Security Target

For

Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages)

Assessment Engine Build 22212
Asset Manager Build 4974
Detect Server Build 3249
HostInfo – Windows (32 bit) Build 1875
HostInfo – Windows (64 bit) Build 1875
HostInfo – Mac Build 1793
HostInfo – Unix (Solaris and Red Hat) Build 1878

Version 2.1

July 30, 2010

Prepared For

Telos Corporation

Telos™ Advanced technology solutions that protect your vital assets™

Prepared By

CYGNACOM SOLUTIONS

7925 Jones Branch Drive♦Suite 5400 ♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

Security Target for Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8

Security Target for Xacta® IA Manager: Assessment Engine and
Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8

Table of Contents

Section
Page

Table of Tables and Figures

Table / Figure **Page**

Security Target for Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8

1 Security Target Introduction

1.1 Security Target Reference

ST Title:	Security Target for Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages)
ST Version:	Version 2.1
ST Date:	July 30, 2010
ST Author:	CygnaCom Solutions, Inc.

1.2 TOE Reference

TOE Identification:	Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages) Assessment Engine Build 22212 Asset Manager Build 4974 Detect Server Build 3249 HostInfo – Windows (32 bit) Build 1875 HostInfo – Windows (64 bit) Build 1875 HostInfo – Mac Build 1793 HostInfo – UNIX (Solaris and Red Hat) Build 1878
TOE Vendor:	Telos Corporation

1.3 TOE Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Xacta IA Manager: Assessment Engine and Xacta IA Manager: Continuous Assessment, V4.0 Service Pack 8 (Commercial and Government Distribution Packages) product, formerly called Xacta IA Manager Enterprise Edition.

The Target of Evaluation (TOE) is being evaluated at assurance level EAL2 augmented with ALC_FLR.2.

The TOE is Xacta IA Manager: Assessment Engine and Xacta IA Manger: Continuous Assessment V4.0 Service Pack 8 (Commercial and Government Distribution Packages). The entire TOE will be referred to as Xacta IA Manager in this ST. The TOE is comprised of the Xacta IA Manger: Assessment Engine and Xacta IA Manger: Continuous Assessment Components (these components will be referred to as the Assessment Engine and Continuous

Assessment in this ST) and includes both the Government and Commercial Distribution Packages that are purchased separately.

Xacta IA Manger is a continuous risk management framework that manages and supports IT security risk and compliance assessment activities for an organization. The TOE includes a knowledge base which contains templates, workflow tasks, process steps, and test scripts. It provides a mechanism to walk customers through the steps to collect data from an enterprise's assets (which may include physical security, organizational procedures and processes, personnel, physical IT assets, etc.), evaluate risk and compliance to a requirement, and publish a pre-formatted document(s) that would then be submitted to the appropriate DAA (Designated Approving Authority) for the organization.

The TOE provides the following security functionality: auditing of security relevant events, TOE user account administration, ability to add a signature to published reports and assessment scripts as proof of origin, TOE user identification and authentication, security role based access to management functions, trusted channel communication between components, and risk and compliance assessment support functions.

Note: The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient is not part of this evaluation.

The product may be purchased by contacting the vendor directly or using one of the contract vehicles listed on their website contracts page: http://www.telos.com/contracts/buy/. The end user will need to indicate that the NIAP Certified version is required when purchasing. The customer will be given instructions on how to download the NIAP certified version which is packaged with the vendor documentation and the CC supplement. Upon special request, Telos will create a DVD and send to the customer.

1.3.1 TOE Type

Xacta IA Manager is a software application for IT security risk and compliance assessment support and management (also known as Governance, Risk and Compliance (GRC)). The TOE is a software-only TOE.

1.3.2 Hardware/Firmware/Software Required by the TOE

This section is to identify any hardware, firmware, or software that is required for the TOE to operate. This listing only includes those pre-installation requirements for the TOE components. Additional Operational Environment (OE) support that is optional, such as LDAP servers, SMTP server, and/or vulnerability scanners is identified later in the Section. None of the objects identified below are in the scope of the TOE.

The TOE requires the following hardware/software environment support in addition to the network infrastructure:

- The following software is required to be pre-installed on the **Xacta IA Manger: Assessment Engine's (AE)** server host platform (minimum recommendation: 2 GB RAM, 120 GB Hard Drive):
  - MS Windows XP / Server 2003 / Vista
  - MS Office XP / 2003 / 2007 (MS Word)
  - MS SQL Express 2005 / MS SQL Server 2000 SP4/2005 / Oracle 8i/9i/10g

    Note: A copy of MS SQL Express 2005 is included with the AE product media. The TOE's installation wizard allows the user to specifically select this version to be installed during the process or select the use of one of pre-installed databases list above. In either circumstance, the user must update the databases separately from the TOE. Xacta does not supply updates/patches for the MS SQL Express 2005 version supplied on the product media or any of the optional databases.
  - MS .NET 2.0 (minimum)

    Note: This version is included with the AE product media. If the installation wizard finds a version of MS .NET 2.0 or higher already installed on the server, it will not overwrite it.
- The **Assessment Engine GUI (aka Dashboard), Asset Manager GUI, and Detect Server GUI** will be presented on a separate machine and is referred to as the Administrative Console.

  The following software must be pre-installed on the Administrative Console:
  - An operating system that can support the software listed below
    - Internet Explorer 6.0 (or greater)/ Netscape Navigator 7.0 (or greater) or equivalent browser capable of supporting SSL communications.
    - .doc file and .xls file readers (e.g. MS Word, MS Excel, OpenOffice)
    - .pdf file reader (e.g. Adobe Acrobat– version 5.0 or later)
    - Java Runtime Environment (JRE)
    - Card Reader for Common Access Cards (CAC) (optional) (ActivCard/ActivIdentity)
- The following software is required to be pre-installed on the **Xacta IA Manger: Continuous Assessment's (CA)** server host platform (minimum recommendation: 4 GB RAM, 120 GB Hard Drive).
  - MS Windows XP / Server 2003 / Vista
  - MS SQL Express 2005 / MS SQL Server 2000 SP4/2005 / Oracle 8i/9i/10g

  Note: A copy of MS SQL Express 2005 is included with the CA product media. The TOE's installation wizard allows the user to specifically select this version to be installed during the process or select the use of one of pre-installed databases list above. In either circumstance, the user must update the databases separately from the TOE. Xacta does not supply updates/patches for the MS SQL Express 2005 version supplied on the product media or any of the optional databases.
  - Winpcap driver 4.1.1

Note: The Winpcap driver is provided with the CA product media. The customer must pre-install this driver and use the version included with the CA product. This must be not be updated by the customer. Updated Winpcap drivers must undergo integration testing with the TOE.

- The following software is required to be pre-installed on the The **Xacta HostInfo Agent's** host platform (network client) pre-installed with one of the following operating systems:
  - MS Windows 2000 / XP / 2003 / Vista, Mac OS X and/or Unix (Red Hat Enterprise Server 4.0, Solaris 10)

1.4 TOE Description

1.4.1 Acronyms

The following two tables define product specific and CC specific acronyms respectively.

Table 1-1: Product Acronyms

Acronym	Definition
ACI	Access Control Item
C&A	Certification and Accreditation
CA	Certificate Authority
CAC	Common Access Card
CLI	Command Line Interface
CMU	Certificate Management Utility
CRL	Certificate Revocation List
CSC	Customer Service Center
DAA	Designated Approving Authority
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocols over SSL
I&A	Identification and Authentication
ID	Identifier
IP	Internet Protocol
IT	Information Technology
JRE	Java Runtime Environment
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
PDF	(Adobe) Portable Document Format
PKI	Public Key Infrastructure
RDBMS	Relational Database Management System
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer

Acronym	Definition
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
XASL	Xacta Automated Script Language
XML	Extensible Markup Language

Table 1-2: CC Acronyms

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

1.4.2 Terminology

The following two tables define product-specific and CC-specific terminology respectively.

Table 1-3: Product Terminology

Term	Definition
Agent	a HostInfo subsystem installed on a system on the target network that will automatically collect asset data (part of the Continuous Assessment Upgrade)
Notification	a notification sent to the individual assigned to a project role upon the occurrence of a designated project event
Artifact	an object, such as a file or a link to a Web site or Web document, that is included for reference within projects
Asset	any device connected to the target network with an IP address that is assessed by the TOE for risks and compliance to security standards
Checklist	a high-level evaluation tool that can be used to quickly assess the overall compliance of a system
Folder	a logical grouping of projects
Housekeeping	background system maintenance performed by the TOE at an administrator scheduled time
JavaScript	JavaScript is an implementation of the ECMAScript language standard, implemented as part of a web browser in order to provide enhanced user interfaces and dynamic websites. “JavaScript" is a trademark of Sun Microsystems.
Keystore	a java file containing a trusted certificate and private key
Knowledge Base	the policies, regulations, requirements, test procedures, vulnerabilities, and scripts needed by the TOE which are stored and updated
Process Step	a key step within the assessment process; a component of a task

Term	Definition
Project	the representation of a system assessment effort; used to define the system, determine the requirements that must be complied with (template), gather system data, test the system, determine the overall level of compliance and the resulting risk, and prepare the documentation that will be submitted to the appropriate authorities for approval to operate
Project Role	a set of project duties assigned to an individual
Publishing	the process of compiling the data gathered from a project's process steps and exporting it to properly formatted documents
Scan Job	the automatic monitoring, updating, and testing of a project's devices and equipment on a regular, recurring basis (part of the Continuous Assessment Upgrade)
Snapshots	backup copies of a project that can be used to restore the project to an earlier state
Task	a stage in the assessment process; a component of a project (selected template)
Template	the collection of work tasks that comprise a particular set of requirements; these tasks comprise the steps needed to gather and evaluate the asset data and publish documents; the templates are named after government and commercial standards that the product supports
Velocity Scripts	Velocity is a Java-based template engine. It can be used as a standalone utility for generating source code, HTML, reports, or it can be combined with other systems to provide template services.

Table 1-4: CC Terminology

Term	Definition
Authorized User	A user who may, in accordance with the TSP, perform an operation.
External IT Entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Identity (ID)	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Security (Administrative) Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

1.4.3 Product Description

Xacta IA Manager is a continuous risk management framework that manages and supports IT security risk and compliance assessment activities for an organization. The TOE includes a knowledge base which contains templates, workflow tasks, process steps, and test scripts. It provides a mechanism to walk customers through the steps to collect data from an enterprise's assets (which may include physical security, organizational procedures and processes, personnel, physical IT assets, etc.), evaluate risk and compliance to a set of controls/requirements, and publish a pre-formatted document(s) that would then be submitted to the appropriate AO/DAA (Authorizing Official/Designated Approving Authority) of the organization.

