National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Configuresoft

Enterprise Configuration Manager 4.10

Report Number: **CCEVS-VR-VID10176-2008**
Dated: **31 July 2008**
Version: **1.2**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Configuresoft Enterprise Configuration Manager 4.10, the Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is neither expressed nor implied.

The evaluation of the Configuresoft Enterprise Configuration Manager 4.10 product was performed by InfoGard Laboratories, Inc., San Luis Obispo, CA in the United States and was completed in April 2008. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004 Evaluation Assurance Level 3 (EAL 3) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2, January 2004.

The Configuresoft Enterprise Configuration Manager (ECM) Version 4.10 (hereafter referred to as the Configuresoft ECM) is a network software product that allows administrators to manage configuration control over Enterprise network resources. The Configuresoft ECM offers a scalable, cross platform solution to help customers effectively manage and control the configuration of Network resources from a centralized Administrator workstation.

The Configuresoft 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 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 the Configuresoft 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 Configuresoft 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. Configuresoft 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.

The following tables identify hardware and/or software components of the system and indicate whether each component is in the TOE or in the Environment.

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® Internet Explorer 6.0 or higher

Collector Machine

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

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

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

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

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

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)

Collector Machine

TOE or Env	Component Name	Description of Component
TOE	Enterprise Configuration Manager Revision 4.10	TOE Software package
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)

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 Cert. #240) DSSBASE, DSSENH Cert. #103 (2000) (selections are OS dependant)	Provides cryptographic services for securing Windows based Agent sessions. (operating non-FIPS)

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 Cert. #642)	Provides cryptographic services for the UNIX Agent (operating non-FIPS mode)

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 Cert. #642)	Provides cryptographic services for the Linux Agent (operating non-FIPS mode)

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 Cert. #103) DSSBASE, DSSENH	Provides cryptographic services for securing Windows Active Directory based Agent sessions. (operating non-FIPS)

It is important to note that the following components ***are included in the product but are 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
- 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 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

2 Identification of the TOE

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL pay a fee for their product's NIAP Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Configuresoft Enterprise Configuration Manager 4.10
Protection Profile	N/A
Security Target	Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL3, Version 1.1, June 27 2008
Dates of Evaluation	June 2006 – June 2008
Conformance result	EAL 3
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 2.2, January 2004
Common Evaluation Methodology (CEM) Version	CEM Version 2.2, January 2004
Evaluation Technical Report (ETR)	Evaluation Technical Report Configuresoft Enterprise Configuration Manager 4.10 for Windows, UNIX, and Active Directory, Document ID 08-955-R-0026, Version 1.1
Sponsor/Developer	Configuresoft, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Albert Chang, Kenji Yoshino, Phillip Bramwell
CCEVS Validators	Deborah Downs, Scott Shorter

3 Security Policy

The Security Functional Policies (SFPs) implemented by the Configuresoft Enterprise Configuration Manager 4.10 provide a mechanism so that only the identified/authenticated administrator has access to TOE resources, provides accountability for actions by logging security events, a protection mechanism that provides the security policies, and provides security assessment templates.

The Configuresoft Enterprise Configuration Manager 4.10 performs the following security functionality:

- 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.
- Security Audit
  - The Configuresoft ECM TOE generates audit events within the Collector machine to log TSF events by creating Windows Operating System events.
- 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.
  - The ECM TOE secures communication between the Collector Machine and Agent machines with using the DCOM or TLS protocol and leveraging the Microsoft Cryptographic module or the OpenSSL cryptographic module in the IT Environment.
- 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.
- Assessment
  - The Assessment Security function provides analysis capabilities through the TSF to evaluate data collected and compare it to compliance matrices.
- Remediation
  - The Remediation Security Function provides the ability for the TSF to initiate changes to the specific Windows configuration through the Administrator Console.
- TOE Protection
  - The Collector requires physical and logical protection to assure that TOE related security functions are not bypassed or altered.
- Identification & Authentication
  - The TOE requires that all users are successfully identified and authenticated prior

to gaining access to TSF resources.

- Security Management
    - The Security Management Security Function provides the Security Management functions for the Collector machine and CMDB resources.

4 Assumptions

4.1 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 Agent machine and placed in the CMDB for review.

4.2 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.

4.3 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.

4.4 Threats Countered and Not Countered

The TOE or IT environment addresses the security threats identified below:

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).

4.5 Organizational Security Policies

There are no applicable organizational security policies

5 Architectural Information

The Configuresoft ECM is broken into five components: Configuration Management Database (CMDB), Collector, Collector Machine Web App, Agent, and Crypto Module. The figure below depicts the TOE and the intended TOE environment.

