.9 Security Management

The Security Management Security Function provides the Security Management functions for the Collector machine and CMDB resources. Security Management functions are provided by the Web App component of the Collector Machine working through the Windows Internet Explorer Browser component of the Web Console Machine. Various management functions are available to allow Administrators to create ECM accounts, create network authority accounts, assign ECM account attributes such as passwords/roles, configure Machine Groups, configure application installation parameters, collect data from Agent Machines, evaluate data within the CMDB and initiate Remediation measures as required.

Agent machines can be organized within the ECM application by groupings called Machine Groups which allow specific Agent machines to be defined as a group and thereby allow easy assignment of access to User by Machine Group, instead of individually assigning Agent machine access.

The ECM application uses ECM accounts called Network Authority accounts to assign domain administrator privileges for Agent machines to the ECM application using existing NetBIOS domains, Active Directory domains or machine groups and thereby provide the Collector machine (ECM application) the required access to Agent machines within the enterprise.

The Security Management security function supports the management of ECM users maintained on the Collector Machine within the CMDB (database) structure. User attributes managed through the ECM account setup include username/password credentials (shared with the underlying OS account), assigned ECM administrative user role, and an SQL server role (separate from the ECM role) that relates to CMDB (SQL) access privileges.

The TOE supports the following roles: Configuresoft ECM Administrator, ECM read-only, Windows ECM Administrator, Active Directory ECM Administrator, UNIX ECM Administrator. The Configuresoft ECM Administrator has full read/write access to all ECM collected data regardless of Agent machine type and ECM application TSF data. The ECM read-only role has this same level of access but only read privileges, Windows, UNIX, and Active Directory ECM Administrators have read/write access to Collected Data of the applicable Agent machine type (ie: Windows ECM Administrator may access only Windows Agent collected data). The Collector and Web App subsystems within the Collector machine provide the prime support for the Security Management security function.

2.5.10 Session Termination by the IT Environment

ECM Session Termination – FTA_SSL.3

The IIS component of the IT Environment terminates ECM sessions after an ECM Administrator configured time period of inactivity to assure that sessions do not remain unattended or active for an extended period of time. This protects the TOE by limiting sessions to active usage and terminating the session when unused to lessen the chance that an unauthorized user may attempt to access the TOE through an unattended session. As this session termination function is supported by the IIS component in the IT Environment, this session termination event is not logged via the ECM TOE or Collector machine OS mechanisms.

2.6 Items Excluded from the TOE

The following items are excluded from the Common Criteria Evaluated configuration. The Common Criteria Evaluation configuration of the Configuresoft ECM product features a customized GUI, excludes most aspects of the full application not supported for Common Criteria.

2.6.1 Exclusions

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

- All ECM Compliance Auto Enforcement (Remediation)
- Rollback – (Rollback is the ability set a value back to its previous value from the change log screen)
- Use of the ECM Job Manager Tool
- Use of Mozilla for ECM Web Console (browser)
- Editing of various configuration settings, including Machine Groups, Filters, Compliance Toolkit Templates and Reports
- Assessment to criteria other than the Configuresoft ECM Rule Set
- All import / export, except to import the templates included with the CC installation image
- Split install and Collector Upgrade
- All Roles and the ability to create roles except the Configuresoft ECM Administrator, ECM Read-Only, Windows ECM Administrator, UNIX ECM Administrator, and Active Directory Administrator which are provided in the CC Evaluated Configuration.
- All Discovery types, except File List
- Disable function relating to Collector auditing functionality (must be enabled at all times)
- The Debug Event Viewer for access to debug events (EcmDebugEventViewer.exe shipped with release)
- User Scheduled Collections
- Agent installation using the Collector – Only Manual Installation using the .EXE installers allowed for CC
- All Collector initiated changes to Agent Machine configuration, except Starting / Stopping Services, Changes to the Registry and Resetting of Administrative Passwords for Windows Agent machines
- ECM Remote, Remote Command execution (from Collector to Agents) and File Upload / Download
- Patch Installation from Collector Console (only manual installation of patches to agent machine allowed)
- Security Update Manager (SUM) - (patch assessment and verification feature module)
- Enterprise Configuration Manager for Microsoft SMS (ECM for SMS)
- Enterprise Configuration Manager Management Extensions (ECMMX) for DCM
- Enterprise Configuration Manager for Windows Server Update Services (ECM for WSUS)

- Enterprise Configuration Manager Management Extensions (ECMMX) for Assets
- Enterprise Configuration Manager for Virtualization
- Enterprise Configuration Manager Service Desk Integration for Remedy
- ECM Web Services (SDK package) Toolkit
- ECM Reports other than those included within the CC evaluated configuration

3 TOE Security Environment

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

3.1 Assumptions

The assumptions are ordered into three categories: personnel assumptions, physical environment assumptions, and operational assumptions.

3.1.1 Personnel Assumptions

A.ADMIN	The authorized users of the TOE are assumed to be competent, trustworthy, non-hostile and to be conformant with guidelines supplied in applicable documentation.
A.LOG_COLLECT	The Administrative Users of the TOE are assumed to perform the necessary Collections to assure that log activity is collected from the Agent machine and placed in the CMDB for review.

3.1.2 Physical Environment Assumptions

A.LOCATE	The Collector is assumed to be located in a Server Room location providing physical protection and limited (Administrator only) access.

3.1.3 Operational Assumptions

A.USE	The Collector Machine is assumed to be dedicated to its use in supporting the ECM application (only the TOE and supported OS is running on Collector machine), the underlying Operating System users are all authorized ECM administrative users and there are no general purpose computing or storage repository capabilities available on the Collector Machine.
A.AGENT_PROT	The underlying OS (Windows, Active Directory, UNIX/Linux) of ECM Agent machines is assumed to provide essential protection to installed ECM Agent software.

3.2 Threats

The TOE or IT environment addresses the threats identified in this section. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.CONFIG_ERR	Configuration information from machines under TOE control may have an unknown configuration status to the TOE resulting in potential violation of the TOE security policy (sum of security functionality).
T.MASQ_USER	An unauthorized user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.
T.TSF_COMP	A User or Process may cause through an unsophisticated attack, TSF data to be inappropriately accessed (viewed, modified or deleted).

3.3 Organizational Security Policies

There are no Organizational Security Policies for this TOE.

4 Security Objectives

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

4.1 Security Objectives For The TOE

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

O.DATA_ACCESS	The TOE will provide role based access control functions to specific SFP objects and operations based on selected security attributes.
O.AUDIT_GEN	The TOE will provide the capability to detect and create records of security-relevant events.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit information.
O.CONFIG_MGMT	The TOE will provide the capability to collect, analyze, store, and remediate configuration information on specified data types in the CMDB for Windows, and Active Directory based machines.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.SECURE_COMM	The TOE will establish and require secure communications for all data transfers utilizing either DCOM, HTTPs or TLS secure protocols.
O.PART_SELF_PROT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosures through its own interfaces.

4.2 Security Objectives for the Environment

The following IT security objectives for the environment are to be addressed by the IT environment by technical means.

OE.CRYPT	The IT Environment of Collector/Agent machines will provide a cryptographic module for use by the TOE for session encryption.
OE.ACCESS_CONT	The IT Environment of the Collector machine will provide access control functions to specific SFP objects and operations based on selected security attributes.
OE.AGENT_PROT	The IT Environment of the Agent machines will provide essential protection to ECM Agent software installed on ECM Agent Machines.
OE.AUD_STOR	The IT Environment of the Collector machine maintains the Windows Event Log mechanism and the IT Environment of the Agent machine maintains either the Windows Event log mechanism (Windows, AD Agents) or the UNIX/Linux based logging mechanism which is used for the logging of ECM related events. Adequate storage resources are provided to assure retention of TOE related audit records and the IT Environment shall protect the stored audit records from unauthorized modification or deletion.
OE.LOG_COLLECT	ECM Administrative Users shall perform the necessary Collections to ensure that Agent machine log data is collected to the CMDB database where it is available for periodic Administrator review.
OE.NO_BYPASS	The IT Environment of Collector/Agent machines will provide mechanisms to assure that access control measures in the TOE cannot be bypassed through the IT Environment.
OE.TIME_STAMPS	The IT Environment of the Collector machine shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.

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

OE.PHYSEC	The TOE is physically secure and physical access to the Collector Machine is controlled to assure only authorized administrators have access.
OE.NO_EVIL	Authorized administrators are non-hostile and follow all administrator guidance.

OE.ROBUST_ADMIN	Sites will ensure that the Administrators of the TOE Environment are competent, trustworthy and conform to guidance supplied in applicable documentation.
OE.USE	The Collector Machine is dedicated to its use in supporting the ECM application (only the ECM Collector software and supporting OS are running on the Collector machine), the underlying Operating System users are all authorized ECM administrative users and there are no general purpose computing or storage repository capabilities available on the Collector Machine.

4.3 Mapping of Security Environment to Security Objectives

The following table represents a mapping of the threats and assumptions to the security objectives defined in this ST.

	A.ADMIN	A.LOG_COLLECT	A.AGENT_PROT	A.LOCATE	A.USE	T. CONFIG_ERR	T.TSF_COMP	T.AUDACC	T.MASQ_USER
O.DATA_ACCESS									X
O.AUDIT_GEN								X	
O.AUDIT_REVIEW								X	
O.CONFIG_MGMT						X			
O.MANAGE							X		
O.SECURE_COMM									X
O.PART_SELF_PROT									X
OE.ACCESS_CONT							X		X
OE.AGENT_PROT			X						
OE.LOG_COLLECT		X							
OE.AUD_STOR								X	
OE.CRYPT									X
OE.NO_BYPASS							X		

OE.NO_EVIL	X								
OE.PHYSEC				X					
OE.ROBUST_ADMIN	X								
OE.TIME_STAMPS								X	
OE.USE					X				

	A.ADMIN	A.AGENT_PROT	A.LOCATE	A.USE	T. CONFIG_ERR	T.TSF_COMP	T.AUDACC	T.MASQ_USER
O.DATA_ACCESS								X
O.AUDIT_GEN							X	
O.AUDIT_REVIEW							X	
O.CONFIG_MGMT					X			
O.MANAGE						X		
O.SECURE_COMM								X
O.SECURE _DATA						X		
O.PART_SELF_PROT								X
OE.ACCESS_CONT						X		X
OE.AGENT_PROT		X						
OE.AUD_STOR							X	
OE.CRYPT								X
OE.NO_BYPASS						X		
OE.NO_EVIL	X							
OE.PHYSEC			X					
OE.ROBUST_ADMIN	X							

OE.TIME_STAMPS							X	
OE.USE				X				

Table 14: Threats & IT Security Objectives Mappings

4.4 Rationale For Threat Coverage

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

T. TSF_COMP	The threat T.TSF_COMP is mitigated by O.MANAGE which supports restricting TSF functions and facilities from unauthorized use. OE.ACCESS_CONT further mitigates this threat in the IT Environment by providing Access Controls on the machine where the TOE is installed. OE.NO_BYPASS further mitigates this threat by assuring that the access controls mechanisms are not bypassed.
T.AUDACC	The threat T.AUDACC is mitigated by O.AUDIT_GEN and O.AUDIT_REVIEW that assures audit records are generated for all changes to the TSF or configuration changes and are available for review within the TSF. OE.AUD_STOR assures that a facility within the IT Environment exists for the generation of audit records for use by the ECM application and that adequate storage resources are provided.. OE.TIME_STAMPS assures that audit records include accurate time references provided by a time source within the IT Environment.
T.CONFIG_ERR	The threat T.CONFIG_ERR is mitigated by O.CONFIG_MGMT which assure that the TOE properly identifies specified Network Resources for Collection and Collects specified data types for Windows, Active Directory and UNIX/Linux based machines.