Xacta IA Manager provides two types of templates:

- **Project templates**. Project templates are based on a known assessment method, such as DCID, DIACAP, DITSCAP, NIST, COBIT, or ISO 27001. These templates

include process steps that enable users to perform a certification/assessment and produce the appropriate documentation. Project templates are compatible with the Service Pack identified in their title or in the Customer Support Center Web site.

- **Content-only templates**. These templates provide access to a new regulation that has not been added to the standard list of project templates. These templates have the word "Content" in the title with no specific version. Administrators have the ability to restore the Content-only templates and then copy from the content template into their current project, and begin to use the new regulations/test procedures.

Note: The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient is not part of this evaluation.

Active Update is used to update the product's knowledge base of policies, regulations, requirements, test procedures, vulnerabilities, and scripts and can be used to download new content either automatically or on command. Active Update can be configured to retrieve updated content automatically on a configured schedule or manually on administrator command. Active Update is disabled by default. The administrator must enter an Installation Key at configuration which is required to verify and authorize Active Update to retrieve content from the update server and an optional Certificate Distinguished Name parameter allows a certificate validity check.

SCAP Content Update is used by the product to download new and up-to-date CVE (Common Vulnerabilities and Exposures), CCE (Common Configuration Enumeration), and CPE (Common Product Enumeration) data. As with Active Update, SCAP Content Update is disabled by default and may be configured to retrieve data either automatically or manually. When enabled:

- CVE data is downloaded from the NVD database at http://static.nvd.nist.gov/feeds/xml/cve/
- CCE data is downloaded from the CCE dictionary dataset at http://cce.mitre.org/lists/data/downloads/
- CPE data is downloaded from the NVD database at http://nvd.nist.gov/cpe.cfm/official-cpe-dictionary_v2.1.xml

These updates can also be imported from another location such as a memory stick or hard drive. Manual and automatic updates are included in the scope of the TOE.

The three types of SCAP data retrieval can be enabled and disabled separately.

The TOE can be purchased as either a commercial or government package. The government package contains the TOE as defined in this document along with a folder of government standard templates. The commercial package contains the TOE as defined in this document and a folder of commercial templates. The TOE is the same in both the commercial and government package. Some additional commercial templates can be purchased separately. There are additional government standard templates which require additional information from the customer. The evaluated configuration will include tests for both the government and commercial templates.

Xacta IA Manager: Assessment Engine (Assessment Engine) and *Xacta IA Manager: Continuous Assessment (Continuous Assessment)* are two separate components of the Xacta

IA Manager V4.0 SP8 framework. These two components are separately licensed and are included in the scope of this evaluation. There is a third separately licensed component of the framework called Xacta IA Manager: Process Enforcer. The Process Enforcer is used to automate, enforce and verify remediation processes, is not included in the TOE.

The TOE's components and external interfaces are shown in Figure 1 below. Xacta technologies are database driven Web applications that are supported by Tomcat/Apache web services and the Java Runtime Environment (JRE) that is packaged with the product. The supplied Tomcat/Apache and JRE are installed by the TOE's installation process and are instantiations that are only available for the TOE's use.

The TOE is intended to be operated in a system high environment where all data is controlled to the highest level of security classification assigned to the operating environment.

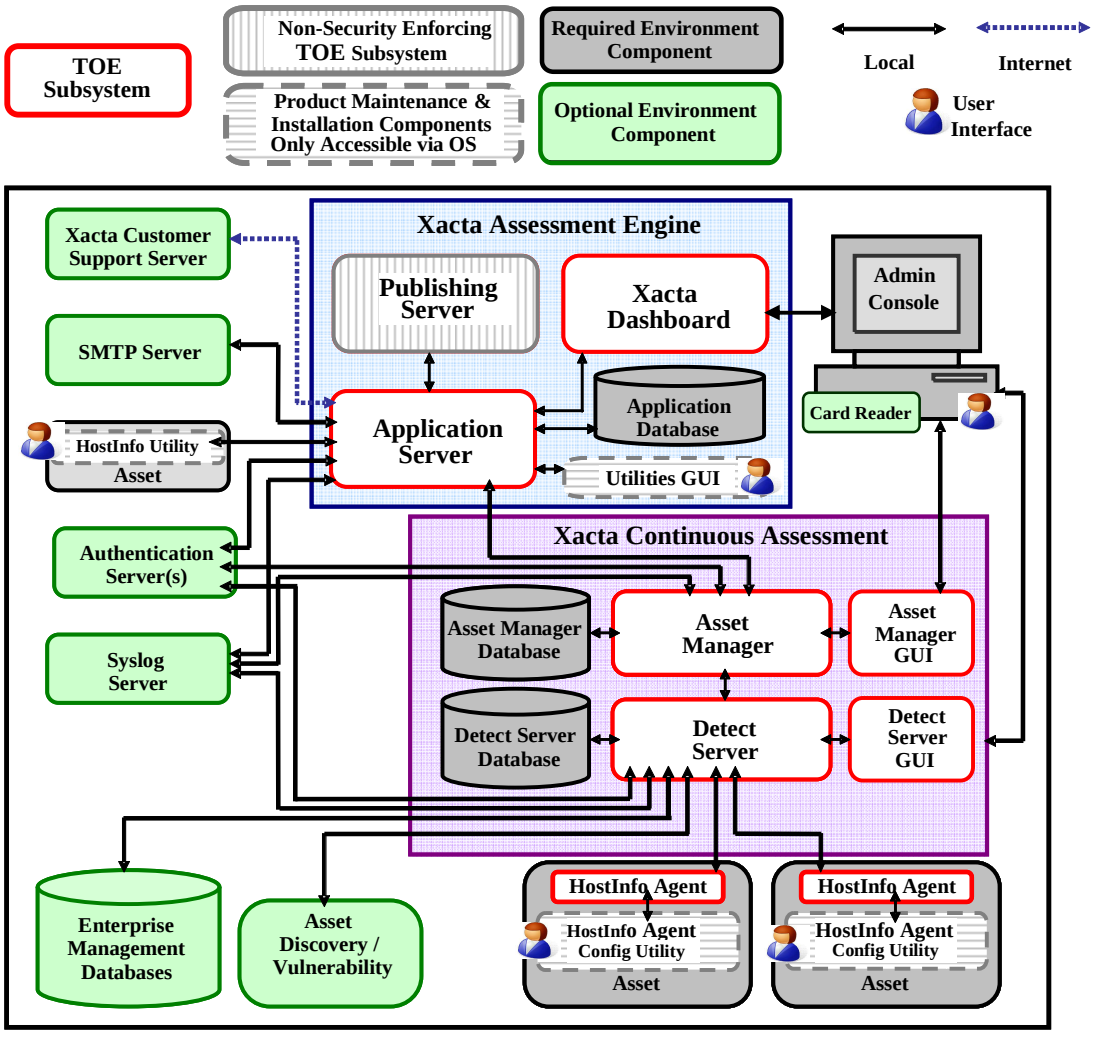

Figure 1: Xacta IA Manager: Assessment Engine and Xacta IA Manager: Continuous Assessment Components and Interfaces

The evaluated configuration of the TOE covers both the standalone deployment (AE and CA components installed on one machine) AND standard network deployment (AE separately installed from CA components). Pictured above is the standard network deployment.

1.4.3.1 Xacta IA Manager: Assessment Engine (Assessment Engine)

The Assessment Engine (AE) component consists of software designed to facilitate IT security risk and compliance assessment business functions, such as supporting the data collection and document publishing for a Certification & Accreditation approval process. It consists of the following subsystems described below.

1.4.3.1.1 AE Security Enforcing TOE Subsystems:

1.4.3.1.1.1 Assessment Engine Application Server (Application Server)

The Application Server subsystem provides the core business logic of the application. As such, all other Xacta IA Manager subsystems communicate with the Application Server. The Application Server analyzes the collected IT network asset information and calculates risk and compliance with the requirements derived from the administratively selected template.

The following steps summarize the basic Xacta IA Manager workflow:

1) A project is started with the selection of a template
2) The project's tasks are assigned to individuals who have designated roles
3) The collection and assessment tasks are performed (either automatically and/or manually)
4) Documents are published from the resulting task data for the project
5) The operational environment of the project can then be continuously monitored, updated, and re-assessed for deviations

The Application Server maintains data in a centralized database (Application Database). This data includes:

- an organization's baseline risk posture and configuration information
- TOE user account information, audit records, and system configuration data
- snapshots that are backup copies of a project that can be used to restore the project to an earlier state
- published documents

The Application Database's records are automatically updated when a risk element file is imported.

The database instance (schema and initial data) is created inside a third-party RDBMS during installation. The RDBMS's I&A decision and enforcement, access control functionality, and interfaces, though used by the TOE, are not controlled by the TOE and are considered part of the OE.

An encrypted SSL channel is required for communications between the Application Server and the database even if they are installed on the same server. The database must be specially configured to enable this encryption.

The following third party subsystems (not shown in figure above) are included on the AE product installation media and are considered part of the AE component:

- Tomcat 5.5.27
- JRE 6 update 13
- iReasoning SNMP Subagent Service v1
- Bouncy Castle 1.40 (used for certificate revocation checking)
- RSA BSafe Crypto-J v3.6 (JSafe and JCE)

Note: The supplied Tomcat/Apache and JRE are installed by the TOE's installation process and are instantiations that are only available for use by the TOE and must not be upgraded by the customer.

1.4.3.1.1.2 Xacta Dashboard (Dashboard)

The Dashboard is a web based graphical user interface through which all the Assessment Engine's management functions are accessed. This interface is only accessible to AE account holders. The Dashboard is accessed with a SSL/TLS enabled standard web browser, such as Internet Explorer. The Dashboard consists of server-side application software.

1.4.3.1.2 AE Non-Security Enforcing TOE Subsystems:

1.4.3.1.2.1 Publishing Server (Publishing Server or Publisher)

The Publisher Server does not make security relevant decisions or enforce any security functionality. Therefore, it is considered a non-security relevant component and is included only for completeness.

The Publishing Server is used by Assessment Engine to generate C&A documentation. It produces documents in either Adobe portable document format (.pdf) or Microsoft Word format (.doc). The final documentation package can then be submitted to a Designated Approving Authority (DAA).

Publishing is the process of inserting the data gathered from the project's collection steps into the pre-formatted template (that corresponds to the selected project). The template consists of an XML document with Velocity script information embedded. Velocity is a Java-based template engine. Template information is saved as an attribute for each process step within Assessment Engine. When a publishing action is requested, the Publisher service parses/interprets the XML documents and Velocity scripts and converts the information into a Microsoft Word document, and then is converted into a .pdf document, if a .pdf document was selected as the final output.

The Publisher can currently be implemented on Windows platforms only.

Note: Customizing the report templates (i.e editing/coding of the Velocity scripts) is a functionality that is excluded from the Logical Scope of the TOE.