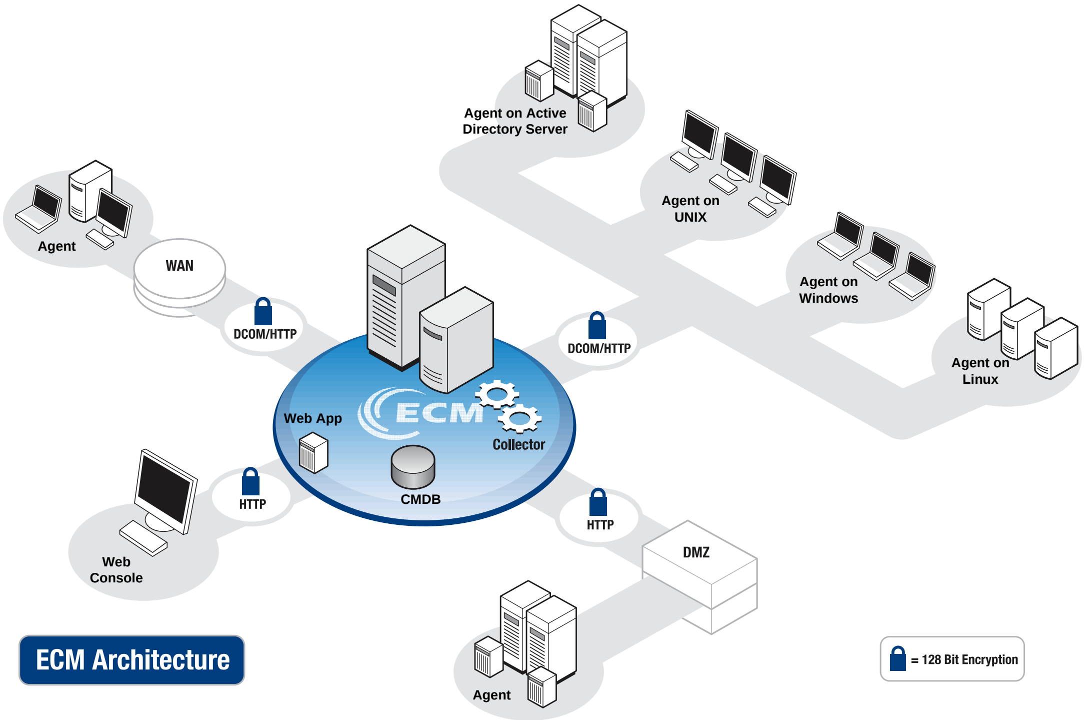

Figure 1: Configuresoft ECM Network Environment

5.1 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.

5.2 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 5.3 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 5.4 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 from 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.

5.3 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.

5.4 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.

5.5 Logical Boundaries

In terms of logical boundaries, the following table enumerates the division between services provided *by* the TOE:

Functional Area	**Services Provided *By* The TOE**	**Services Provided *To* The TOE By The Operating Environment**
ECM Data Access Control	The ECM Data Access Control Security Function provides Role based access control to collected data that resides within the CMDB.	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.
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.	TSF events and changes are stored using the IT Environment Event Log mechanism and protected through the Collector Operating System access control measures.
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.	None
Data Consolidation	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.	None
Assessment	The Assessment Security Function provides the capability for Users on the ECM Collector to evaluate collected data stored within the CMDB against criteria contained within a compliance template.	None
Remediation	The Remediation Security function provides the capability for a Collector Administrator to initiate changes on Agent machines from the Collector machine.	None
TOE Protection	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.	Valid logon credentials must be entered, validated by the Collector Machine Operating System in the IT environment.
ID & Authentication	The ID & Authentication Security Function provides the mechanism for Collector Administrator Users to be positively identified and authenticated prior to accessing	The Collector machine Operating System (IT Environment) authentication mechanism provides identification and authentication

	Collector and CMDB TSF resources.	services to the ECM application.
Security Management	The Security Management Security Function provides the Security Management functions for the Collector machine and CMDB resources.	Access to the Collector machine is exclusively through the Web Console machine in the IT Environment.

Table 1: TOE Security Functions

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Configuresoft Enterprise Configuration Manager 4.10. Note that not all evidence is available to customers.

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is *not* delivered is shown in a normal typeface.

The TOE is physically delivered to the end User. The guidance is part of the TOE components and is either delivered with the TOE or downloaded through the web.

6.1 Design Documentation

Document	Revision	Date
EAL 3 Design Documentation: High Level Design ADV_HLD.2 Configuresoft Enterprise Configuration Manager 4.10 (ADV_HLD.2, AVA_MSU.1)	1.1	June 27, 2008
EAL 3 Configuresoft ECM Design Documentation Functional Specification and Implementation Representation (ADV_FSP.1, ADV_RCR.1, AVA_MSU.1)	1.1	June 27, 2008

6.2 Guidance Documentation

Document	Revision	Date
ECM Installation and Getting Started Guide 4.10.0 (Getting Started Guide)	**ECMIGSG-04100-R1**	**January 18, 2008**
Configuresoft Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3 (AGD_ADM.1)	**1.1**	**June 27, 2008**
ECM Web App Console 4.10 (AVA_MSU.1)		
ECM Hardware and Software Requirements 4.9.0 (AVA_MSU.1)	**ECM_REQ_4.9.0.0**	**October 2007**

Document	Revision	Date
Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3 (ST)	1.1	June 27, 2008