T.MASQ_USER	The threat T.MASQ_USER is mitigated by O.DATA_ACCESS which establishes access control restrictions to specific SFP objects and operations based on selected security attributes. O.PART_SELF_PROT mitigates this threat by assuring that the TOE maintains a domain for its own execution that protects itself and its interfaces from external interference, tampering, or unauthorized disclosures. O.SECURE_COMM also mitigates this threat by the TOE utilizing either DCOM or TLS secure protocols for communication between the Collector and Agent subsystems This threat is also mitigated by OE.CRYPT which provides cryptographic services in the IT Environment for use by the TOE in establishing secure sessions. OE.ACCESS_CONT further mitigates this threat by providing Access Controls within the IT Environment for the machine where the TOE is installed.

4.5 Rationale For Organizational Policy Coverage

There are no Organizational Policies for this TOE.

4.6 Rationale For Assumption Coverage

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

A.ADMIN	The assumption A.ADMIN is addressed in the objective OE.ROBUST_ADMIN which ensures that Administrators of the IT Environment are competent, trustworthy and conform to guidance supplied in applicable documentation. The assumption is further supported by OE.NO_EVIL which specifies that Administrators managing IT Environment resources supporting the TOE are non-hostile.
A.LOG_COLLECT	The assumption A.LOG_COLLECT is addressed in the objective OE.LOG_COLLECT which specifies that Administrative Users will perform the necessary Collections from Agent machines to ensure logs are copied to the CMDB database where they are available for Administrator review.
A.AGENT_PROT	The assumption A.AGENT_PROT addressed in the objective OE.AGENT_PROT which specifies that the underlying Operating System (IT Environment) will provide essential protection to the

	ECM Agent installed on the ECM Agent machine platform.
A.LOCATE	The assumption A.LOCATE is addressed in the objective OE.PHYSEC which specifies that the resources housing TOE components are physically secure and physical access to the Collector machine is controlled to assure only authorized administrators have access.
A.USE	The assumption A.USE is restated directly in the objective OE.USE which specifies that the Administrator ensures there are no general-purpose computing capabilities (e.g., compilers, editors, or user applications unrelated to TOE functionality) are available on the Collector machine.

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 - 5.11.

TOE Security Functional Requirements (from CC Part 2)	
FAU_GEN.2	User identity association
FAU_SAR.1	Audit Review
FIA_ATD.1	User attribute definition
FIA_UID.2	User Identification before any action
FIA_UAU.2	User Authentication before any action
FMT_MOF.1a	Management of security functions behaviour-***Modify***
FMT_MOF.1b	Management of security functions behaviour-***Enable/Disable***
FMT_MTD.1a	Management of TSF data-***Query, Modify, Delete***
FMT_MTD.1b	Management of TSF data-***Query***
FMT_MTD.1c	Management of TSF data-***Query (audit records)***
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RVM.1	Non-Bypassibility of the TSP
TOE Explicit Security Functional Requirements	
FAU_GEN.EXP.1a	Security Audit Generation
FDC_ANL.EXP.1	Data Collect functions
FDC_DTA.EXP.1a	System Data Collection – ***Windows***
FDC_DTA.EXP.1b	System Data Collection – ***UNIX/Linux***
FDC_DTA.EXP.1c	System Data Collection – ***Active Directory***
FDC_RDR.EXP.1a	Restricted Data Review-***Global***
FDC_RDR.EXP.1b	Restricted Data Review-***Windows***
FDC_RDR.EXP.1c	Restricted Data Review-***UNIX/Linux***
FDC_RDR.EXP.1d	Restricted Data Review-***Active Directory***
FDC_REM.EXP.1	Remediation

FPT_SEP.EXP.1	TSF ***partial*** domain separation

Table 15: Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 Class FAU: Security Audit

FAU_GEN.2 **User identity association**

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 **Audit review**

FAU_SAR.1.1 The TSF shall provide **Configuresoft ECM Administrator, ECM Read Only, Windows ECM Administrator, UNIX ECM Administrator, Active Directory ECM Administrator** with the capability to read **all audit trail data** 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.

5.1.2 Class FIA: Identification and authentication

FIA_ATD.1 **User attribute definition**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **Username, Configuresoft ECM assigned role.**

FIA_UID.2 **User identification before any action**

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.

FIA_UAU.2 **User authentication before any action**

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

5.1.3 Class FMT: Security management

FMT_MOF.1a **Management of security functions behaviour-*Modify***

FMT_MOF.1.1a The TSF shall restrict the ability to modify the behaviour of the functions **Data Consolidation, Collector Configuration, Rule Based Compliance Evaluation, Remediation** to **Configuresoft ECM Administrator, Windows ECM Administrator, UNIX ECM Administrator, Active Directory ECM Administrator**.

FMT_MOF.1b **Management of security functions behaviour-*Enable/Disable***

FMT_MOF.1.1b The TSF shall restrict the ability to enable, disable the functions **Collector Service** to **Configuresoft ECM Administrator, Windows ECM Administrator, UNIX ECM Administrator, Active Directory ECM Administrator**.

FMT_MTD.1a **Management of TSF data-*Query, Modify, Delete***

FMT_MTD.1.1a The TSF shall restrict the ability to query, modify, delete the **User: Accounts, ECM Role assignments, Assign roles to OS user accounts** to **Configuresoft ECM Administrator.**

FMT_MTD.1b **Management of TSF data-*Query***

FMT_MTD.1.1b The TSF shall restrict the ability to query the **CMDB Data listed in Table 24, Table 25 & Table 26** to **Configuresoft ECM Administrator, ECM Read-Only, Windows ECM Administrator, Active Directory ECM Administrator, UNIX ECM Administrator.**

FMT_MTD.1c **Management of TSF data-*Query (audit records)***

FMT_MTD.1.1c The TSF shall restrict the ability to query the **Audit Records** to **Configuresoft ECM Administrator, ECM Read-Only, Windows ECM Administrator.**

FMT_SMF.1 **Specification of Management Functions**

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

a. **Review audit logs**

b. **Establish new ECM Admin Accounts**

c. **User Account management/ User Role Assignment/ User Machine Group Assignment**

d. **Collector Configuration – set data types for collection, collection filters**

e. **Rule based Compliance Evaluation of CMDB data (Windows, Active Directory, UNIX, Linux)**

f. **Report generation based on CMDB data/Compliance Evaluation**

g. **Remediation of Windows Agent Data (manual)**

h. **Manual Data Collection (CMDB data)**

i. **Machine management configuration incl. discovery list upload, Group Assignment – Agent machines**

j. **Network Authority configuration – Agent network access credentials entry/management**

k. **CMDB data management of collected data, query**

FMT_SMR.1 **Security roles**

FMT_SMR.1.1 The ***TSF of the Collector*** shall maintain the roles **Configuresoft ECM Administrator, ECM Read-Only, Windows ECM Administrator, Active Directory ECM Administrator, UNIX ECM Administrator.**

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

5.1.4 Class FPT: Protection of the TSF

FPT_ITT.1 **Basic internal TSF data transfer protection**

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

FPT_RVM.1 **Non-bypassability of the TSP**

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.

5.2 Explicitly Stated TOE Security Functional Requirements

5.2.1 Class FAU: Security Audit (Explicit)

FAU_GEN.EXP.1a Audit data generation

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

a) All auditable events for the not specified level of audit; and
b) **defined auditable events listed in Table 16: Audited Events**

Component	Event	Details (examples)
FAU_GEN.EXP.1 FIA_UID.2 FIA_UAU.2	Access to System, Login/Logout to Web Console	Successful ECM Logon Failed ECM Logon Successful ECM Logout Failed ECM Logout Successful ECM User disabled Failed ECM User disabled
FMT_SMF.1	Security Management functions	Success Network Authority Account Add Failed Network Authority Account Add Success ECM User Account Add Failed ECM User Account Add Success ECM User Account Delete Failed ECM User Account Delete
FMT_MOF.1a	Data Consolidation, Collector Configuration, Rule Based Compliance Evaluation, Remediation	Successful Collection Failed Collection Successful Collector Configuration Failed Collector Configuration Successful Compliance Evaluation Failed Compliance Evaluation Successful Remediation (ie: registry change) Failed Remediation (ie: registry change)
FMT_SMR.1	Modification to the User Role assignments	ie: User Role Assignment Success User Role Assignment Failure
FDC_DTA.EXP.1a FDC_DTA.EXP.1b FDC_DTA.EXP.1c	Data Collection Events through installed Agents	Successful Collection Failed Collection
FDC_REM.EXP.1	Remediation Actions	Successful Remediation (ie: registry change) Failed Remediation (ie: registry change) Successful Remediation (ie: agent password change) Failed Remediation (ie: agent password change) Successful Remediation (ie: Start/Stop service) Failed Remediation (ie: Start/Stop service)

Table 16: Audited Events

*registry change is a data type that may be changed on Agent Machines through the manual remediation process described in FDC_REM.EXP.1

FAU_GEN.EXP 1.2a 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 audit relevant information.**

5.2.2 Class FDC: Data Collect functions (Explicit Class)

FDC_ANL.EXP.1 **Collected Data Analysis**

FDC_ANL.EXP.1.1 The Collector shall provide the capability to evaluate ECM collected data in the CMDB against Administrator selected Compliance templates and provide an analytical result in a report format.