1.4.3.1.3 AE Product Subsystems Not Included in the TOE:

The following subsystems are product utilities used only by customers during the installation, initial configuration, and maintenance of the TOE. They are not used during the run-time operation of the TOE and their functionality is not part of the TOE Security Functionality. Users of these utilities must have physical access to the platform on which they are installed. Identification and authentication of users of these utilities is done by the OS of the platform. The TOE does not audit use of the utilities.

1.4.3.1.3.1 Xacta HostInfo Utility (HostInfo Utility)

The HostInfo Utility is used to manually retrieve host information from Windows assets that cannot run the HostInfo Agent. Data obtained by the HostInfo Utility can be saved to a file, zipped, and imported into Assessment Engine's Equipment Inventory process step.

To use the HostInfo Utility, it must be copied to a floppy disk or portable storage device (or accessed from a shared network location) and then executed on each Windows machine, individually. The data gathered by the utility can be output to an XML file which must be zipped and then manually imported into Assessment Engine's Equipment Inventory process step.

The HostInfo Utility is executed from the target machine's command prompt. Therefore, the HostInfo Utility user must have physical access and a login account on the target machine's OS. To operate the HostInfo Utility requires a file containing test scripts that were exported from the Asset Manager's script library to be executed.

1.4.3.1.3.2 Xacta Utilities GUI

This utility is automatically installed during installation and can be accessed from the Windows task bar under *Start* > *Programs* > *Xacta* > *Xacta Utilities*. The Xacta Utilities GUI user must have physical access to the Assessment Engine server and a login account on the server's OS. The main utility screen provides access to the utilities associated with each of the installed components and subsystems. The following utilities are available through the GUI:

- **Application File Digest Checker Utility**

  This utility calculates the checksum for the program files and then compares the results with a list from Xacta or with previous scan results generated by the utility to enables customers to verify the authenticity and integrity of their Xacta software.

- **Certificate Management Utility**

  The Certificate Management Utility (CMU) helps create and manage Java-standard keystores, their private keys, and certificates. This includes the ability to generate self-signed certificates, import existing certificates and key pairs, and migrate a certificate, and replace a self-signed certificate with one duly signed by a trusted Certificate Authority (CA).

- **Database Management Utility**

  The Database Management Utility is exclusive for the Assessment Engine. This utility lets customers perform entire backups, restore from backups, and update the password encryption for the database.

- **Publisher SNMP Utility**

The Publisher SNMP Utility allows customers to configure the TOE's SNMP subagent to report to a master SNMP agent.

- **Web Server Configuration Utility**

  The Assessment Engine Web Server Configuration Utility lets customers switch between Non-SSL and SSL protocol and change the URL of the Assessment Engine Web server.

1.4.3.2 Xacta IA Manager: Continuous Assessment (Continuous Assessment)

The Continuous Assessment (CA) component is a set of integrated subsystems designed to automate risk and compliance assessment business functions. It includes the subsystems described below.

1.4.3.2.1 CA Security Enforcing TOE Subsystems:

1.4.3.2.1.1 Xacta Asset Manager (Asset Manager)

The Asset Manager is a service that enables the management of an enterprise's IT network assets. It is a Web-based application that automatically collects and updates data about network devices, creates and maintains an asset inventory, tests asset configurations and vulnerabilities, and generates detailed reports. The Asset Manager provides the Assessment Engine with up-to-date host and vulnerability data as part of the assessment process.

The Asset Manager maintains data in its own database instance (Asset Manager Database) consisting of collected asset information, script results, and data from third-party asset discovery/vulnerability scanners for assets in its associated Detect Server(s) specified IP Range.

1.4.3.2.1.2 Xacta Detect Server (Detect Server)

The Detect Server is responsible to manage a configured set of assets (hosts with HostInfo agents). When the Asset Manager Server has a task, it sends it to the appropriate Detect Server.

Depending on the type of task to be performed, the Detect Server either executes it by itself or forwards it to the correct HostInfo Agent(s). When the task is complete, the Detect Server passes the information back to the Asset Manager Server.

Detect Servers can perform network discovery scans or request data from third-party enterprise management tools such as Microsoft SMS, IBM Tivoli, ISS Site Protector, eEye REM, and Nessus. Detect Servers can request detailed equipment scans and vulnerability tests from HostInfo Agents.

Each Detect Server can only perform scans on equipment within its specified IP Range and will only accept HostInfo Agents within this range. The IP Range limit is specified when the Detect Server is configured. Multiple Detect Servers may be configured to be used in a single installation.

Each Detect Server maintains data in its own database instance (Detect Server Database) consisting of collected asset information, script results, and data from third-party asset

discovery/vulnerability scanners for assets in the Detect Server's specified IP Range. Each Detect Server's database records are replicated within the Asset Manager Database on a near real-time basis. The synchronization of this data is a function of the Asset Manager and Detect Server subsystems.

The Continuous Assessment databases (Asset Manager Database and Detect Server Databases) are similar in implementation to the database used by the Application Server. These are two database instances (schema and data) inside a third-party RDBMS. This RDBMS, the I&A and access control functionality it provides, and its interfaces, though used by the TOE, are not controlled by the TOE. Therefore, the I&A and access control functionality to the third-party RDBMS are specified in the OE objectives.

The following third party subsystems (not shown in figure above) are included on the CA product installation media and are considered part of the CA component:

- Tomcat 5.5.27
- JRE 6 update 13
- iReasoning SNMP Subagent Service v1
- Bouncy Castle 1.40 (used for certificate revocation checking)
- RSA BSafe Crypto-J v3.6 (JSafe and JCE)

Note: The supplied Tomcat/Apache and JRE are installed by the TOE's installation process and are instantiations that are only available for use by the TOE and must not be upgraded by the customer.

1.4.3.2.1.3 Asset Manager and Detect Server GUIs

The Asset Manager and the Detect Servers each have their own associated web based graphical user interface used by all AM and DS account holders for administration purposes. These GUIs act similarly to the Dashboard. The management functions and information displayed in each pertain only to the appropriate Asset Manager or Detect Server. Only AM account holders can gain access to the AM GUI and only DS account holders can gain access to the DS GUI.

The Asset Manager and Detect Server GUIs are accessed with a SSL/TLS enabled standard web browser, such as Internet Explorer. Each Asset Manager and Detect Server GUI has its own individual web pages and a unique URL.

1.4.3.2.1.4 Xacta HostInfo Agent (HostInfo Agent)

A HostInfo Agent is an application that resides on a host computer (IT network asset). The agent is designed to collect detailed data about its host and transmit it back to the Detect Server using encrypted Secure Sockets Layer (SSL) protocol. The agent can also run tests on its host.

Agents are designed to periodically contact the Detect Server to see if updated information is required about the agent's host. If updated information is required, the agent performs the Detect Server's requested task, passes the resulting information back to the server, and returns to idle mode.

HostInfo Agents produce a log file that can be configured and read through the OS utilities of its host. This log file is used for diagnostics and debugging and is not considered part of the security audit log definition.

1.4.3.2.2 CA Product Subsystems/Components Not Included in the TOE:

The following subsystems are product utilities used only by customers during the installation, initial configuration, and maintenance of the TOE. They are not used during the run-time operation of the TOE and their functionality is not part of the operational TOE Security Functionality. Users of these utilities must have physical access to the platform on which the utilities are installed. Identification and authentication of users of these utilities is done by the OS of the platform. The TOE does not audit use of the utilities.

1.4.3.2.2.1 HostInfo Agent Configuration Utility

This utility provides a graphical user interface that allows customers to start and stop agents, view agent logs, and configure all major agent properties. This utility is installed on each asset as part of the agent installation.

1.4.3.2.2.2 Xacta Utilities GUI

The Xacta Utilities GUI is also available on the Asset Manager Server in a distributed configuration. The Xacta Utilities GUI user must have physical access to the Asset Manager Server and a login account on the AM server's OS. See Section 1.4.3.1 for details:

1.4.4 Data

All TOE data is TSF data and includes:

- The System Parameters set by Administrators to configure the security of the TOE
- TOE User Account data
- Asset System Data collected by the HostInfo Utilities and Agents
- Published Compliance Documents
- Vulnerability and Non-Compliance Assessment data
- Government, Commercial and User Created Templates
- Government, Commercial and User Created Test Scripts

1.4.5 Users

All users of the TOE have access to TSF data and management functions and therefore all are considered administrators. The data and management functions that can be accessed are determined by the account type (security role) and the folders, projects and IP address ranges assigned to that individual's account.

TOE users are authenticated by the TOE for use of the Dashboard (Assessment Engine GUI), Asset Manager GUI and Detect Server GUI. These are three separate authentication processes. A user who successfully logs in to one of the management GUI is not automatically authenticated to use the other two.

Note: Users of the HostInfo Agent Configuration Utility, HostInfo Utility and Xacta Utilities GUI are not considered TOE users. They are identified and authenticated by the OS of the utility's host platform which is considered part of the OE.

1.4.6 Cryptographic Functions

The following table summarizes the TOE's use of cryptographic functions:

Table 1-5: TOE Cryptographic Functionality

TOE Operation	Cryptographic Functionality	Cryptographic Functionality Provider	Reference	FIPS Certified?
Local Password Storage	SHA1 Password Hash	RSA BSafe Crypto-J JSafeJCE	RFC 3174	Yes Cert 355
PKI Authentication	X.509 Certificate Authentication	Client: Browser Crypto Module or Hardware Module embedded in Common Access Card	RFC 5280	No
		Server: RSA BSafe Crypto- J		Yes
OCSP Revocation Checking	Certificate Revocation Checking	Bouncy Castle	RFC 2560	No
External Authentication Server Data Storage	Symmetric-Key Encryption using PBEWithMD5andDES	RSA BSafe Crypto-J	RFC 2898	Yes
3rd Party Application Password Storage	Symmetric-Key Encryption using PBEWithMD5andDES	RSA BSafe Crypto-J	RFC 2898	Yes
Data transmitted between AE and Publisher	Symmetric-Key Encryption using PBEWithMD5andDES	RSA BSafe Crypto-J	RFC 2898	Yes
Communications between TOE Components	TLS V1 (SSL V3.1) via FIPS 140-2 Validated Ciphers	RSA BSafe Crypto-J	RFC 2246	Yes
Communications between TOE and External Servers	3DES 128 bit, AES 128 bit, or AES 256; SSL V3.1 or TLS V1	RSA BSafe Crypto-J	RFC 2246	Yes
Communications between TOE and Xacta Customer Support Server	HTTPS/SSL V3.1	RSA BSafe Crypto-J	RFC 2246	Yes
Communications between TOE and network assets	HTTPS/SSL V3.1 or TLS V1	RSA BSafe Crypto-J	RFC 2246	Yes