6.3 Configuration Management and Lifecycle

Document	Revision	Date
EAL 3 Configuration Management and Development Security Documentation: Configuresoft Enterprise Configuration Manger 4.10 (ACM_CAP.3, ALC_DVS.1)	1.0	April 28, 2008
Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3 (ST)	1.1	June 27, 2008

6.4 Delivery and Operation Documentation

Document	Revision	Date
Common Criteria Supplement Secure Delivery Document: Enterprise Configuration Manager 4.10 EAL 3 (ADO_DEL)	1.0	April 28, 2008
Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3 (ST)	1.1	June 27, 2008

6.5 Test Documentation

Document	Revision	Date
Tests Activity ATE Configuresoft Enterprise Configuration Manager 4.10 EAL 3 (ATE_COV.2, ATE_DPT.1, AVA_MSU.1)	1.1	June 27, 2008
EAL 3 Design Documentation: High Level Design Configuresoft Enterprise Configuration Manager 4.10 (ADV_HLD.2, AVA_MSU.1)	1.1	June 27, 2008
EAL 3 Configuresoft ECM Design Documentation Functional Specification and Implementation Representation (ADV_FSP.1, AVA_MSU.1)	1.1	June 27, 2008
Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3 (ST)	1.1	July 27, 2008

6.6 Vulnerability Assessment Documentation

Document	Revision	Date
Enterprise Configuration Manager 4.10 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 3 (AVA_VLA.1)	1.0	April 28, 2008
Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3 (ST)	1.1	June 27, 2008
Configuresoft Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL3 (AGD_ADM.1)	1.1	June 27, 2008
EAL 3 Design Documentation: High Level Design ADV_HLD.2 Configuresoft Enterprise Configuration Manager 4.10 (ADV_HLD.2, AVA_MSU.1)	1.1	June 27, 2008

6.7 Security Target

Document	Revision	Date
Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3 (ST)	1.1	June 27, 2008

7 IT Product Testing

This section describes the testing efforts of the Developer and the evaluation team.

7.1 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. During the evaluation of the ATE_FUN.1, the evaluation team identified inconsistencies in the test cases and worked with the Developer to create accurate test cases. Inconsistencies included missing/misleading test procedures, ambiguous expected results, and inconsistent actual results.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 3. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

7.2 Evaluation Team Independent Testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team reran 30 of the Sponsor's test cases and specified additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

7.3 Vulnerability Analysis

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Vulnerability Analysis, the evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis, the evaluation team devised penetration testing (as listed in Table 3 above) to confirm that the TOE was resistant to penetration attacks performed by an attacker with an expertise level of average. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing. This resulted in a set of three penetration tests.

No vulnerabilities in the TOE were found during the final search of vulnerability databases after independent testing.

8 Evaluated Configuration

The evaluated configuration of the Configuresoft Enterprise Configuration Manager 4.10, as defined in the Security Target, consists of several components. P lease refer to Table 2-13 for the TOE's hardware and software components.

The Configuresoft Enterprise Configuration Manager 4.10 must be configured in accordance with the following Guidance Documents:

- Configuresoft Enterprise Configuration Manager 4.10 Common Criteria Supplement EAL 3 ,Version 1.0, April 28, 2008.
- ECM Installation and Getting Started Guide 4.10.0
- ECM Hardware and Software Requirements 4.9.0

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

InfoGard Laboratories has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 3 without augmentation. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in April 2008.

The Security Target did not claim conformance to a validated Protection Profile. The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

10 Validator Comments/Recommendations

The TOE makes use of cryptographic modules and algorithms in order to fulfill some security functions. The cryptography used in this product identified as FIPS 140-2 validated by the National Institute of Standards and Technology (NIST) has not been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

By default, when communicating with agent machines running Windows, the TOE uses the DCOM protocol to secure the connection. The details of that protocol are Microsoft proprietary information, and DCOM has not been evaluated by the CCEVS or CMVP to be a secure protocol. The validators recommend configuring the product to use TLS for Windows agents instead of DCOM.

11 Annexes

N/A

12 Security Target

Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3, Version 1.1, June 27, 2008.

13 Glossary

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 used to store detailed configuration information from Machines.

Crypto module: Refers to a logical subsystem abstraction that groups cryptographic software modules used within ECM to secure Agent/Console to Collector sessions.

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.

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.

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.

14 Bibliography

1.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 2.2, January 2004. CCIMB-2004-01-0001.

2.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 2.2, January 2004. CCIMB-2004-01-002..

3.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 2.2, January 2004. CCIMB-2004-01-003.

4.) Common Criteria Project Sponsoring Organisations. Common Criteria Common Methodology for Information Technology Security Evaluation. January 2004 CCIMB-2004-01-004.

5.) Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, January 2002.

6.) InfoGard Laboratories, Inc. Configuresoft Enterprise Configuration Manager 4.10 Security Target – EAL 3 Version 1.1, June 27, 2008

7.) InfoGard Laboratories, Inc. Evaluation Technical Report Configuresoft Enterprise Configuration Manager 4.10 for Windows, Unix and Active Directory, Version 1.1, July 30, 2008.