FDC_ANL.EXP.1.2 The Collector shall record within each analytical result at least the following information:

"Run Date" = Date and time of the result

"Machine/Object" = Identification of data source

"Run By" = Identification of user

"Data Type" = Data Type

"Property" = Property Name

"Value Expected" = Value expected

"Value Found" = Value found

"Status" = Status of the analysis

FDC_DTA.EXP.1a **System Data Collection - *Windows***

FDC_DTA.EXP.1.1a The TOE shall collect the following information from the targeted IT resources and store the collected data in the Configuration Management Database (CMDB):

a. Collected data types (default) for Windows based Clients as listed in Table 24: Collected data types (default) for Windows based Clients

FDC_DTA.EXP.1b **System Data Collection – *UNIX/Linux***

FDC_DTA.EXP.1.1b The TOE shall collect the following information from the targeted IT resources and store the collected data in the Configuration Management Database (CMDB):

a. Collected data types (default) for UNIX/Linux based Clients as listed in Table 25: Collected data types (default) for UNIX/Linux based Clients

FDC_DTA.EXP.1c **System Data Collection – *Active Directory***

FDC_DTA.EXP.1.1c The TOE shall collect the following information from the targeted IT resources and store the collected data in the Configuration Management Database (CMDB):

a. Collected data types (default) for Active Directory based Clients as listed in Table 26: Collected data types (default) for Active Directory based Clients

FDC_RDR.EXP.1a **Restricted Data Review (EXP) - *Global***

FDC_RDR.EXP.1.1a The Collector shall provide ECM Administrator, ECM Read-Only with the capability to read Data listed in Table 24: Collected data types (default) for Windows based Clients, Table 25: Collected data types (default) for UNIX/Linux based Clients, Table 26: Collected data types (default) for Active Directory based Clients from the CMDB.

FDC_RDR.EXP.1.2a The Collector shall provide the CMDB data in a manner suitable for the user to interpret the information.

FDC_RDR.EXP.1.3a The Collector shall prohibit all users read access to the CMDB data, except those users that have been granted explicit read-access.

FDC_RDR.EXP.1b **Restricted Data Review (EXP) - *Windows***

FDC_RDR.EXP.1.1b The Collector shall provide Windows ECM Administrator with the capability to read Data listed in Table 24: Collected data types (default) for Windows based Clients from the CMDB.

FDC_RDR.EXP.1.2b The Collector shall provide the CMDB data in a manner suitable for the user to interpret the information.

FDC_RDR.EXP.1.3b The Collector shall prohibit all users read access to the CMDB data, except those users that have been granted explicit read-access.

FDC_RDR.EXP.1c	**Restricted Data Review (EXP) – *UNIX/Linux***
FDC_RDR.EXP.1.1c	The Collector shall provide UNIX/Linux ECM Administrator with the capability to read Data listed in Table 25: Collected data types (default) for UNIX/Linux based Clients from the CMDB.
FDC_RDR.EXP.1.2c	The Collector shall provide the CMDB data in a manner suitable for the user to interpret the information.
FDC_RDR.EXP.1.3c	The Collector shall prohibit all users read access to the CMDB data, except those users that have been granted explicit read-access.

FDC_RDR.EXP.1d	**Restricted Data Review (EXP) – *Active Directory***
FDC_RDR.EXP.1.1d	The Collector shall provide Active Directory ECM Administrator with the capability to read Data listed in Table 26: Collected data types (default) for Active Directory based Clients from the CMDB.
FDC_RDR.EXP.1.2d	The Collector shall provide the CMDB data in a manner suitable for the user to interpret the information.
FDC_RDR.EXP.1.3d	The Collector shall prohibit all users read access to the CMDB data, except those users that have been granted explicit read-access.

FDC_REM.EXP.1	**Remediation**
FDC_REM.EXP.1.1	The collector shall perform remediation actions on Windows Agent machines to initiate configuration changes based on the following:

A: Manual remediation - the TSF shall be capable of initiating the following changes on Windows Agent machines from the ECM Collector:

- Registry – Add Registry Key, Delete Registry Key, Add Registry Value, Modify Registry Value, Delete Registry Value
- Change Password – Local Machine Accounts, Domain Accounts
- Windows Services – Start/Stop Services (configured for Automatic or Manual Startup*)

* Services in a disabled state on the Agent machine are not changed using the ECM remediation function.

FDC_REM.EXP.1.2 Remediation actions generate an audit record on the Collector machine.

FDC_REM.EXP.1.3 If the change has been completed, success or failure of the remediation event is indicated by:

A: If the Remediation event was successful the Collector indicates this by creating a Success audit event.

B: If the Remediation event was unsuccessful, the Collector indicates this by creating a Failure audit event.

5.2.3 Class FPT: Protection of the TSF (Explicit Class)

FPT_SEP.EXP.1 **TSF *partial* domain separation**

FPT_SEP.EXP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.3 IT Environment Security Functional Requirements

The SFRs on the IT environment defined in this section are taken from Part 2 of the CC.

IT Environment Security Functional Requirements (from CC Part 2)	
FAU_STG.1	Protected audit trail storage
FCS_CKM.1a	Cryptographic Key Management- ***software RNG (symmetric)***
FCS_CKM.1b	Cryptographic Key Management - ***software RNG (asymmetric)***
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1b	Cryptographic Operation **– *Administrator Sessions***
FCS_COP.1c	Cryptographic Operation **– *Collector/Agent Communication***
FIA_UAU.2	User Authentication by IT Environment
FIA_UID.2	User Identification by IT Environment

FPT_RVM.1	Non-Bypassibility of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Time Stamps
FTA_SSL.3	~~TSF~~ ***IT Environment-Initiated Termination***
IT Environment Explicit Security Functional Requirements	
FAU_GEN.EXP.1b	Audit data generation - explicit
FAU_GEN.EXP.2	User Identity Association - explicit

Table 17: IT Environment SFRs

5.3.1 Class FAU: Security Audit

FAU_STG.1 **Protected audit trail storage**

FAU_STG.1.1 The ~~TSF~~ ***IT Environment*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The ~~TSF~~ ***IT Environment*** shall be able to prevent unauthorized modifications to the audit records in the audit trail.

5.3.2 Class FCS: Cryptographic Support

FCS_CKM.1a Symmetric Key Gen – ***software RNG (symmetric)***

FCS_CKM.1.1a The ~~TSF~~ ***IT Environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Software RNG using AES/3DES** and specified cryptographic key sizes **128, 192, 256 bit (192 bit 3DES)** that meet the following: **ANSI X9.31, FIPS 186-2, or FIPS SP 800-90**

FCS_CKM.1b Cryptographic key generation-***software RNG (asymmetric)***

FCS_CKM.1.1b The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie-Hellman** and specified cryptographic key sizes **512, 1024, 2048** that meet the following: **RFC 2631, FIPS PUB 140-2**..

FCS_CKM.4 **Cryptographic key destruction-*session keys***

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

FCS_COP.1b **Cryptographic operation – *Administrator Sessions***

FCS_COP.1.1b The ~~TSF~~ ***IT Environment*** shall perform **encryption/decryption for ECM Web Console sessions** in accordance with a specified cryptographic algorithm **3DES, AES with SHA1 using RSA, Diffie-Hellman for key exchange** and cryptographic key sizes **168 bits (3DES) 256 bit (AES) 512, 1024, 2048 (RSA/DH)** that meet the following: **FIPS 46-3 (3DES), ANSI X9.31 (RSA), RFC 2631 (DH) and RFC 4346 (TLS)**.

FCS_COP.1c **Cryptographic operation – *Collector/Agent Communication***

FCS_COP.1.1c The ~~TSF~~ ***IT Environment*** shall perform **encryption/decryption for Collector/Agent sessions** in accordance with a specified cryptographic algorithm **3DES,AES with SHA1/MD5 HMAC and using RSA for key exchange** and cryptographic key sizes **168 bits (3DES) 128 bit (AES) 512, 1024, 2048 bit (RSA)** that meet the following: **FIPS 46-3 (3DES), FIPS 197 (AES).**

5.3.3 Class FIA: Identification and authentication

FIA_UAU.2 **User authentication *by IT Environment***

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

FIA_UID.2 **User identification *by IT Environment***

FIA_UID.2.1 The ~~TSF~~ ***IT Environment of the Collector*** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.3.4 Class FPT: Protection of the TSF

FPT_RVM.1 **Non-bypassability of the TOE Security Policy (TSP)**

FPT_RVM.1.1 The ~~TSF~~ ***IT Environment*** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to

proceed.

FPT_SEP.1 **TSF domain separation**

FPT_SEP.1.1 The ~~**TSF**~~ ***IT Environment*** shall maintain a security domain for *the TOE's* execution that protects ***the TOE*** from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ~~**TSF**~~ ***IT Environment*** shall enforce separation between the security domains of subjects in the TSC**.**

FPT_STM.1 **Reliable Time Stamps**

FPT_STM.1.1 The ~~TSF~~ ***IT Environment*** shall be able to provide reliable time stamps for ***the TOE and*** its own use.

5.3.5 Class FTA: TOE Access

FTA_SSL.3 ~~**TSF**~~ ***IT Environment*** **-initiated termination**

FTA_SSL.3.1 The ~~TSF~~ ***IT Environment*** shall terminate an interactive session after a **Configuresoft ECM Administrator configured time interval of user inactivity**.

*note: IIS in the IT Environment logs off the ECM session as configured for Common Criteria.

5.4 Explicitly Stated IT Security Functional Requirements

5.4.1 Class FAU: Security Audit (Explicit)

FAU_GEN.EXP.1b **Audit data generation - explicit**

FAU_GEN.EXP 1.1b The ~~TSF~~ ***IT Environment*** shall be able to generate an audit record of the following auditable events:

a) Failed login attempts to ECM by a non-admin user*

*these must be logged by the Collector IT Environment as access to the application audit resources is denied

FAU_GEN.EXP 1.2b The ~~TSF~~ ***IT Environment*** shall provide the logging infrastructure within the underlying operating system environment for use by the TSF in generating audit logs.

FAU_GEN.EXP 1.2c The ~~TSF~~ ***IT Environment*** shall record within each audit record at least the following information:

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

FAU_GEN.EXP.2 **User identity association- explicit**

FAU_GEN.EXP.2.1 For audit events resulting from actions of *non ECM* users, the ~~TSF~~ ***IT Environment*** shall be able to associate each auditable event with the identity of the user that caused the event.

5.5 TOE Strength of Function Claim

There are no probabilistic or permutational mechanisms used in the product and therefore no Strength of Function claim for the TOE.

5.6 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 as defined by the CC. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.3	Authorisation 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

Assurance Class	Assurance Components	
	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 18: Assurance Requirements: EAL3

*Note: Product usage is transparent to network users therefore this requirement (AGD_USR.1) requirement is vacuously satisfied (ref: PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied).