TOE Operation	Cryptographic Functionality	Cryptographic Functionality Provider	Reference	FIPS Certified?
Project Backup and Restore	3DES Encryption/Decryption (MD5 for backwards compatibility on restore only)	RSA BSafe Crypto-J	NIST Special Publication 800-67	Yes
Digital Signatures for Test Scripts	Asymmetric-Key Encryption using SHA1WithDSA, SHA256WithRSA to create Digital Signatures via:	Browser Crypto Module or CAC Hardware Module		No
	1. Soft Certificate Private Key (PKCS8) stored in a Java Keystore File (JKS)		RFC 5208	
	2. Common Access Card (PKCS11)		http://www.rsa.com/rsalabs/node.asp?id=2133	
	3. Personal Information Exchange Syntax Standard (PKCS12) -.pfx or .p12 file format		http://www.rsa.com/rsalabs/node.asp?id=2138	
Digital Signatures for Documents and Reports	Asymmetric-Key Encryption using SHA1WithDSA, SHA1WithRSA to create Digital Signatures via:	Browser Crypto Module or CAC Hardware Module		No
	1. Common Access Card (PKCS11)		http://www.rsa.com/rsalabs/node.asp?id=2133	
	2. Personal Information Exchange Syntax Standard (PKCS12) -.pfx or .p12 file format		http://www.rsa.com/rsalabs/node.asp?id=2138	

Note: The cryptographic functions marked with a 'No' in the last column of the table above have not been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard will not be part of this evaluation. FIPS certified cryptographic support is provided by RSA BSafe Crypto-J v3.6 JSafe Software Module (cert #812) or JCE Provider Module (cert #820).

1.4.7 Product Guidance

The following product guidance documents are provided with the TOE. These documents are available in PDF format inside the downloaded zip or on the specially requested installation

DVD. All but the CC supplement may be accessed directly through the *Resources* link on the Dashboard, AM, and DS interfaces.

1.4.8 References

Table 1-6 provides the references used to develop this Security Target.

Table 1-6: CC References

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2007-09-002, Version 3.1, Revision 2	[CC]

Table 1-7: User Guidance Documents

References on product media	ID
Xacta® IA Manager: Assessment Engine™ Reference Manual Version 4.0, Service Pack 8, December 21, 2009	[AEREF]
Xacta® IA Manager: Assessment Engine™ Version 4.0, Service Pack 8 Release Notes, December 10, 2009	[AEREL]
Xacta® IA Manager: Continuous Assessment™ Reference Manual Version 4.0, Service Pack 8, December 21, 2009	[CAREF]
Xacta® IA Manager: Continuous Assessment™ Version 4.0, Service Pack 8 Release Notes 7 December , 10 2009	[CAREL]
Xacta® JavaScript Extensions Reference Manual for Version 4.0, Service Pack 8, June 15 2009	[ERM]
Secure Installation & Configuration Supplement for Version 4.0, Service Pack 8 Xacta® IA Manager: Assessment Engine™ and Xacta® IA Manager: Continuous Assessment , July 23, 2010	[CCSUP]
Product Web Page	**ID**
http://www.telos.com/solutions/information assurance/xacta ia manager/	[WEB]

1.4.9 Previous Product Certifications

A previous version of the product, Xacta IA Manager Enterprise Edition V4.0 SP2, Build 485, was Common Criteria evaluated and certified at EAL2 in January 2005.

The following product components have received NIST SCAP validation:

- Xacta IA Manager: Continuous Assessment, Version 4.0 SP8 (SCAP Website lists as 4.8), Validation Date: June 5th, 2009
- Xacta IA Manager (Xacta HostInfo), Version 4.0 SP8 (SCAP Website lists as 4.8), Validation Date: March 19th, 2009

Information about the SCAP validation is available at: http://nvd.nist.gov/validation_telos.cfm

Note: While Xacta IA Manager: Continuous Assessment and Xacta HostInfo have themselves been SCAP validated, the product itself does not do SCAP validation. It provides support for commercial and government compliance to the customer.

1.4.10 Physical Scope of the TOE

The TOE consists of the components and subsystems described in Section 1.4.3. The physical boundary of the TOE is the Assessment Engine and Continuous Assessment components of the Xacta IA Manager V4.0 SP8 framework as commercially available from the developer, except per exclusions noted in section 1.4.10.2 below. The evaluated configuration of the TOE covered both the standalone and standard network deployment (distributed AE separately installed from CA components). The TOE Boundary for the standard network deployment is depicted in Figure 1.

1.4.10.1 Included in the TOE:

The evaluated configuration will include the following components and subsystems:

- Xacta IA Manager: Assessment Engine (Assessment Engine)
  - Assessment Engine Application Server
  - Dashboard
  - Publishing Server
  - Third party subsystems included as part of the AE that are installed with the TOE:
    - Tomcat 5.5.27
    - JRE 6 update 13
    - iReasoning SNMP Subagent Service v1
    - Bouncy Castle 1.40
    - RSA BSafe Crypto-J v3.6 (JSafe and JCE)
- Xacta IA Manager: Continuous Assessment (Xacta Continuous Assessment)
  - Asset Manager
  - Asset Manager GUI
  - Detect Server
  - Detect Server GUI
  - HostInfo Agents
  - Third party subsystems included as part of the AM and DS installed with the TOE:
    - Tomcat 5.5.27
    - JRE 6 update 13
    - iReasoning SNMP Subagent Service v1
    - Bouncy Castle 1.40
    - RSA BSafe Crypto-J v3.6 (JSafe and JCE)

- Default Government or Commercial Templates included with the product

Note: The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient is not part of this evaluation.

- Default Test Scripts included with the product
    - JavaScript Extensions

Note: The assessment scripts with the JavaScript Extensions defined in the Xacta® JavaScript Extensions Reference Manual for Version 4.0, Service Pack 8, June 15 2009 will be/were tested for basic functionality and that the results provided by scripts were used by the AE's risk assessment process.

1.4.10.2 Excluded from the TOE:

The following components of the Xacta IA Manager V4.0 SP8 framework are not included in the TOE:

- Xacta IA Manager: Process Enforcer (separately licensed)
- Legacy HostInfo Agents (previous agents from earlier versions of the TOE)

The following product subsystems are used for installation and maintenance and are not included in the TOE:

- HostInfo Utility
- HostInfo Agent Configuration Utility
- Xacta Utilities GUI

The following OE components are excluded from the scope of the evaluation:

- None of the Underlying operating system (OS) software and hardware of the TOE component's (servers and agents) host platforms
- Underlying third-party relational databases (including the MS SQL Express 2005 that is packaged with the product)
- MS Office (MS Word must be completely installed for the Publishing Server)
- .NET framework (.NET 2.0 is included with the product, but will only be installed if there is not a version 2.0 or better .NET framework installed.
- Winpcap driver 4.1.1 (The customer must pre-install this driver and use the version included with the CA product. This must be not be updated by the customer. Updated Winpcap drivers must undergo integration testing with the TOE.)
- SSL capable Web Browser installed on any platform being used as an Administrative Console
- Third-party applications used to view TOE output (e.g. MS Word, MS Excel, OpenOffice, or Adobe Acrobat). (These applications do not come with the product and must be separately installed by the customer)

- LDAP or Active Directory Server (optional)
- SMTP Server (optional)
- SNMP Network Management Station/Server (optional)
- Syslog Server (optional)
- Third-party Asset Discovery/Vulnerability Scanners/ Enterprise Management Databases (optional)
  - NESSUS (Version 2.0)
  - eEye Retina / REM (Retina 5.x with REM Event server 3.6)
  - ISS Internet Scanner (7.0 SP2)
  - ISS Site Protector (Version)
  - Microsoft SMS (2003 Server)
  - IBM Tivoli (Version)
- Public Key Infrastructure components (includes any drivers needed for operation)
  - Card Reader for Common Access Cards (CAC)
  - Certificate Authorities
- Network Infrastructure
- Protocol Implementations

1.4.11 Logical Scope of the TOE

This is a software-only TOE; therefore it relies on the OE to support its security functionality. The security features provided by the OE to support the TOE are described in Section 7 TOE Summary Specification.

The TOE provides the following security functionality:

1.4.11.1 Security Audit

The TOE provides a de-centralized auditing functionality. The TOE provides its own auditing capabilities separate from those of the host operating systems. The TOE provides the ability to search, sort, order, and view its own audit records.

Security Audit relies on functionality in the OE to provide: protection of the audit information stored in the TOE components' databases and in files on the TOE platforms' operating system; access to the audit information stored in an external or local Syslog; and reliable timestamps for the audit records.

1.4.11.2 Proof of Origin

The TOE provides the ability for administrators to digitally sign documents, reports and scripts to verify the origin of the information contained within them.

Proof of Origin relies on functionality in the OE to provide: PKI Infrastructure functionality; Adobe Acrobat digital signing functionality; and use of an optional Browser Crypto Module or CAC as a security provider for generation of digital signatures.

Note: The cryptographic functions used for digitally signing documents and scripts have not been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard will not be part of this evaluation.

1.4.11.3 Identification and Authentication

The TOE provides user identification and authentication for the Dashboard, Asset Manager GUI, and Detect Server GUI through the use of user accounts. Each account holder must be successfully identified and authenticated with a username and password by the TSF or by an authentication service invoked by the TSF before access to the TOE is allowed. In addition the TSF enforces a password policy and requires users to be re-authenticated after a specified period of inactivity.

The TOE enhances the security of an individual's TOE session by displaying a warning message (banner) when the session is initiated.

Identification and Authentication relies on functionality in the OE to provide: PKI Infrastructure functionality including keystore; protection of the user account information stored in the TOE components' databases; encryption support; use of an optional external authentication server; and trusted communications between the TOE and any external authentication server. Maintenance and Installation Utilities require OS I&A for access.

Note: The cryptographic functions used for certificate authentication and revocation checking have not been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard will not be part of this evaluation.

1.4.11.4 Security Management

The TOE provides security management through the use of individual administrator graphical user interfaces for each of the 3 main components (AE, AM, DS). Through the enforcement of the individual component's administrative access control policy, access to the management functionality and TSF data is controlled by security (administrative) role assignments.

Security Management relies on functionality in the OE to provide: protection of the maintenance and installation utilities; and trusted communications between the TOE and external servers, and external authentication servers (if configured to be used).

1.4.11.5 Trusted Channel

The TOE provides for trusted communication channels among its distributed application components by invoking the secure communications functionality of the OE and by providing cryptographic functions using third-party algorithms.

See Section 1.4.6 Cryptographic Functions for the details of the cryptographic functions used for trusted communications.

Trusted Channel relies on functionality in the OE for TCP/IP protocols.

Note: *The cryptographic functions used for secure communications between TOE components have been FIPS certified (RSA BSafe Crypto-J v3.6 JSafe Software Module (cert #812) and JCE Provider Module (cert #820)). The correctness of cryptographic modules used by the TOE for other purposes is by Vendor assertion; the correctness and conformance of those modules to any standard will not be part of this evaluation.*

1.4.11.6 Risk and Compliance Assessment

The TOE provides risk and compliance assessment of IT network assets including: collection of asset data, evaluation of the collected data, and sending notifications to appropriate personnel for significant events in the assessment process.

Note: The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient is not part of this evaluation.

Risk and Compliance Assessment relies on functionality in the OE to provide: proper configuration of the HostInfo Agent platforms for proper data collection; optional third-party asset discovery/vulnerability scanning; optional third-party enterprise management database functionality; PKI Infrastructure functionality; protection of data and script files on the host platforms; trusted communications between the TOE and the host platforms; and optional SMTP Server functionality for notifications.

1.4.11.7 Functionality Excluded from the TOE

The following functionality is not included in the Logical Scope of the TOE:

- Use of deprecating Xacta Automated Script Language (XASL).
- Correctness and modification of Velocity scripts to publish and customize reports.
- Publisher Component's use of the Velocity scripts and the data provided by the AE to correctly and accurately publish the report(s) (i.e the functionality to generate a report is in scope just not the verification that the report is correct and/or accurate).
- Verification of the correctness and completeness of the
    - project templates to meet claimed standard
    - process steps assigned to the project templates

  - assigned assessment scripts to the process steps
  - published reports to meet selected C&A submittal requirements for claimed standards

- Correctness, modification, customization, or creation of the individual assessment scripts (TOE's ability to assign, execute, and retrieve results from scripts is in scope).
- Verification of the Job Scheduler to correctly invoke scheduled jobs at the times configured
- WYSIWYG Editor
- System of Systems configuration (hierarchical deployment of DS servers)
- Project Control Implementation Inheritance application feature.
- Verification of the correctness and completeness of the imported SCAP or OVAL scripts.
- Use of security markings

Note: Xacta IA Manager is intended to be operated in a system high mode of operation. Security classification markings are only used to display a visual reminder of the highest classification level of data that should be stored in the application. The TOE is NOT a mult-level security (MLS) product. No enforcement of any kind is based off of this label and is not considered a security function.

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2 from the Common Criteria Version 3.1 R2.

2.2 Protection Profile Claim

This ST does not claim conformance to any existing Protection Profile.

2.3 Package Claim

This ST does not claim conformance to any existing Security Requirement Package.

3 Security Problem Definition

3.1 Threats

The TOE must counter threats to itself and the security of the IT network assets that it assesses. These threats are listed in Table 3-1. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

Table 3-1: TOE Threats

Item	Threat ID	Threat Description
1	T.AssetRisks	Security risks, vulnerabilities and non-compliance may exist on the IT network assets that the TOE assesses, leading to a compromise of those assets.
2	T.Intercept	An attacker may gain access to and/or modify secure data while it is being transmitted between TOE components.
3	T.Masquerade	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources via the TOE interfaces.
4	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
5	T.NoPrivilege	An authorized user may gain access to management functions or TSF data for which they have no privilege, resulting in the TSF data being compromised.
6	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for the TOE.

3.3 Assumptions

The assumptions regarding the security environment and the intended usage of the TOE are listed in Table 3-2.

Table 3-2: Assumptions

Item	Assumption ID	Assumption Description
1	A.Admin	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, trained for the secure operation of the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
2	A.Manage	It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.
3	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.
4	A.Physical	It is assumed that the TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.
5	A.ProtectComm	It is assumed that those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote users are configured to use secure channels.
6	A.ProtectDB	It is assumed that those responsible for the TOE will ensure that data stored in the databases used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.
7	A.ProtectFiles	It is assumed that those responsible for the TOE will ensure executable and data files used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.
8	A.ProtectPwd	It is assumed that users will protect their authentication data.
9	A.SupportAgent	It is assumed that the host computer on which the HostInfo Agent has been installed has been configured to allow the agent to collect the data the TOE needs for risk and compliance assessment (i.e. the assessment scripts are able to “see” the necessary data).

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in Table 4-1.

Table 4-1: TOE Security Objectives

Item	TOE Objective	Description
1	O.Access	The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.
2	O.Analyze	The TOE will be capable of analyzing the collected asset data to derive conclusions about risks and compliance of the IT network assets.
3	O.Attributes	The TOE will be able to store and maintain user attributes.
4	O.AuditGeneration	The TOE will provide the capability to selectively create records of security-relevant events and associate these events with the user who caused the event.
5	O.AuditReview	The TOE will provide the capability for review of the audit information to authorized users via the TOE interfaces.
6	O.Collect	The TOE will collect configuration data from the IT network assets.
7	O.CryptoComm	The TOE will provide cryptographic functions for secure communications between TOE components.
8	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.
9	O.Notify	The TOE will notify responsible personnel when designated events occur in the assessment process.
10	O.Password	The TOE will be able to support an administrator defined password policy.
11	O.ProtectAuth	The TOE will provide protected authentication feedback.
12	O.RobustTOEAccess	The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.
13	O.Sign	The TOE will provide mechanisms to allow digital signing of files to prove the origin of the information contained within them.
14	O.TransProtect	The TOE will invoke the Operational Environment to provide a trusted communications path that provides for the protection of the data from modification or disclosure while being exchanged between TOE components.

4.2 Security Objectives for the Operational Environment

The security objectives for the Operational Environment are listed in Table 4-2.

Table 4-2: Security Objectives for the Operational Environment

Item	Environment Objective	Description
1	OE.AuthService*	The Operational Environment will provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.

Item	Environment Objective	Description
2	OE.NoUntrusted	The administrator will ensure that there are no untrusted users and no untrusted software on the TOE component servers.
3	OE.Operations	The TOE will be installed, configured and operated in a secure manner as outlined in the supplied guidance.
4	OE.Person	Personnel working as authorized administrators will be carefully selected and trained for proper operation of the system.
5	OE.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
6	OE.ProtectAudit	The Operational Environment will provide a means for secure storage and protection of the TOE audit information from unauthorized users via the Operational Environment interfaces.
7	OE.ProtectAuth	Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
8	OE.ProtectComm	Those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote users are via a secure channel.
9	OE.ProtectDB	The Operational Environment will be configured by those responsible for the TOE to protect information stored in the database systems used by the TOE via the Operational Environment interfaces.
10	OE.ProtectFiles	The Operational Environment will be configured by those responsible for the TOE to protect executable and data files used by the TOE via the Operational Environment interfaces.
11	OE.Sign	The Operational Environment will provide mechanisms to support digital signing of files to prove the origin of the information contained within them.
12	OE.TransProtect	The Operational Environment will provide a mechanism to establish a trusted communications path that provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents.
13	OE.Time	The underlying operating system will provide reliable time stamps.
14	OE.CollectionSupport	Responsible personnel will configure each host computer on which the HostInfo Agent has been installed to allow the agent to collect the data the TOE needs for risk and compliance assessment.

**Note: OE.AuthService is only applicable to the TOE is configured to use an external authentication service. (I.e. LDAP or Active Directory Server)*

4.3 Security Objectives Rationale

Table 4-3: Mapping of TOE Security Objectives to Threats/Policies

Item	TOE Objective	Threat
1	O.Access	T.NoPrivilege
2	O.Analyze	T.AssetRisks
3	O.Attributes	T.NoPrivilege
4	O.AuditGeneration	T.Undetect
5	O.AuditReview	T.Undetect
6	O.Collect	T.AssetRisks
7	O.CryptoComm	T.Intercept

Item	TOE Objective	Threat
8	O.Manage	T.Mismanage
9	O.Notify	T.AssetRisks
10	O.Password	T.Masquerade
11	O.ProtectAuth	T.Masquerade
12	O.RobustTOEAccess	T.Masquerade
13	O.Sign	T.Intercept T.Masquerade
14	O.TransProtect	T.Intercept

Table 4-4: Mapping of Security Objectives for the Operational Environment to Threats/Policies/Assumptions

Item	Environment Objective	Threat/Policy/Assumption
1	OE.AuthService	T.Masquerade
2	OE.NoUntrusted	A.NoUntrusted
3	OE.Operations	A.Manage
4	OE.Person	A.Admin
5	OE.Physical	A.Physical
6	OE.ProtectAudit	T.Undetect
7	OE.ProtectAuth	A.ProtectPwd
8	OE.ProtectComm	A.ProtectComm
9	OE.ProtectDB	A.ProtectDB
10	OE.ProtectFiles	A.ProtectFiles
11	OE.Sign	T.Intercept T.Masquerade
12	OE.Time	T.Undetect
13	OE.TransProtect	T.Intercept
14	OE.CollectionSupport	A.SupportAgent

Table 4-5 shows that all the identified Threats to security are countered by Security Objectives. Rationale is provided for each Threat in the table.

Table 4-5: All Threats to Security Countered

Item	Threat ID	Objective	Rationale
1	T.AssetRisks Security risks, vulnerabilities and non-compliance may exist on the IT network assets that the TOE assesses, leading to a compromise of those assets.	O.Analyze The TOE will be capable of analyzing the collected asset data to derive conclusions about risks and compliance of the IT network assets.	This objective plays a role in mitigating this threat by analyzing the collected asset data for risks, vulnerabilities and non-compliance to security standards.
		O.Collect The TOE will collect configuration data from the IT network assets.	This objective also contributes to mitigating this threat by providing the TOE's analyzer with the appropriate configuration data collected from the assets.

Item	Threat ID	Objective	Rationale
		O.Notify The TOE will notify responsible personnel when designated events occur in the assessment process.	This objective also contributes to mitigating this threat by notifying the appropriate personnel when a significant event happens as a result of the analysis process on the collected data.
		OE.CollectionSupport Responsible personnel will configure each host computer on which the HostInfo Agent has been installed to allow the agent to collect the data the TOE needs for risk and compliance assessment.	This objective also contributes to mitigating this threat by requiring that the host computers undergoing risk and compliance assessment have been properly configured to allow collection of the data needed by the TOE.
2	T.Intercept An attacker may gain access to and/or modify secure data while it is being transmitted between TOE components.	O.TransProtect The TOE will invoke the Operational Environment to provide a trusted communications path that provides for the protection of the data from modification or disclosure while being exchanged between TOE components.	This objective contributes to mitigating this threat by ensuring that the TOE only uses secure communications paths that have been established by the Operational Environment for the transmission of security data.
		O.Sign The TOE will provide mechanisms to allow digital signing of files to prove the origin of the information contained within them.	This objective contributes to mitigating this threat by providing the ability for the TOE to digitally sign the scripts that are transmitted between the TOE components.
		OE.Sign The Operational Environment will provide mechanisms to support digital signing of files to prove the origin of the information contained within them.	This objective contributes to mitigating this threat by providing cryptographic and security functions in the Operational Environment to support the digital signing of the scripts that are transmitted between the TOE components.
		O.CryptoComm The TOE will provide cryptographic functions for secure communications between TOE components.	This objective contributes to mitigating this threat by ensuring that the TOE will encrypt the data being transmitted between TOE components.