5.6.1 ACM_CAP.3 Authorisation controls

Developer action elements

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.

Content and presentation of evidence elements

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.

ACM_CAP.3.7C The CM system shall uniquely identify all configuration items.

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.

Evaluator action elements

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.2 ACM_SCP.1 TOE CM coverage

Developer action elements

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

Content and presentation of evidence elements

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.

Evaluator action elements

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

5.6.3 ADO_DEL.1 Delivery procedures

Developer action elements

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.

Content and presentation of evidence elements

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.

Evaluator action elements

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

5.6.4 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements

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.

Evaluator action elements

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.

5.6.5 ADV_FSP.1 Informal functional specification

Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements

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.

Evaluator action elements

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 requirements.

5.6.6 ADV_HLD.2 Security enforcing high-level design

Developer action elements

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

Content and presentation of evidence elements

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.

Evaluator action elements

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.

5.6.7 ADV_RCR.1 Informal correspondence demonstration

Developer action elements

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

Content and presentation of evidence elements

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.

Evaluator action elements

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

5.6.8 AGD_ADM.1 Administrator guidance

Developer action elements

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

Content and presentation of evidence elements

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 behavior 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.

Evaluator action elements

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

5.6.9 AGD_USR.1 User guidance

Developer action elements

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements

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 behavior 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.

Evaluator action elements

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

5.6.10 ALC_DVS.1 Identification of security measures

Developer action elements

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

Content and presentation of evidence elements

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.

Evaluator action elements

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.

5.6.11 ATE_COV.2 Analysis of coverage

Developer action elements

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

Content and presentation of evidence elements

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.

Evaluator action elements

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

5.6.12 ATE_DPT.1 Testing: high-level design

Developer action elements

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

Content and presentation of evidence elements

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.

Evaluator action elements

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

5.6.13 ATE_FUN.1 Functional testing

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements

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.

Evaluator action elements

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

5.6.14 ATE_IND.2 Independent testing - sample

Developer action elements

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

Content and presentation of evidence elements

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.

Evaluator action elements

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.

5.6.15 AVA_MSU.1 Examination of guidance

Developer action elements

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements

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).

Evaluator action elements

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.

5.6.16 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements

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.

Content and presentation of evidence elements

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.

Evaluator action elements

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.

5.6.17 AVA_VLA.1 Developer vulnerability analysis

Developer action elements

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

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

Content and presentation of evidence elements

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.

Evaluator action elements

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.

5.7 Rationale For TOE Security Requirements

5.7.1 TOE Security Functional Requirements

	O.DATA_ACCESS	O.AUDIT_GEN	O.AUDIT_REVIEW	O.CONFIG_MGMT	O.MANAGE	O.SECURE_COMM	O.PART_SELF_PROT
FAU_GEN.2		X					
FAU_SAR.1			X				
FIA_ATD.1	X						
FIA_UAU.2	X						

	O.DATA_ACCESS	O.AUDIT_GEN	O.AUDIT_REVIEW	O.CONFIG_MGMT	O.MANAGE	O.SECURE_COMM	O.PART_SELF_PROT
FIA_UID.2	X						
FMT_MOF.1a					X		
FMT_MOF.1b					X		
FMT_MTD.1a					X		
FMT_MTD.1b					X		
FMT_MTD.1c					X		
FMT_SMF.1					X		
FMT_SMR.1	X				X		
FPT_ITT.1						X	
FPT_RVM.1							X
FPT_SEP.EXP.1							X
FAU_GEN.EXP.1		X					
FDC_ANL.EXP.1				X			
FDC_DTA.EXP.1a				X			
FDC_DTA.EXP.1b				X			
FDC_DTA.EXP.1c				X			
FDC_RDR.EXP.1a	X						
FDC_RDR.EXP.1b	X						
FDC_RDR.EXP.1c	X						
FDC_RDR.EXP.1d	X						
FDC_REM.EXP.1				X			

Table 19: SFR and Security Objectives Mapping

Security Objective	Mapping Rationale
O.DATA_ACCESS	FMT_SMR1. supports this objective by providing role based access mechanisms and supporting access restrictions based on assigned role to specified TOE resources. FIA_ATD.1 supports this objective by providing the security attributes: Username and Configuresoft ECM assigned role for access control purposes in the TSF. FDC_RDR.EXP.1a,b,c,d supports this objective by providing role based access restrictions for the review of TSF data and by providing TSF data in a suitable format for usage by Administrator personnel. FIA_UID.2 supports this objective by the requiring Identification of users prior to gaining access to TSF resources. FIA_UAU.2 supports this objective by requiring that users are authenticated prior to gaining access to TSF resources.
O.AUDIT_GEN	FAU_GEN.EXP.1 and FAU_GEN.2 support this objective by specifying that the TOE generates audit records based on TSF operations, associated by users and specifies the list of data that shall be recorded in each record. FAU_SAR.1 supports this objective by specifying that the TOE provides the ability to review audit records.
O.AUDIT_REVIEW	FAU_SAR.1 supports this objective by providing administrative users with the ability to review audit records in a suitable form.
O.CONFIG_MGMT	FDC_DTA.EXP.1a supports this objective by specifying that the TOE shall be capable of collecting information on specific data types for Windows based machines on the supported network. FDC_DTA.EXP.1b supports this objective by specifying that the TOE shall be capable of collecting information on specific data types for UNIX based machines on the supported network. FDC_DTA.EXP.1c supports this objective by specifying that the TOE shall be capable of collecting information on specific data types for Active Directory based machines on the supported network. FDC_ANL.EXP.1 supports this objective by specifying that the TOE shall provide the capability to analyze collected data. FDC_REM.EXP.1 supports this objective by specifying that the TOE shall provide the capability to change data through remediation based on the collection and analysis processes.
O.MANAGE	FMT_MOF.1a, FMT_MOF.1b supports this objective by specifying that the TOE restricts the ability to perform specified security related functions to authorized roles.

	FMT_SMF.1 supports this objective by specifying that the TOE includes functions to support security management of the TOE. FMT_SMR.1 specifies that the TOE supports access to TSF resources based on role based access control mechanisms within the TOE. FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c specifies the TSF data that can be queried, modified or deleted by use of the TOE's management functions.
O.SECURE_COMM	FPT_ITT.1 supports this objective by specifying that data must be protected from modification or disclosure by the TSF when transmitted between separate parts of the TOE.
O.PART_SELF_PROT	FPT_RVM.1 Non-bypassability of the TSP supports this objective by ensuring that TSP enforcement functions are invoked and succeed before TSF access is allowed. FPT_SEP.EXP.1 Partial Domain Separation supports this objective by providing domain separation and protection from untrusted users. This SFR was made explicit as this is realized in conjunction with protective aspects provided by the IT Environment.

5.7.2 TOE Security Assurance Requirements

EAL3 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

5.8 Rationale For IT Environment Security Requirements

	OE.ACCESS_CONT	OE.AUD_STOR	OE.NO_BYPASS	OE.TIME_STAMPS	OE.CRYPT
FIA_UAU.2	X				

	OE.ACCESS_CONT	OE.AUD_STOR	OE.NO_BYPASS	OE.TIME_STAMPS	OE.CRYPT
FIA_UID.2	X				
FPT_RVM.1			X		
FPT_SEP.1			X		
FPT_STM.1				X	
FAU_STG.1		X			
FCS_CKM.1a,b					X
FCS_COP.1b,c					X
FCS_CKM.4					X
FAU_GEN.EXP.1b		X			
FAU_GEN.EXP.2		X			

Table 20: SFR and Security Objectives Mapping

Environment Security Objective	Mapping Rationale
OE.ACCESS_CONT	FIA_UAU.2 supports this objective by assuring that the IT Environment requires authentication prior to allowing access to TSF resources. FIA_UID.2 supports this objective by assuring that the IT Environment requires identification prior to allowing access to TSF resources. FTA_SSL.3 support this objective by terminating inactive Administrative user sessions.
OE.AUD_STOR	FAU_STG.1 supports this objective by specifying that the IT Environment shall protect the stored audit records from unauthorized modification or deletion. FAU_GEN.EXP.1B specifies that the IT Environment (OS) provides the logging mechanisms that the TOE utilizes for capturing TOE related events. FAU_GEN.EXP.2

OE.CRYPT	FCS_CKM.1a,b supports this objective by specifying which Key generation methods are utilized for securing transmission and storage in support of the TOE. FCS_COP.1b, c support this objective by specifying cryptographic operations performed by the IT Environment in support of the TOE in securing Collector to Agent transmissions and data storage within the Collector Machine. FCS_CKM.4 support this objective by specifying which key destruction methods are utilized for cryptographic keys used to support the TOE.
OE.NO_BYPASS	FPT_RVM.1 Non-bypassability of the IT Environment Security Policy ensures that TSP enforcement functions are invoked and succeed before TSF access is allowed. FPT_SEP.1 supports this objective by providing a secure domain within the IT Environment for the TSF execution thereby protecting the TSF from interference and tampering by untrusted subjects.
OE.TIME_STAMPS	FPT_STM.1 supports this objective by specifying that the IT Environment provide for Time and Date references for use in recording audit records by time/date.

5.9 Rationale for Explicitly Stated Security Requirements

Table 21 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FDC_DTA.EXP.1a	System Data Collection - *Windows*	This explicit SFR is necessary to specify the ability of the TOE to collect information on specified data types on machines within the Network, when Agents have been installed on those machines. This SFR specifies Windows based machines. Modeled after IDS_SDC.1*see reference
FDC_DTA.EXP.1b	System Data Collection – *UNIX/Linux*	This explicit SFR is necessary to specify the ability of the TOE to collect information on specified data types on machines within the Network, when Agents have been installed on those machines. This SFR specifies UNIX/Linux based machines. Modeled after IDS_SDC.1*see reference
FDC_DTA.EXP.1c	System Data Collection – *Active Directory*	This explicit SFR is necessary to specify the ability of the TOE to collect information on specified data types on machines within the Network, when Agents have been installed on those machines. This SFR specifies Active Directory based machines. Modeled after IDS_SDC.1*see reference
FDC_ANL.EXP.1	Collected Data Analysis	Modeled after IDS_ANL.1*see reference Necessary to specify the data analysis function – CC Part 2 does not specify this requirement

Explicit Requirement	Identifier	Rationale
FDC_RDR.EXP.1a	Restricted Data Review - *Global*	Modeled after IDS_RDR.1*see reference necessary to specify data review restrictions for all data (Global) – CC Part 2 does not specify this requirement
FDC_RDR.EXP.1b	Restricted Data Review- *Windows*	Modeled after IDS_RDR.1*see reference– necessary to specify data review restrictions for Windows – CC Part 2 does not specify this requirement
FDC_RDR.EXP.1c	Restricted Data Review- *UNIX/Linux*	Modeled after IDS_RDR.1*see reference– necessary to specify data review restrictions for UNIX/Linux – CC Part 2 does not specify this requirement
FDC_RDR.EXP.1d	Restricted Data Review- *Active Directory*	Modeled after IDS_RDR.1*see reference – necessary to specify data review restrictions for Active Directory – CC Part 2 does not specify this requirement
FDC_REM.EXP.1	Remediation	Modeled after IDS_RCT.1*see reference – necessary to specify the ability to initiate manual remediation changes from the Collector to Windows Agent machines – CC Part 2 does not specify this requirement
FAU_GEN.EXP.1a	Audit Generation	This explicit SFR is necessary as the TOE does not provide audit records for the startup or shutdown of the Auditing Function due to the fact that these options are not supported by ECM (auditing is on by default and cannot be disabled within ECM) as included in the FAU_GEN.1 SFR from Part 2 of the CC.
FPT_SEP.EXP.1	Partial TSF domain separation	The FPT_SEP SFR from CC Part 2 cannot be completely satisfied by an application TOE. This component defines the separation that may be performed by applications.
FAU_GEN.EXP.1b	Audit Generation	This explicit SFR for the IT Environment is necessary as the TOE ECM Application cannot log failed login attempts to the ECM application, as access to ECM components is not allowed, therefore, for non-ECM (unauthenticated) users, the underlying Collector OS logs these attempts using the Event Log mechanism without using TOE mechanisms. This explicit SFR is modeled after FAU_GEN.1 from Part II of the Common Criteria standard.
FAU_GEN.EXP.2	User Identity Association	This explicit SFR for the IT Environment is necessary as to characterize that the underlying OS identifies claimed user identity during login attempts or other activities by non-ECM authenticated users as described in FAU_GEN.EXP.1b above. This explicit SFR is modeled after FAU_GEN.2 from Part II of the Common Criteria standard.

Table 21: Explicitly Stated SFR Rationale

* Reference: Intrusion Detection System - System Protection Profile Version 1.5 March 9, 2005

5.10 Rationale For IT Security Requirement Dependencies

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

Functional Component	Dependency	Included/Rationale
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	No *(FAU_GEN.1) (FAU_GEN.EXP.1) FIA_UID.1 reqt. satisfied through FIA_UID.2)
FAU_SAR.1	FAU_GEN.1	No* see (FAU_GEN.EXP.1)
FIA_ATD.1	None	Yes
FIA_UAU.2	FIA_UID.1	Yes, via FIA_UID.2
FIA_UID.2	None	Yes
FMT_MOF.1a	FMT_SMF.1, FMT_SMR.1,	Yes
FMT_MOF.1b	FMT_SMF.1, FMT_SMR.1,	Yes
FMT_MTD.1a	FMT_SMF.1, FMT_SMR.1,	Yes
FMT_MTD.1b	FMT_SMF.1, FMT_SMR.1,	Yes
FMT_MTD.1c	FMT_SMF.1, FMT_SMR.1,	Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes FIA_UID.1 reqt. satisfied through FIA_UID.2)
FPT_ITT.1	None	Yes
FPT_RVM.1	None	Yes
FPT_SEP.EXP.1	None	Yes
FAU_GEN.EXP.1a	FPT_STM.1	No
FDC_ANL.EXP.1	FDC_RDR.EXP.1a, FDC_RDR.EXP.1b, FDC_RDR.EXP.1c, FDC_RDR.EXP.1d FDC_DTA.EXP.1a, FDC_DTA.EXP.1b, FDC_DTA.EXP.1c	Yes
FDC_DTA.EXP.1a	None	Yes
FDC_DTA.EXP.1b	None	Yes
FDC_DTA.EXP.1c	None	Yes

Functional Component	Dependency	Included/Rationale
FDC_RDR.EXP.1a	None	Yes
FDC_RDR.EXP.1b	None	Yes
FDC_RDR.EXP.1c	None	Yes
FDC_RDR.EXP.1d	None	Yes
FDC_REM.EXP.1	FDC_DTA.EXP.1a, FDC_DTA.EXP.1b, FDC_DTA.EXP.1c	Yes

Table 22: SFR Dependencies

5.11 Rationale for Unsatisfied Dependencies

The following security requirements are depended upon by the security requirements for the TOE, yet were not included within this ST. These requirements and their justification is provided below.

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FAU_GEN.2	FAU_GEN.1	The dependency of FAU_GEN.1 (from Part 2) for FAU_GEN.2 is satisfied through explicit SFR FAU_GEN.EXP.1. This explicit contains all the requirements of FAU_GEN.1 from Part 2, except for the startup and shutdown of audit generation within the TOE. By containing nearly all aspects of FAU_GEN.1 from Part 2, FAU_GEN.EXP.1 adequately satisfies the dependencies required by FAU_GEN.2.
FAU_GEN.EXP.1a	FPT_STM.1	This dependency is not satisfied by TOE mechanisms as the TOE does not provide a time standard mechanism for use in audit logs. This is provided by the IT Environment (hardware/software (OS)) for use by the TOE in providing time stamp references in audit logs.

Table 23: Rationale for unsatisfied dependencies

5.12 Rationale for Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in **Table 22: SFR Dependencies**
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.7
- including the SFRs FPT_RVM.1 and FPT_SEP.EXP.1 to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

5.13 Rationale for Strength of Function Claim

The strength of function analysis is N/A as the TOE does not include any permutational or probabilistic mechanisms

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of the following Security Functions:

- ECM Data Access Control
- Security Audit
- Secure Communications
- Data Consolidation
- Assessment
- Remediation
- TOE Protection
- ID & Authentication
- Security Management

6.1.1 ECM Data Access Control

The ECM Data Access Control Security Function provides Role based access control to collected data that resides within the CMDB. Using the ECM Roles within the ECM Collector, access to CMDB data and analysis processes are restricted as described in the Security Management Section 6.1.9.

Collected Data Access Control FDC_RDR.EXP.1a, FDC_RDR.EXP.1b, FDC_RDR.EXP.1c, FDC_RDR.EXP.1d

Collected data from the deployed Configuresoft ECM Agents is stored in a SQL based database referred to in the TOE as the CMDB. This configuration data is collected to allow authorized users to review the configuration data in a variety of ways to determine security status and compliance to the various compliance templates provided within the ECM TOE.

Administrative access to this data is presented via a GUI on the Web Console Machine and access to this data is regulated by the access control methods described in Identification and Authentication, Section 6.1.8. The primary format of the data is in a columnar form referred to as the Data Grid.

Data viewed through the Data Grid can be selected through applying various filters which group data by rules selected or data attributes that correspond to collected data types and compliance template criteria. The interface also provides a mechanism to execute a search within the

CMDB, organizing the data and presenting it in the selected reporting format.

Icons and active buttons allow the user to navigate the page to view items by sorting or column grouping, based on the role of the user. Icons and menus on the screen dynamically update to indicate available access based on Role and display only objects that can be accessed through the current login credentials. Upon selecting an object to view in the GUI, the TSF accesses the CMDB via a dynamic SQL query which returns Role attributes. The TSF uses the Role attributes to either grant execute access to the requested object or return a null value if access is not granted. This access control is positively enforced through a dynamic SQL query which looks up the Role attributes within the CMDB and grants read access only upon returning a positive result. The TSF builds a dynamic SQL query based on the Role of the User and then displays the results of the query in the Data Grid.

When the Configuresoft ECM Administrator adds a user to ECM, ECM adds the user to a table in the Master CMDB, assigns a SQL Server role, distinct from ECM Roles, and assigns an ECM Role. There are two primary SQL Server roles – ECM Admin and ECM User. These roles govern what the user has access to in SQL Server. These roles work within the construct of the Web App, which is used to filter the query results and available functions from the CMDB. The SQL roles are not used by the Collector Service.

When a user logs in to ECM, their ECM role determines access within the application and that roles maps to an SQL role, which determines the level of access within the CMDB (SQL) database.

6.1.2 Security Audit

Security Audit events are generated by the Configuresoft ECM Collector component and are captured by the Collector Windows based Operating System event log in the IT Environment. The Security Audit security function records TSF events and changes as specified in Table 16: Audited Events which are stored using the IT Environment Event Log mechanism and protected through the Collector Operating System access control measures. Configuresoft Agent machine Event logs, residing in the Agent machine Operating System environment, are captured by the Collector component through the Data Consolidation security function using collection processes. This applies to both Collector based activities, such as ECM configuration changes and to collection operations launched from the Collector to Agent machines.

During collection processes, Agent Machine event logs (windows) or syslogd /var/log/messages (UNIX/Linux) are captured and placed in the CMDB database. The Collector contacts the applicable Agents and requests that specified data types (including audit logs) are collected for transmission to the Collector machine (consolidation). The Agent accesses the data and queues it for secure transmission to the Collector machine. The Collector machine then acquires the data over a symmetrically encrypted session and places the data in the CMDB. Once stored within the CMDB, logs are available for review by authorized Administrative Users.

Access to this data within the CMDB is controlled by role based TSF Identification and Authentication mechanisms. The TOE, through support from the underlying Operating System,

generates audit events for security related items and TSF configuration changes. The Administrator accesses audit records through the Web Console Machine interface and can view audit records through the ECM hosted GUI interface.

Audit Generation FAU_GEN.EXP.1a FAU_GEN.2, FAU_SAR.1

The Configuresoft ECM Collector component, working with the Event log mechanism within the Window Operating System, generates audit records within the Collector machine to log Collector machine TSF events. Events that are logged include access to TSF information, changes to security management settings and collection and analysis functions as listed in Table 16: Audited Events.

The Windows and Active Directory Agents do not actively trigger or store audit records as these are captured and stored exclusively by the Window's Agent Operating System event log mechanism. These event log entries include Collection activities and Remediation changes made to the applicable Agent machine. UNIX/Linux Agents also do not actively participate in logging and leverage the resident syslogd logging daemon to record ECM Agent activities on Agent machines and stores them locally in the /var/log/messages system file. The capturing of audit events related to the ECM TOE by the IT Environment is incidental as the ECM Agent component does not trigger or otherwise participate in audit logging on the Agent machine.

The Agent machine's event log or syslogd data is captured during ECM Collection processes and is stored as collected data types within the CMDB on the Collector machine where it can be reviewed. The security audit security function cannot be disabled within the ECM application by any users. This allows the ECM Administrator to collect audit logs from all Agent machines and the Collector and review these logs from a centralized location (the ECM Console) through the ECM GUI.