Item	Threat ID	Objective	Rationale
		OE.TransProtect The Operational Environment will provide a mechanism to establish a trusted communications path that provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents.	This objective also contributes to mitigating this threat by ensuring that the Operational Environment will use only secure mechanisms to establish the communication paths used by the TOE.
3	T.Masquerade A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.	O.Password The TOE will be able to support an administrator defined password policy.	This objective mitigates the threat by providing a policy to enforce strong user passwords and limiting brute force guessing attacks.
		O.ProtectAuth The TOE will provide protected authentication feedback.	This objective mitigates the threat by providing the masking of a user's password to keep it from being overseen by another.
		O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.	This objective mitigates this threat by controlling the logical access to the TOE and its resources through the login process. By constraining how authorized users can access the TOE, and by mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective allows the TOE to correctly interpret information used during the authentication process so that it can make the correct decisions when identifying and authenticating users. This objective also requires the re-authentication of a user after a defined period of inactivity.
		O.Sign The TOE will provide mechanisms to allow digital signing of files to prove the origin of the information contained within them.	This objective mitigates this threat by providing the ability for the TOE to digitally sign the published documents and reports that are produced by the TOE.

Item	Threat ID	Objective	Rationale
		OE.Sign The Operational Environment will provide mechanisms to support digital signing of files to prove the origin of the information contained within them.	This objective contributes to mitigating this threat by providing cryptographic and security functions in the Operational Environment to support the digital signing of the published documents and reports that are produced by the TOE.
		OE.AuthService The Operational Environment will provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.	This objective mitigates the threat by allowing the use of an external user authentication service that is invoked by the TSF.
4	T.Mismanage Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	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.	This objective mitigates this threat by providing management tools to make it easier for administrators to manage the TOE security functions. More specifically, it provides administrators with the capability to configure and operate the TOE via a GUI.
5	T.NoPrivilege A user may gain access to management functions or TSF data for which they are not authorized resulting in the TSF data being compromised.	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.	This objective mitigates this threat by limiting the functions a user can perform and the data they can access via the TOE interfaces through the use of user security roles and permissions.
		O.Attributes The TOE will be able to store and maintain user attributes.	This objective also mitigates the threat by providing the capability to store user security roles and data permissions for each user account.
6	T.Undetect Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.	O.AuditGeneration The TOE will provide the capability to selectively create records of security-relevant events and associate these events with the user who caused the event.	This objective mitigates this threat by providing the TOE with an audit logging function that keeps records of security significant events.
		O.AuditReview The TOE will provide the capability for review of the audit information to authorized users via the TOE interfaces.	This objective also mitigates this threat by providing administrative personnel with the capability to efficiently review the audit information and spot a security breach.

Item	Threat ID	Objective	Rationale
		OE.ProtectAudit The Operational Environment will provide a means for secure storage and protection of the TOE audit information from unauthorized users via the Operational Environment interfaces.	This objective mitigates the threat by ensuring that the audit records cannot be accessed by unauthorized personnel through the Operational Environment interfaces (both through the DBMS and the operating systems of the TOE Servers).
		OE.Time The underlying operating system will provide reliable time stamps.	This objective contributes to mitigating the threat by providing each audit record with an accurate time stamp.

Table 4-6 shows that the security objectives for the operational environment uphold all assumptions. Rationale is provided for each Assumption in the table.

Table 4-6: All Assumptions Upheld

Item	Assumption ID	Objective	Rationale
1	A.Admin It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, trained for the secure operation of the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.	OE.Person Personnel working as authorized administrators will be carefully selected and trained for proper operation of the system.	This objective provides for competent personnel to administer the TOE.
2	A.Manage It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.	OE.Operations The TOE will be installed, configured and operated in a secure manner as outlined in the supplied guidance.	This objective ensures that all TOE users follow the guidance for secure installation, configuration and operation procedures.
3	A.NoUntrusted It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.	OE.NoUntrusted The administrator will ensure that there are no untrusted users and no untrusted software on the TOE component servers.	This objective provides for the protection of the TOE from untrusted software and users.
4	A.Physical It is assumed that the TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.	OE.Physical Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.	This objective provides for the physical protection of the TOE software.
5	A.ProtectComm It is assumed that those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote users are configured to use secure channels.	OE.ProtectComm Those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote users are via a secure channel.	This objective provides for the configuration of secure communication paths between the TOE components and between the TOE components and remote users by an authorized administrator.

Item	Assumption ID	Objective	Rationale
6	A.ProtectDB It is assumed that those responsible for the TOE will ensure that data stored in the databases used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.	OE.ProtectDB The Operational Environment will be configured by those responsible for the TOE to protect information stored in the database systems used by the TOE via the Operational Environment interfaces.	This objective provides for the secure configuration of the databases by an authorized administrator to prevent unauthorized access to the stored data through the Operational Environment interfaces.
7	A.ProtectFiles It is assumed that those responsible for the TOE will ensure executable and data files used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.	OE.ProtectFiles The Operational Environment will be configured by those responsible for the TOE to protect executable and data files used by the TOE via the Operational Environment interfaces.	This objective provides for the secure configuration of the executable and data files by an authorized administrator to prevent unauthorized access to the TOE files through the Operational Environment interfaces.
8	A.ProtectPwd It is assumed that users will protect their authentication data.	OE.ProtectAuth Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.	This objective provides for all TOE users protecting their authentication data.
9	A.SupportAgent It is assumed that the host computer on which the HostInfo Agent has been installed has been configured to allow the agent to collect the data the TOE needs for risk and compliance assessment (i.e. the assessment scripts are able to “see” the necessary data).	OE.CollectionSupport Responsible personnel will configure each host computer on which the HostInfo Agent has been installed to allow the agent to collect the data the TOE needs for risk and compliance assessment.	This objective provides for the proper configuration of the host computers so that the HostInfo Agent can collect data needed by the TOE for risk and compliance assessment.

5 Extended Components Definition

All of the components defined below have been modeled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding "_EXT" in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FCO_SIG_EXT.1	Generation of digital signatures
2	FIA_UAU_EXT.2	TSF user authentication before any action
3	FTA_SSL_EXT.1	TSF-initiated session locking
4	FTP_ITC_EXT.1	Partial Intra-TSF trusted channel among distributed TOE components
5	RCA_COL_EXT.1	Asset data collection
6	RCA_EVL_EXT.1	Risk and compliance evaluation
7	RCA_NOT_EXT.1	Asset security notifications

5.1 FCO_SIG_EXT.1 Generation of digital signatures

5.1.1 Extended Component Definition

5.1.1.1 Class

FCO: Communications

See Section 9 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 2.

5.1.1.2 Family

Digital signing (FCO_SIG)

5.1.1.3 Family Behaviour

This family defines the types of digital signing mechanisms supported by the TSF. This family also defines the type of information being signed and the originator of the signature request.

5.1.1.4 Management

The following actions could be considered for the management functions in FMT:

- The management of changes to information types, originator attributes and digital signature configuration parameters.

5.1.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: The identity of the user who requested that evidence of origin would be generated.
- Minimal: The invocation of the non-repudiation service.
- Basic: Identification of the information, the destination, and a copy of the evidence provided.

5.1.1.6 Definition

FCO_SIG_EXT.1 Generation of digital signatures

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_SIG_EXT.1.1 The TSF shall be able to generate evidence of origin either by the TSF itself or by a digital signature mechanism in the Operational Environment invoked by the TSF for transmitted *[assignment: list of information types]* at the request of the *[selection: originator, recipient, [assignment: list of third parties]]*.

5.1.2 Rationale

FCO_SIG_EXT.1 is modeled closely on the standard component FCO_NRO.1: Selective proof of origin. FCO_SIG_EXT.1 needed to be defined as an extended component because the digital signatures are generated either by the TSF itself (through Java Plugins in the GUI subsystems of the TOE) or by the Operational Environment (via CAC functionality) at the request of the TSF. Only the generation of the digital signatures is covered by this SFR; verification of the evidence of origin may be done outside the TOE. Therefore, only FCO_NRO.1.1 was used as a template for FCO_SIG_EXT.1.

5.2 FIA_UAU_EXT.2 TSF user authentication before any action

5.2.1 Extended Component Definition

5.2.1.1 Class

FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 2.

5.2.1.2 Family

User authentication (FIA_UAU)

5.2.1.3 Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

5.2.1.4 Management

The following actions could be considered for the management functions in FMT:

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

5.2.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism
- Basic: All use of the authentication mechanism

5.2.1.6 Definition

FIA_UAU_EXT.2 TSF user authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

5.2.2 Rationale

FIA_UAU_EXT.2 is modeled closely on the standard component FIA_UAU.2: User authentication before any action. FIA_UAU_EXT.2 needed to be defined as an extended component because the standard component was broadened by adding the text *"either by the TSF or by an authentication service in the Operational Environment invoked by the TSF".*

5.3 FTA_SSL_EXT.1 TSF-initiated session locking

5.3.1 Extended Component Definition

5.3.1.1 Class

FTA: TOE Access

See Section 17 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 2.

5.3.1.2 Family

Session locking and termination (FTA_SSL)

5.3.1.3 Family Behaviour

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

5.3.1.4 Management

The following actions could be considered for the management functions in FMT:

- Specification of the time of user inactivity after which lock-out occurs for an individual user;
- Specification of the default time of user inactivity after which lock-out occurs;
- Management of the events that should occur prior to unlocking the session.

5.3.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Locking of an interactive session by the session locking mechanism.

- Minimal: Successful unlocking of an interactive session.
- Basic: Any attempts at unlocking an interactive session.

5.3.1.6 Definition

FTA_SSL_EXT.1 TSF-initiated session locking

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL_EXT.1.1 The TSF shall lock an interactive session after *[assignment: time interval of user inactivity]* by disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL_EXT.1.2 The TSF shall require the following events to occur prior to unlocking the session: *[assignment: events to occur].*

5.3.2 Rationale

FIA_SSL_EXT.1 is modeled closely on the standard component FIA_SSL.1: TSF-initiated session locking. FIA_SSL_EXT.1 needed to be defined as an extended component because the TOE uses Web-based GUIs for administration which cannot be cleared when an inactivity time-out occurs. Therefore, the condition "***clearing or overwriting display devices, making the current contents unreadable;"*** was deleted from the definition of this SFR.