Within each audit record the date and time of the event is logged, the identity of the User associated with the event and the success or failure of the event.

The Security Audit Security Function generates audit records for ECM within the Collector for TSF management functions as described in Security Management, Section 6.1.9.

6.1.3 Secure Communications

The Secure Communications Security Function assures the integrity and security of data transfers between the ECM Agent Machines and the ECM Collector through the Data Consolidation Security Function. Two options are available based on the Operating System of the ECM Agent Machines. Windows based Operating Systems with the ECM Agent installed may secure data transfers using either the DCOM or TLS protocol. The secure protocol implementation is supported through Microsoft Cryptography module for Windows and Active Directory agent machines and OpenSSL object module for UNIX/Linux agent machines in the IT Environment. To implement secure communications between the Collector and Agent components, the ECM application makes calls to the applicable cryptographic modules in the IT Environment, passes the information to be encrypted/decrypted, and then receives the object

back for transmission within the TSC. The data is then transferred via DCOM or TLS protocol over HTTP transport and upon acquisition by the ECM Collector queued for processing to the CMDB as applicable.

Securing Data Transfers from Agent machines to the Collector FPT_ITT.1

The Configuresoft ECM TOE has two methods of secure data transfer between the Collector machine and Agent machines, DCOM and TLS protocol over HTTP transport.

For Windows based Agent machines, DCOM may be used to secure communications. DCOM includes a set of interfaces that allow objects to request services from server program objects with other computers in the network. Use of DCOM within the TOE leverages the packet privacy security setting to provide the highest level of security. DCOM creates a packet privacy based channel that sends info to the DCOM agent and then the Agent executes the instructions. The Collector polls the Agent for status and then upon completion, the Collector transfers the results and saves the data to the CMDB. Based on the collected location and data class attributes, the data is saved to the corresponding location in the Collector Machine file system and then, when the transfer is completed, the Collector inserts the data into the CMDB tables.

UNIX/Linux Agent machines cannot utilize DCOM, therefore TLS (via OpenSSL) is used for UNIX/Linux Agent Machines and as an option for Windows Agent machines. When creating a TLS session between the Collector and Agent, the TOE utilizes the TLS protocol to establish the secure session. The root certificate is installed during the initial Collector installation. The Collector serves as the TLS server for these sessions and holds a private key and associated certificate. The applicable Agent serves the TLS client and initiates the TLS session (Client Hello) to the Collector machine. This is not to be confused with network connect order where the Collector initiates the TCP connect with the Agent. The TLS handshake process conforms to and is described in RFC 4346.

ECM's usage of TLS for securing Collector to Windows, Active Directory or UNIX/Linux Agent machine sessions is limited (hard coded) to:

3DES 112 EDE (TLS_RSA_WITH_3DES_EDE_CBC_SHA) and AES 128 (TLS_RSA_WITH_AES_128_CBC_SHA) cipher suites.

DCOM when used for ECM Collector to Windows Agent sessions utilizes the RC4 cipher.

Collector – Agent Authentication

During the session initiation process, the Collector sends the certificate to the Agent, the Agent validates the certificate and then upon acceptance, generates a session key, encrypted with the Collector's public key. The Collector decrypts this session key with the associated private key and the session is established. All subsequent communication is encrypted using this session key. The Collector root certificate, which is created during initial installation and deployment of the TOE, is copied to Agents during Agent installation processes. This establishes certificate trust for each Agent machine.

Regardless of the protocol used, all cryptography utilized by the TOE is provided by either the

Microsoft SChannel security package (associated modules) or the OpenSSL cryptographic module in the respective Agent machine IT Environment.

Communication and data transfer between the Collector machine and Agent machines is executed through a Collection/Change request, initiated by an authorized Administrator from the Web Console Machine. Once the Collection button has been activated a wizard based dialog is launched and machine groups and Data Classes are selected for Collection. Upon completing the Wizard, a request is generated by the CMDB and sent to the Collector service. Then, the request is parsed and executed against each Agent Machine in a multi-threaded fashion.

Securing Data Transfers from the Console Machine to the Collector FPT_ITT.1

The ECM TOE secures the communication from the Web Console machine to the Collector's Web App subsystem using the HTTPs protocol and leveraging the Microsoft Cryptographic Modules in the IT Environment for encryption/decryption operations. This assures that Administrator sessions with the ECM application are secured via TLS using 3DES, 168 bit or AES 128 bit symmetric encryption. These sessions utilize the following ciphersuites:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA.

The console is an IIS hosted web service on a Windows platform. All cryptography used by the Configuresoft Web Application or the IIS server itself (including all cryptography used during authentication) calls the CryptoAPI. The CryptoAPI dispatches these calls to the installed cryptographic service provider (CSP).

All cryptographic functionality supporting the TOE's secure communication security function is provided by Cryptographic modules in the IT Environment (outside the TOE boundary), therefore, the cryptographic functionality was not tested as part of the Common Criteria Evaluation process.

6.1.4 Data Consolidation

The Data Consolidation Security Function reflects the Data Collection process executed on Agent machines as realized through Configuresoft ECM Agent functionality.

The Data Collection Security Function provides the ability for the ECM Collector to collect data from installed Agents within the Network and store the data within the CMDB for evaluation and remediation activities as described in Security Function, Remediation, Section 6.1.6 and Assessment, Section 6.1.5. By design, all communications between the Collector and Agents is initiated by the Collector. Data Collection utilizes configuration options that allow for selecting Agent machine to execute collection activities based on various attributes.

Machines Groups may be used to organize the Agent machines into logical groups for easier data collection and filters can be engaged to further focus Collection efforts. The default Machine Group provided is the All Machines group. Static machine groups may include Windows, UNIX and AD Agent machines and are configured by the Administrator whereas Dynamic machine groups may only include a single type of Agent machine where members are determined by filter

selections. The TOE includes pre-configured machine group definitions for “Windows Agent”, “UNIX Agent”, “Linux Agent”, “Active Directory” and “All Agent” machines. In practice, Machine Groups are used by ECM as a filtering mechanism to determine access for viewing, collection, and remediation. Only the provided machine groups may be used for the CC Evaluated configuration.

The Data Collection utilizes functionality from four discrete types of ECM Agent software components: one for Window based operating systems, one for UNIX based Operating Systems, one for Linux based Operating Systems and a fourth for Active Directory Agents. Agents are manually installed on the selected machines within the network for the CC Evaluated Configuration.

The Collector is able to access data on the Agent Machine through Network Authority accounts created and maintained within the CMDB as part of the ECM application. Network Authority accounts are established during installation and assign existing domain administrator privileges for the Agent machine within the network to the ECM application (Collector machine). These can be assigned to Agent machines via NetBIOS domains, Active Directory domains or machine groups. Network Authority data is maintained by the TSF and is used to associate domain administrator privileges to specific domains or machine groups to facilitate access to Agent Machines. This data is manually entered by the Configuresoft ECM Administrator and maintained in the CMDB to convey network domain access control privileges to the Configuresoft ECM Collector for use in accessing Agent machines on the network. Once Network Authority accounts are applied to Agent machine accounts (domain or machine group) with ECM, the Collector can access those Agent machines with domain Administrator access rights.

In summary, access to ECM objects is orchestrated through:

ECM Roles – are used security measures which restrict certain ECM Administrative Users to certain parts of the application as controlled by the GUI. Restricted objects for a given role are not displayed and/or are not accessible via the presented GUI screens. For example: a UNIX/Linux Administrator cannot see or access Windows Agents or Data via the GUI.

Machine Groups are used to organize the Agent machine for the purpose of filtering access for viewing, collection and remediation. If an Administrative User is not assigned to a machine group, they cannot access that collection of Agent machines/collected data. For the CC Evaluated Configuration, only the provided Machine Groups (“Windows Agent”, “UNIX Agent”, “Linux Agent”, “Active Directory” and “All Agent”) may be used for this purpose as editing of machine groups is excluded from the Common Criteria evaluation.

Domain is one aspect used to assign Network Authority accounts (credentials) used by the ECM Application (Collector) to access the Agent machines. For example: a given Network Authority account (containing domain administrator privileges) may be assigned to a NetBIOS or AD domain or machine group applying that level of Agent Machine access to the ECM application for collection and remediation.

Essential functionality for Common Criteria includes:

- Display filter-based Windows Registry entries from the entire enterprise
- Display all defined users for Windows, UNIX, Linux based systems
- Collect a defined set of configuration variables
- Track the file name, size, file version and file integrity data for any file type
- Store process information centrally, view the processes running on all machines
- Track files opened by processes on UNIX/Linux agent machines
- Collect history of system logs for Audit trail review purposes

The Collection process gathers detailed configuration information from targeted Machines based on a selected group of filters. A filter specifies exactly what information is to be collected based on data type.

FDC_DTA.EXP.1a Data Consolidation for Windows Agent Machines

Upon selecting a Windows network machine for Collection, the Configuresoft ECM Administrator manually installs the Configuresoft ECM Windows Agent software on the selected machine (manual installation of agents is required for the Common Criteria Evaluated configuration). During the installation, the Administrator is prompted to select a Secure Communication protocol, DCOM, TLS or both. Also during the installation process, the DCOM service is registered with the service control manager (SCM) and the binaries are copied and registered. If TLS is selected, those binaries are copied and registered as well. When the Collector does an agent machine inspection, if the HTTP listener is detected, the protocol is set to HTTP (using TLS), otherwise, the protocol utilizes DCOM by default for Windows machines.

Collection Process - Windows

Data is collected by the Collector through issuing a request to the Agent using the secure communication techniques detailed in the Secure Communications Security Function, Section 6.1.3. The Collector machine uses a series of pings (unless disabled) and makes multiple connection attempts with Agents. In the event that an Agent does not respond following a configured number of access attempts, the machine is marked as “Failed” within ECM. Once a machine has been marked as “Failed”, it applies to a given Collection request. Upon a new Collection request, contact will be again attempted and, upon success, the status is changed from “Failed” to “Succeeded”.

Upon successful communication, the Agent parses the Filters (contained in the request) and then loads the appropriate subsystem in the TSF to load the data from the targeted machine. Data Collection results are encrypted and then stored locally in a temporary file on the Agent machine. The Collector reinitiates communication by opening and closing sessions at intervals to determine if the collection is complete and transfer can commence. When the Agent responds

that collection is complete, the Collector requests transmission of the data over DCOM or TLS as applicable.

A Master File for each data class is maintained on the Agent machine to support Collector configuration verification activities, allowing the Collector to only collect data that has changed since the last collection session. The Configuresoft ECM TOE refers to this process as Delta.

The range of data types that can be collected on a given machine is maintained and controlled at the Collector by role based access control mechanisms. The list of data types that may be collected from Windows Agent Machines is contained in Table 24: Collected data types (default) for Windows based Clients.

Data types available for collection on Windows based systems include:

Accounts Policy	Event Log Settings	Event Log Events
Accounts	File System	Registry
Audit Policy	Groups	Security Policy
Disk Space	Machines	Services
Shares	User Rights	Machine Accounts

Table 24: Collected data types (default) for Windows based Clients

Data Consolidation for UNIX/Linux Agent Machines FDC_DTA.EXP.1b

The Configuresoft ECM UNIX or Linux Agent software is manually loaded onto the selected Agent machine in the same manner as the Window's Agent above (manual installation of agents is required for the Common Criteria Evaluated configuration). In the case of the UNIX installation, the UNIX listener is registered with the machine's inetd service and then the binaries are copied and registered.

Contact between the Collector and UNIX/Linux Agent Machines is established using the same methods described above for Windows based Agents. Secure Communications methods utilized are described in Section 6.1.3; UNIX/Linux machines utilize TLS for secure communications as DCOM is not supported for these machines.

Data types that may be collected from UNIX/Linux Agent Machines are listed in Table 25: Collected data types (default) for UNIX/Linux based Clients.

Separate subsystems within the TSF are invoked to execute activities on the UNIX/Linux Agent, however, the operation of the Collection and Secure Communication process is the same as detailed for the Window Agent.

Data types available for collection from UNIX/Linux based systems include:

Processes	System Initialization – Kernel Parameters	IP Info
Patches	System Logs- sulog	Services - Network
Disk Info	System Logs- syslog(-ng) Events & Settings	Services - Cron
System Initialization – Boot Parameters	Device Drivers (UNIX)	Services - RPC
System Initialization – Startup Scripts	File System	Groups (UNIX)
Installed Software	Exported Services	General Machine Data

Table 25: Collected data types (default) for UNIX/Linux based Clients

[1] ECM extracts the data from specific Machine configuration files. UNIX/Linux based systems have many security configuration parameters in specific system files. ECM parses the data from these configuration files and makes it available to the Administrator for assessment and change detection. For example: the file /etc/sudoers may contain information on users, which applications they are allowed to access and on which UNIX/Linux systems they can have access.

Data Consolidation for Active Directory Agent Machines FDC_DTA.EXP.1c

The Configuresoft ECM Active Directory Agent software is manually loaded onto the selected Agent machine in the same manner as the Window's Agent above (manual installation of agents is required for the Common Criteria Evaluated configuration). Data types that may be collected from Active Directory Agent Machines are listed in Table 26: Collected data types (default) for Active Directory based Clients.

Separate subsystems within the TSF are invoked to execute activities on the Active Directory Agent, however, the operation of the Collection and Secure Communication process is the same as detailed for the Window Agent.

Data types available for collection from Active Directory based systems include:

Schema / Classes*	Active Directory Objects: Contacts	Sites: Site Links
Schema / Attributes*	Active Directory Objects: Computers	Sites: Site Link Bridges
Schema / Class Attribute Map*	Active Directory Objects: Printers	Sites: Sub nets
GPO Objects	Active Directory Objects:	Sites: Inter-site Transports

	Shares	
Active Directory Objects: Users	Active Directory Objects: OUs	Sites: Servers
Active Directory Objects: Groups	Sites: Sites	Sites: Connections
Domains & Trusts: Domains	Domain Controller Configuration	Trusted Domains

* are gathered initially as part of "Administration -> Machines Manager -> Additional Components -> ECM for Active Directory -> Setup DCs" and then are gathered nightly as part of an ECM automatically created scheduled collection. This scheduled collection is driven from the application and differs from User Scheduled Collections which are excluded from the CC Evaluated Configuration.

Table 26: Collected data types (default) for Active Directory based Clients

6.1.5 Assessment

The Assessment Security Function provides the capability for Users on the ECM Collector to evaluate collected data stored within the CMDB (as detailed in the Data Consolidation Security Function Section 6.1.4) against criteria contained within a compliance template. This functionality allows users to utilize selectable criteria to determine the configuration, security status, and compliance of Agent machines by evaluating data contained within the CMDB.

Data Assessment and Analysis FDC_ANL.EXP.1

The Configuresoft ECM Collector performs compliance evaluations on CMDB data through the Web Console Machine interface, to determine if the configuration of Agent machines represented by the collected data set meets applicable standards for minimum security requirements. After the Administrator selects the applicable compliance template for evaluation, the Collector evaluates the data and returns the results using various reporting formats. The formats provided include Dashboards that allow the user to view reports in specific formats based on the information provided and subject matter and a column based format, Data Grid, which includes more detailed collected data. Users can navigate from the Dashboard view to the Data Grid view by double clicking on a data set, which deconstructs the data elements into the Data Grid that displays the collected entry.

Within each analytical result, the Collector returns the Date and Time of the result, the identification of the data source, identification of the User, the data type, Property Name, value expected (based on rule), value found and status or outcome of the analysis. This security function is supported through interactions between the Web Console (passes instructions and selections to the Collector), the Collector (executing requests against data in the CMDB database) and the CMDB.

6.1.6 Remediation

The Remediation Security function provides the capability for a Collector Administrator to initiate changes on Agent machines from the Collector machine. The basis for what data may require remediation is based on the Analysis provided in the Assessment Security Function Section 6.1.5 or based on Administrator review of CMDB data. Only manual remediation is supported for the Common Criteria Evaluated configuration.

Remediation of Data on Agent Machines FDC_REM.EXP.1

The TSF allows authorized Administrators to initiate changes on Windows Agent Machine configurations from the Web Console Machine through functionality provided by the applicable ECM Agent. Remediation actions taken on Agent Machines may either be based on the result of analysis techniques described in the Assessment Security Function or determination by the Administrator that a configuration change is needed to conform to the security policy in force for the deployment. Remediation occurs by selecting a data object from the CMDB database, selecting it for modification, entering the changed value and during the next synchronization between the Collector and the Agent the change instruction is sent to the Agent. The Collector, during the synchronization cycle, contacts the applicable Agent over a secure session and pushes the change to the Agent which implements it locally.

The following changes can be made through the Remediation security function by either selecting an icon on the Data Grid display or by right clicking on the applicable object on the Data Grid:

- Registry – Add Key, Delete Key, Add Value, Modify Value, Delete Value
- Change Password – Local Machine Accounts, Domain Accounts
- Windows Services – Start/Stop Services (configured for Automatic or Manual Startup)

The changes requested from the Collector are communicated to the Agent using the Secure Communications Security Function. The ECM Agent executes the changes based on the Collector Machine's instructions.

Any remediation actions executed result in an audit record being generated in both the Collector machine event log and the applicable Agent machine event log. If the remediation attempt is successful the Collector indicates this by creating a "Success" audit event. If the event was unsuccessful, the Collector audit record indicates a "Failure" audit event.

Remediation actions are executed by the Collector Services through jobs that are executed against CMDB data based on the Administrator's selections. As a result of remediation action taken against CMDB objects, configuration information is assigned to Jobs in a pool of threads. This results in file changes which are executed during the next synchronization between the Collector and Agent.

6.1.7 TOE Protection

Protection of the TSF FPT_RVM.1, FPT_SEP.EXP.1 (partial)

Protection of the TOE from physical and logical tampering is ensured by the physical security assumptions and by the domain separation requirements on the TOE and the IT Environment. The external interfaces of the TOE require that users be identified and authenticated by the Collector Environment and ensure users have a valid role within the TOE prior to accessing TSF resources. The TOE maintains a separate secure session for each interaction with the TOE.

The GUI, as the sole External Interface to the ECM Application, ensures that users must login prior to accessing the TOE from the Web Console. The only external interface that is user accessible is through the browser within the Web Console machine. Valid logon credentials must be entered, validated by the Collector Machine Operating System (in the IT Environment) and validated by the ECM application (TOE) as holding a valid account and role within the application.

Agents installed on network machines do not provide any external interfaces and may not be accessed from the Agent Machine directly. Agents only respond to requests and instructions from the Collector subsystem within the Collector machine and can only respond to requests through secure channels (DCOM or TLS). The Collector and Agent components of the TOE maintain a separate session for each Collector/Agent interaction.

Additional Agent protections which apply specifically to the UNIX & Linux agents include:

- Files and directories are owned by the ECM group, therefore, only members may access
- The HTTP “listener” process for accepting and executing Collector requests runs under a “nobody” type account with minimal privileges (this mitigates what can be done should a hacker take possession of the process)
- The awk script (used for interaction with the UNIX/Linux OS through command-line calls to gather requested data) is run as “root” only when necessary and at the last moment; “least privileged” approach

Agent protection relating to Windows/AD agents include:

- Runs under the established network authority permissions in ECM for that network resource
- Agent listener process uses the “least privilege”

6.1.8 ID & Authentication

The ID & Authentication Security Function provides the mechanism for Collector Administrator Users to be positively identified and authenticated prior to accessing Collector and CMDB TSF resources. The Collector machine Operating System (IT Environment) authentication

mechanism provides identification and authentication services to the ECM application.

The Administrative User accesses the ECM application on the Collector Machine from the Web Console machine in the IT Environment using a browser. Upon entering username and password credentials, the ECM Web App subsystem of the Collector machine passes the credentials to the Collector's Microsoft Windows Server 2003 Operating System for validation. Since the ECM user must also be administrators on the Collector machine, the User is first verified to be a Collector machine administrator and then, validated within the TOE as being an ECM user with an assigned role.

The TSF verifies the User as being an ECM Administrator by the Web App TOE subsystem accessing the token in the Collector Operating System and verifying the credentials against the ECM authorized users and role contained within the CMDB database subsystem. Security attributes are assigned to Users that are used for Data Access Control functions as specified in ECM Data Access Control.

ID & Authentication FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FMT_SMR.1

The Configuresoft ECM Collector Machine maintains the security attributes of Username (includes the Domain Name), the Configuresoft ECM assigned Role, and the Machine Group membership Associated with that Role. Machine Groups are described in Section 6.1.4. These attributes are used by the TSF to assign access control privileges to specific Administrative Users.

The Collector maintains the roles of Configuresoft ECM Administrator with full privileges for all functions, Windows ECM Administrator – allowing full access for all Window's based Agents & associated data, UNIX ECM Administrator - allowing full access for all UNIX/Linux based Agents & associated data, Active Directory ECM Administrator allowing full access for all Active Directory based Agents & associated data and ECM Read-Only which allows Read-Only access to all resources. The Configuresoft ECM Collector requires that users are identified by role prior to allowing any TSF mediated actions.