5.4 FTP_ITC_EXT.1 Partial Intra-TSF trusted channel among distributed TOE components

5.4.1 Extended Component Definition

5.4.1.1 Class

FTP: Trusted path/channels

See Section 18 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 2.

5.4.1.2 Family

Inter-TSF trusted channel (FTP_ITC)

5.4.1.3 Family Behaviour

This family defines requirements for the creation of a trusted channel between the TSF and other trusted IT products for the performance of security critical operations. This family should be included whenever there are requirements for the secure communication of user or TSF data between the TOE and other trusted IT products.

5.4.1.4 Management

The following actions could be considered for the management functions in FMT:

- Configuring the actions that require trusted channel, if supported

5.4.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure of the trusted channel functions
- Minimal: Identification of the initiator and target of failed trusted channel functions
- Basic: All attempted uses of the trusted channel functions
- Basic: Identification of the initiator and target of all trusted channel functions

5.4.1.6 Definition

FTP_ITC_EXT.1 Partial Intra-TSF trusted channel among TOE components

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC_EXT.1.1 The TSF shall invoke the Operational Environment to establish a trusted communication channel among its distributed component applications that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure using the encryption and certificate services from the Operational Environment.

FTP_ITC_EXT.1.2 The TSF shall use this trusted channel for all communication among its distributed application components.

5.4.2 Rationale

FTP_ITC_EXT.1 is modeled closely on the standard component FTP_ITC.1: Inter-TSF trusted channel. FTP_ITC_EXT.1 needed to be defined as an extended component because the

standard component did not take into account the interdependency between the TOE and the Operational Environment to implement the trusted channel.

5.5 RCA_COL_EXT.1 Asset data collection

5.5.1 Extended Component Definition

5.5.1.1 Class

RCA: Risk and compliance assessment

This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a risk and compliance assessment product. While most of the SFRs that follow were modeled on existing IDS requirements that have been used in validated Protection Profiles, these requirements needed further modification to meet the specific needs of risk and compliance assessment rather than intrusion detection.

5.5.1.2 Family

Asset data collection (RCA_COL)

5.5.1.3 Family Behaviour

This family defines the types of scanning of IT network assets supported by the TSF. This family also defines the asset information collected by the scanner components of the TOE. The scanners would generally collect static configuration information and send that onto an analytical component.

5.5.1.4 Management

The following actions could be considered for the management functions in FMT:

- Configuration of the collected asset information by an administrator
- Configuration of the scanner operation by an administrator

5.5.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: error return from scanning process
- Basic: time of scan; successful/unsuccessful outcome of scan

5.5.1.6 Definition

RCA_COL_EXT.1 Asset data collection

Hierarchical to: No other components

Dependencies: No dependencies

RCA_COL_EXT.1.1 The TSF shall be able to collect configuration information from the IT network assets on the target network via the following methods *[assignment: list of collection methods].*

RCA_COL_EXT.1.2 At a minimum, the TSF shall collect and record the following information: *[assignment: list of asset information].*

5.5.2 Rationale

RCA_COL_EXT.1 is modeled on IDS_SCN.1 Scanner Data Collection (EXT) as defined in the IDS Scanner Protection Profile Version 1.3 July 25, 2007. This SFR was modified to be more general and also specify the collection of asset data via the listed methods of collection.

5.6 RCA_EVL_EXT.1 Risk and compliance evaluation

5.6.1 Extended Component Definition

5.6.1.1 Class

RCA: Risk and compliance assessment

See Section 5.5.1.1.

5.6.1.2 Family

Risk and compliance evaluation (RCA_EVL)

5.6.1.3 Family Behaviour

This family defines the evaluation of the data collected from the scanning of IT network assets supported by the TSF. It describes the actions of the analytical component of a risk and compliance management TOE. It also requires that the results of the evaluation must be available for user interpretation.

5.6.1.4 Management

The following actions could be considered for the management functions in FMT:

- Configuration of any evaluation parameters or reporting of results by an administrator

5.6.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: generation of evaluation results

5.6.1.6 Definition

RCA_EVL_EXT.1 Risk and compliance evaluation

Hierarchical to: No other components

Dependencies: RCA_COL_EXT.1

RCA_EVL_EXT.1.1 The TSF shall be capable of performing the following evaluation function(s) on the collected IT network asset data*: [assignment: list of evaluation functions].*

5.6.2 Rationale

RCA_EVL_EXT.1 is modeled on IDS_ANL.1 Analyzer analysis (EXT) as defined in IDS Analyzer Protection Profile Version 1.3 July 25, 2007. The SFR was made more general to specify the list of functions used for the evaluation and assessment of various types of risk and compliance data.

5.7 RCA_NOT_EXT.1 Asset security notifications

5.7.1 Extended Component Definition

5.7.1.1 Class

RCA: Risk and compliance assessment

See Section 5.5.1.1.

5.7.1.2 Family

Asset security notifications (RCA_NOT)

5.7.1.3 Family Behaviour

This family defines the notifications generated by the TSF as a result of scanning IT network assets and analyzing the asset data. This family also defines the destination(s) of the notifications that are generated. The scanners would generally collect static configuration information and send that onto an analytical component which would cause the notifications to be generated.

5.7.1.4 Management

The following actions could be considered for the management functions in FMT:

- Configuration of the notification destination by an administrator

5.7.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: time notification generated, source and destination of notification, notification type

5.7.1.6 Definition

RCA_NOT_EXT.1 Asset security notifications

Hierarchical to: No other components

Dependencies: RCA_EVL_EXT.1

RCA_NOT_EXT.1.1 The TSF shall send a notification to *[assignment: notification destination]* when *[assignment: event]* occurs during the risk and compliance assessment process.

5.7.2 Rationale

RCA_NOT_EXT.1 is modeled on IDS_RCT.1 Analyzer react (EXT) as defined in IDS System Protection Profile Version 1.7 July 25, 2007. This SFR was modified to apply to the various events that can be generated by a risk and compliance assessment system rather than only the detection of an intrusion. This SFR uses the term “notification” rather than “alert” because the TOE sends this information via email (SMTP Server or native messaging within the product) and

therefore cannot guarantee that the recipient will acknowledge or read the event information in a timely manner.

6 Security Requirements

This section provides the security functional and assurance requirements for the TOE.

6.1 Security Functional Requirements for the TOE

Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined as:

iteration: allows a component to be used more than once with varying operations;

assignment: allows the specification of parameters;

selection: allows the specification of one or more items from a list; and

refinement: allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in ***[italicized bold text].***
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.

Iterations are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. “*” refers to all iterations of a component.

Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

Extended components defined in Section 5 have been denoted with the suffix “_EXT” following the family name.

The functional security requirements for the TOE consist of the following components taken directly from Part 2 of the CC and the extended components defined in Section5, and summarized in Table 6-1 below.

Table 6-1: Functional Components

Item	SFR ID	SFR Title
1	FAU_GEN.1	Audit data generation
2	FAU_GEN.2	User identity association
3	FAU_SAR.1	Audit review
4	FAU_SAR.2	Restricted audit review
5	FAU_SAR.3	Selectable audit review
6	FCO_SIG_EXT.1-1	Generation of digital signatures (documents and reports)
7	FCO_SIG_EXT.1-2	Generation of digital signatures (scripts)
8	FCS_CKM.1	Cryptographic key generation

Item	SFR ID	SFR Title
9	FCS_CKM.4	Cryptographic key destruction
10	FCS_COP.1	Cryptographic operation
11	FIA_AFL.1	Authentication failure handling
12	FIA_ATD.1	User attribute definition
13	FIA_SOS.1	Verification of secrets
14	FIA_UAU_EXT.2	TSF user authentication before any action
15	FIA_UAU.6	Re-authenticating
16	FIA_UAU.7	Protected authentication feedback
17	FIA_UID.2	User identification before any action
18	FMT_MTD.1	Management of TSF data
19	FMT_SMF.1	Specification of Management Functions
20	FMT_SMR.1	Security roles
21	FTA_SSL_EXT.1	TSF-initiated session locking
22	FTA_TAB.1	Default TOE access banners
23	FTP_ITC_EXT.1	Partial Intra-TSF trusted channel among distributed TOE components
24	RCA_COL_EXT.1	Asset data collection
25	RCA_EVL_EXT.1	Risk and compliance evaluation
26	RCA_NOT_EXT.1	Asset security notifications

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) ***[the following auditable events: Events listed in column 2 of Table 6-2].***

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: ***[remote address (if applicable), customer ID (if applicable), folder name (if applicable), project name (if applicable), and event description].***

Application Note: The event description field in the audit log contains additional information including the event outcome, details of security settings changes, and details of script signing.

Table 6-2: Auditable Events

Component (Subsystem)	Event	Description/Comments
Assessment Engine	System Startup	Xacta Assessment Engine startup
	System Shutdown	Xacta Assessment Engine shutdown
	Login Fail	Failed user login
	Login	Successful user login
	Logout	User logout
	Security Policy Change	Security (password) policy changed
	Creation	Creation of database object *
	Modification	Change to database object *
	Deletion	Deletion of database object *
	Application Settings Change	Xacta Assessment Engine configuration settings changed
	User Forced	Forced user logout
	Audit Log State	Xacta Assessment Engine audit turned on/off
	Publisher	Document published (success/failure)
	Log Cleared	Xacta Assessment Engine audit log cleared
	Software Activation	Software activated and issued a confirmation ID
	Project Activation	Project activated
	Event sent	Event notification sent
Continuous Assessment (Asset Manager)	System Startup	Asset Manager startup
	System Shutdown	Asset Manager shutdown
	Login Fail	Failed user login
	Login	Successful user login
	Logout	User logout
	Security Policy Change	Security (password) policy changed
	Application Settings Change	Asset Manager configuration settings changed
	Script Signed	User signed script(s)
	Audit Log State	Asset Manager audit turned on/off
	Log Cleared	Asset Manager audit log cleared
	Creation	Creation of database object *
	Modification	Change to database object *
	Deletion	Deletion of database object *
Continuous Assessment (Detect Server)	System Startup	Detect Server startup
	System Shutdown	Detect Server shutdown
	Login Fail	Failed user login
	Login	Successful user login
	Logout	User logout
	Security Policy Change	Security (password) policy changed
	Application Settings Change	Detect Server configuration settings changed
	Audit Log State	Detect Server audit turned on/off
	Log Cleared	Detect Server audit log cleared
	Creation	Creation of database object *
	Modification	Change to database object *
	Deletion	Deletion of database object *
	Agent Rejected	An agent checked in, but the IP range of the agent did not fall within the IP range of the Detect Server
	Scan Session	Detect Discovery Scan finished session

Component (Subsystem)	Event	Description/Comments
	AM Certificate	Asset Manager Certificate updated and added to the keystore
	Certificate Distribution	New Detect certificate distributed to all the agents

** Application Note: See Table 7-2: Object List (for Database Create, Update and Delete Events) for the list of database objects that apply to these events*

6.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[Master Administrators and Security Administrators]*** with the capability to read ***[all audit information]*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply ***[searches and ordering]*** of audit data based on ***[audit records with information that matches the user's input of one or more of the following fields:***

- ***User Name***
- ***Project Name***
- ***Event Name***
- ***Time span (Start Date, End Date)***
- ***Relevant Term (Description)***

].