6.1.9 Security Management

The Security Management Security Function provides the Security Management functions for the Collector machine and CMDB resources. Various management functions are available to allow Administrators to Collect Data from Agent Machines, Evaluate data within the CMDB and initiate Remediation measures as required. Access to these functions is supported by the ECM Role based privileges established by ECM through the available ECM roles. Access to the Collector machine is exclusively through the Web Console machine in the IT Environment.

Security Management Functions provided by the ECM Collector Machine FMT_SMF.1

The TOE provides Security Management Functions that are implemented within the ECM Collector portion of the TSF. Security Management functions are accessed using a browser from the Web Console machine in the IT Environment. Upon being identified & authenticated by the TSF (through verification by the IT Environment), the Administrator can implement the Security Management functions of the TSF within the confines of the assigned roles. These include the

ability to review audit logs, conduct manual collections, review collected CMDB data, establish new accounts within ECM, User Role Assignments and associated permissions, and Evaluation/Remediation activities utilizing CMDB data. See 5.1.3 for a full listing of Security Management functions provided by the TOE.

Management of Security Function behavior within the ECM Collector FMT_MOF.1a, FMT_MOF.1b

The Configuresoft ECM TOE provides for the management of Security Functions through the ECM Collector subsystem. These management tools allow authorized Administrators to tailor the behavior of the security functions to the specific needs of a given deployment scenario. The TSF restricts the ability to enable or disable the Collector Service to any of the Administrative roles supported by ECM, excluding the ECM Read-Only role. Likewise, the TSF restricts the ability to modify behavior characteristics of the Data Consolidation, Collector Configuration, Rule Based Compliance Evaluation (Assessment) and Remediation functions to the Configuresoft ECM Administrator, Windows ECM Administrator, UNIX ECM Administrator, Active Directory ECM Administrator.

ECM Management of TSF data within the ECM Collector FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c, FMT_SMR.1

The ECM Collector provides tools to manage TSF data through the Web Console Machine that places restrictions on the ability to query, modify or delete data based on assigned roles in the TOE. The roles supported for the CC Evaluated Configuration have fixed access levels based on the needs of the user within the Collector Machine TSF subsystem. The supported roles are: Configuresoft ECM Administrator, ECM Read-Only, Windows ECM Administrator, UNIX ECM Administrator, and Active Directory ECM Administrator.

Within the Web Console Machine, the role of the Administrator user defines what options are available, displayed and enabled as described in ECM Data Access Control - FDC_RDR.EXP.1, Section 6.1.1. The role based access control mechanism, supporting the Security Management function, restricts the ability within the TOE to Query, Delete or Modify data to the Configuresoft ECM Administrator based on the type of TSF data accessed. Specific restrictions are detailed in Section 5 under FMT_MTD.1a, b, c.

Management of Network Authority Accounts

The ECM application utilizes Network Authority accounts to access the domains that the Agent machines are assigned. An account with domain Administrator rights is established that can apply to participating Agent machines in order for the Collector to be able to access Agents throughout the network. Once a Network Authority account has been established with Domain Administrator rights, it may be assigned to ECM NetBIOS domains, Active Directory domains or machine groups to be applied to all Agent machines that are part of the applicable domain or machine group. The Collector uses the applicable Network Authority account to connect to the Agent and thereby has Administrator rights to the Agent Machine Operating System.

6.2 Security Assurance Measures

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Components
ACM_CAP.3	The description of the configuration items is provided in EAL3 Configuration Management and Development Security Documentation: Configuresoft Enterprise Configuration Manager 4.10, Version 1.0.
ACM_SCP.1	The description of the TOE configuration items and evaluation evidence configuration items is provided in EAL3 Configuration Management and Development Security Documentation: Configuresoft Enterprise Configuration Manager 4.10, Version 1.0.
ADO_DEL.1	The description of the delivery procedures is provided in Common Criteria Supplement Secure Delivery Document: Enterprise Configuration Manager 4.10 EAL 3, Version 1.0.
ADO_IGS.1	The installation, generation, and start-up procedures are provided in: Configuresoft Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3, Version 1.1.
ADV_FSP.1	The informal functional specification is provided in EAL 3 Configuresoft ECM Design Documentation Functional Specification and Implementation Representation, Version 1.1.
ADV_HLD.2	The descriptive high-level design is provided in EAL 3 Design Documentation: High Level Design ADV_HLD.2 Configuresoft Enterprise Configuration Manager 4.10, Version 1.1.
ADV_RCR.1	The informal correspondence demonstration is provided in EAL 3 Configuresoft ECM Design Documentation Functional Specification and Implementation Representation, Version 1.1.
AGD_ADM.1	The administrator guidance is provided in the following documents: Configuresoft Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3, Version 1.1.
AGD_USR.1	N/A – The only authenticated users of the TOE are Administrator's therefore User Guidance separate from Admin. Guidance is not provided.
ALC_DVS.1	The development security measures documentation in provided in the following documents EAL 3 Configuration Management and Development Security Documentation: Configuresoft Enterprise Configuration Manager 4.10, Version 1.0.
ATE_COV.2	The evidence of coverage is provided in Tests Activity ATE Configuresoft Enterprise Configuration Manager 4.10 EAL 3, Version 1.1.
ATE_DPT.1	The functional testing of TOE subsystems in contained in Tests Activity ATE Configuresoft Enterprise Configuration Enterprise Configuration Manager 4.10, Version 1.1.
ATE_FUN.1	The functional testing description is provided in Tests Activity ATE Configuresoft Enterprise Configuration Manager 4.10 EAL 3, Version 1.1.

Assurance Requirement	Assurance Components
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_MSU.1	The Examination of Guidance is provided in Configuresoft© Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3, Version 1.1.
AVA_SOF.1	The strength of function analysis is N/A as the TOE does not include any permutational or probabilistic mechanisms.
AVA_VLA.1	The vulnerability analysis performed is provided in Enterprise Configuration Manager 4.10 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 3, Version 1.0.

Table 27: Assurance Requirements: EAL3

6.3 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.

	ECM Data Access Control	Security Audit	Secure Communications	Data Consolidation	Assessment	Remediation	TOE Protection	ID & Authentication	Security Management
FAU_GEN.2		**X**							
FAU_SAR.1		**X**							
FIA_ATD.1								**X**	
FIA_UID.2								**X**	
FMT_MOF.1a									**X**

	ECM Data Access Control	Security Audit	Secure Communications	Data Consolidation	Assessment	Remediation	TOE Protection	ID & Authentication	Security Management
FMT_MOF.1b									**X**
FMT_MTD.1a									**X**
FMT_MTD.1b									**X**
FMT_MTD.1c									**X**
FMT_SMF.1									**X**
FMT_SMR.1								**X**	**X**
FPT_ITT.1			**X**						
FPT_RVM.1							**X**		
FAU_GEN.EXP.1a		**X**							
FDC_ANL.EXP.1					**X**				
FDC_DTA.EXP.1a				**X**					
FDC_DTA.EXP.1b				**X**					
FDC_DTA.EXP.1c				**X**					
FDC_RDR.EXP.1a	**X**								
FDC_RDR.EXP.1b	**X**								
FDC_RDR.EXP.1c	**X**								
FDC_RDR.EXP.1d	**X**								
FDC_REM.EXP.1						**X**			
FPT_SEP.EXP.1							**X**		

Table 28: TOE Security Function to SFR Mapping

6.4 Appropriate Strength of Function Claim

The strength of function analysis is N/A as the TOE does not include any permutational or probabilistic mechanisms. Authentication mechanisms used for TOE access are provided within the IT Environment through the Collector Machine Operating System.

6.5 Rationale for Security Assurance Measures

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.3	EAL 3 Configuration Management and Development Security Documentation: Configuresoft Enterprise Configuration Manager 4.10, Version 1.0	The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ACM_SCP.1	EAL 3 Configuration Management and Development Security Documentation: Configuresoft Enterprise Configuration Manager 4.10, Version 1.0	The scope requirement for CM requires that the TOE implementation representation be included in the list of configuration items. Since this is a software-only TOE, the implementation representation consists solely of source and object code. Evaluation evidence required by the other assurance components in the ST also be included in the list of configuration items.
ADO_DEL.1	Common Criteria Supplement Secure Delivery Document: Enterprise Configuration Manager 4.10 EAL 3, Version 1.0	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.
ADO_IGS.1	Configuresoft© Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3, Version 1.1	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	EAL 3 Configuresoft ECM Design Documentation Functional Specification and Implementation Representation, Version 1.1	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADV_HLD.2	EAL 3 Design Documentation: High Level Design ADV_HLD.2 Configuresoft Enterprise Configuration Manager 4.10, Version 1.1	The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	EAL 3 Configuresoft ECM Design Documentation Functional Specification and Implementation Representation, Version 1.1	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.
AGD_ADM.1	Configuresoft© Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3, Version 1.1	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	*N/A*	Note: Product usage is transparent to network users therefore this requirement (AGD_USR.1) requirement is vacuously satisfied (ref: PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied).
ALC_DVS.1	EAL 3 Configuration Management and Development Security Documentation: Configuresoft Enterprise Configuration Manager 4.10, Version 1.0	The development security document describes practices in place to protect development data and intellectual property within the development facility.
ATE_COV.2	Tests Activity ATE Configuresoft Enterprise Configuration Manager 4.10 EAL 3, Version 1.1	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_DPT.1	Tests Activity ATE Configuresoft Enterprise Configuration Manager 4.10 EAL 3, Version 1.1	This requires testing be completed at the level of the subsystems, in order to demonstrate the presence of any flaws, provides assurance that the TSF subsystems have been correctly realized.
ATE_FUN.1	Tests Activity ATE Configuresoft Enterprise Configuration Manager 4.10 EAL 3, Version 1.1	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	Tests Activity ATE Configuresoft Enterprise Configuration Manager 4.10 EAL 3, Version 1.1	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.

Assurance Requirement	Assurance Measures	Assurance Rationale
AVA_MSU.1	Configuresoft© Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3, Version 1.1	The TOE Guidance documents are reviewed to assure secure procedures for all modes of operation have been addressed and that insecure states are easy to detect.
AVA_SOF.1	*N/A*	The strength of function analysis is N/A as the TOE does not include any permutational or probabilistic mechanisms
AVA_VLA.1	Enterprise Configuration Manager 4.10 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 3, Version 1.0	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 29: Rationale for Security Assurance Measures

7 Protection Profile Claims

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

8 Rationale

8.1 Security Objectives Rationale

Sections 4.3 - 4.6 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.7 - 5.13 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

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