6.1.2 Class FCO: Communications

6.1.2.1 FCO_SIG_EXT.1-1 Generation of digital signatures (documents and reports)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_SIG_EXT.1.1-1 The TSF shall be able to generate evidence of origin either by the TSF itself or by a digital signature mechanism in the Operational Environment invoked by the TSF for transmitted ***[published documents, reports]*** at the request of the ***[originator]***.

6.1.2.2 FCO_SIG_EXT.1-2 Generation of digital signatures (scripts)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_SIG_EXT.1.1-2 The TSF shall be able to generate evidence of origin either by the TSF itself or by a digital signature mechanism in the Operational Environment invoked by the TSF for transmitted ***[scripts]*** at the request of the ***[originator]***.

6.1.3 Class FCS: Cryptographic Support

6.1.3.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[listed in Column 1 of Table 6-3]*** and specified cryptographic key sizes ***[listed in Column 2 of Table 6-3]*** that meet the following: ***[standards listed in Column 4 of Table 6-3].***

Table 6-3: Cryptographic Support Parameters

Key Generation Algorithm	Key Size	Cryptographic Operations	Standards
3DES	128 bits	encryption decryption	SSL version 3.1 (aka TLS version 1 protocol) (RFC 2246)
AES	128bits	encryption decryption	SSL version 3.1 (aka TLS version 1 protocol) (RFC 2246)
AES	256 bits	encryption decryption	SSL version 3.1 (aka TLS version 1 protocol) (RFC 2246)

6.1.3.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[zeroization]*** that meets the following: ***[standards listed in Column 4 of Table 6-3].***

6.1.3.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform ***[operations listed in Column 3 of Table 6-3]*** in accordance with a specified cryptographic algorithm ***[listed in Column 1 of Table 6-3]*** and cryptographic key sizes ***[listed in Column 2 of Table 6-3]*** that meet the following: ***[standards listed in Column 4 of Table 6-3].***

6.1.4 Class FIA: Identification and Authentication

6.1.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***[a Master Administrator configured maximum number of]*** unsuccessful authentication attempts occur related to ***[user login attempts].***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met],*** the TSF shall ***[disable the user account until the account is reactivated by a Master Administrator].***

Application Note: By design, the Master Administrator account is never deactivated from console login.

6.1.4.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

- ***Account Name***

- ***Account Type***
- ***Authentication Type***
- ***Active/Inactive State***
- ***Password***
- ***Password History***
- ***Account Disabled Date (AE and AM)***
- ***Password Expiration (AE and AM)***
- ***Assigned Folder (AE only)***
- ***Assigned Project(s) (AE only)***
- ***IP Range (AM only)***

].

6.1.4.3 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***[the parameters of the Xacta Password Policy set by the Master Administrator (See Table 6-4)].***

Table 6-4: Xacta Password Policy Rules

Parameter	Description
Password Character Classes	Requires passwords to contain characters from specified number of character classes. There are four character classes: 1. Uppercase Alphabetic 2. Lowercase Alphabetic 3. Numeric 4. Special Characters (default = 3)
Password Class Counter	Requires passwords to contain at least the set number of characters from each of the specified number of character classes. (default =1)
Password Expiration	Maximum number of days before a password must be changed. (default =30; 0 = user must change password at each login)
Password History Cycle	Number of previous passwords to be checked against new passwords. (default =3; 0 = same password can be reused indefinitely)
Minimum Password Length	Minimum number of characters required in all passwords. (default = 8; minimum = 1)
Maximum Failed Login Attempts	Number of unsuccessful login attempts that may be made before the login account is disabled. (default = 3; 0 = account is never disabled)

Parameter	Description
Failed Login Time Frame	The time frame allowed for unsuccessful login attempts in seconds. An account will be disabled when the maximum failed login limit is met within the specified time frame. (default = 30 sec.)
Prevent Multiple Logins	Enabling this feature prevents users from logging into Assessment Engine using the same username and password, via multiple browser windows. (default = disabled)
Master Administrator Access	Disables remote login for master administrator accounts. (default = unrestricted access is enabled)
Validate CSP	Validates the CSP (Cryptography Service Provided) implementation used by government agencies that require specific patches of Microsoft Internet Explorer if PKI authentication is to be used to access the application. (default = no validation)
Restrict Non-PKI logon to Console Only	Restricts non-PKI logon to console only. (default = disabled)

6.1.4.4 FIA_UAU_EXT.2 TSF user authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.5 FIA_UAU.6 Re-authenticating

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions ***[after a Master Administrator configurable time of inactivity]***.

6.1.4.6 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only

[

For Username/Password authentication:

- ***display of the typed in account name (username)***
- ***typed in password displayed as dots***

For PKI/Active Directory authentication:

- ***display of CAC subject/Domain username (non-editable account name)***
- ***no password displayed***

]

to the user while the authentication is in progress.

6.1.4.7 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

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.

6.1.5 Class FMT: Security Management

6.1.5.1 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[operations as specified in Tables 6-5, 6-6, and 6-7,]*** the ***[TSF data as specified in Tables 6-5***, ***6-6, and 6-7]*** to ***[user security roles as specified in Tables 6-5, 6-6, and 6-7,].***

Table 6-5: Management of TSF data (Assessment Engine)

User Security Role	Operations	TSF data
Master Administrator	Activate	TOE software
	Configure/View Application settings	Maintenance Time, Verbosity, how enter key behaves, define LDAP server connection, AD Server,
	Configure/View Project Registration	Enable/disable requirement

User Security Role	Operations	TSF data
	Configure/View Audit settings	Enable/Disable audit, set record limit, syslog configuration
	Configure/View Security Policy settings	Password Policy parameters, master admin remote login restriction, preventing multiple logins, restrict non-PKI to local, enable/disable/configure certificate revocation checking.
	Configure/View Database settings	Detect Server Database (name, IP, database, credentials, port, SSL mode, # connections)
	Configure/View Support Services settings	Enable/Disable email support to either Xacta or local.
	Configure Active Update	Active Update URL, certification, enable/disable (templates, vulnerability alerts, script library)
	Configure SNMP settings	Enable/Disable SNMP Agent
	Configure/View Login Warning	Warning Banner
	Select Security Markings	Security classification markings *
	Configure Security Markings	Customize default labels hierarchy, create new labels
	Create, modify, delete User Accounts, reset password history	AE user security attributes: Account Name, Authentication Type, Active/Inactive State, and Password. Role, Notifications, Password expiration, account expiration Folders, and Projects.
	Configure Import from LDAP	PKI user authentication, URL
	Configure Import from LDAP	Windows domain user authentication, URL
	View/Cancel	Publisher queue
	View	Job schedule
	View/Cancel	Job queue
	View, send message to, Force logoff	Online users
	View and export Logs	Process log for AE Server
	View, export, and clear Audit	Audit log for AE Server
	Create Folder and Project Reports and generate .pdf	General reports about accounts, folders, projects, scripts, artifacts, workflow, and project activity, compliance, Risk, Plan of Action & Milestone, inventory, metrics, and others
	Configure/View Security Categories for Risk Assessments	Weight factors for Risk assessment
	Display, download	Backup Projects, encrypt or non encrypted modes
	Create, edit, delete, view Projects within folder, assign to users	Folders
	Create, activate, edit, reset, move, backup, restore, view Tasks within Projects	Projects
	Enable, Configure	Project registration

User Security Role	Operations	TSF data
	Add, edit, copy, replace, delete	Project role
	View, edit, copy, delete, replace, view status, configure status	Tasks
	Configure	Conditional workflow to task (customize tasks), customize project roles,
	Configure	Task's chain of approval
	Create, copy, modify, delete	Subprocesses
	View, create, edit, delete	Template folders
	View, mark as completed, attach artifact to, create, copy, edit, replace, delete	Process steps
	Create, edit, view, copy, filter, delete, attach to process steps	Artifacts
	Connect to AM to submit one time Task	Submitted Tasks (scans or script execution) identified in task.
	Schedule AE to Connect to AM to obtain results on a periodic bases	Results for previously identified task
	Create, edit, import, export, push to Asset Manager, assign labels	Scripts
	Publish, configure, format, view	Documents
	Digitally sign	Documents
	Digitally sign	Reports
	Import	Certificates
	Configure own profile	Reset own password, notification settings, stored backups, inbox, set default page.
	Import	Templates Downloaded from Xacta website
	Import	Test Scripts Downloaded from Xacta website
	View, import	Vulnerability alerts from Xacta website
Administrator (Management functions limited to assigned folder(s))	Create, modify, delete User Accounts, reset password history	AE user security attributes: Account Name, Authentication Type, Active/Inactive State, and Password. Role, Notifications, expiration, account expiration, Folders, and Projects. Password
	Configure Import from LDAP	PKI user authentication, URL
	Configure Import from LDAP	Windows domain user authentication, URL
	View/Cancel	Publisher queue
	View	Job schedule
	View/Cancel	Job queue
	View, send message to, Force logoff	Online users
	Create Folder and Project Reports and generate .pdf	General reports about accounts, folders, projects, scripts, artifacts, workflow, and project activity, compliance, Risk, Plan of Action & Milestone, inventory, metrics, and others

User Security Role	Operations	TSF data
	Configure/View Security Categories for Risk Assessments	Weight factors for Risk assessment
	Display, download	Backup Projects, encrypt or non encrypted modes
	Create, activate, edit, reset, move, backup, restore, view Tasks within Projects	Projects
	View, edit, copy, delete, replace, view status, configure status	Tasks
	Configure	Conditional workflow to task (customize tasks), customize project roles,
	View	Template folders
	View, mark as completed, attach artifact to, create, copy, edit, replace, delete	Process steps
	Create, edit, view, copy, filter, delete, attach to process steps	Artifacts
	Connect to AM to submit one time Task	Submitted Tasks (scans or script execution) identified in task.
	Schedule AE to Connect to AM to obtain results on a periodic bases	Results for previously identified task
	Create, edit, import, export, push to Asset Manager, assign labels	Scripts
	Publish, configure, format, view	Documents
	Digitally sign	Documents
	Digitally sign	Reports
	Import	Certificates
	Configure own profile	Reset own password, notification settings, stored backups, inbox, set default page.
Project Administrator (Management functions limited to assigned projects)	View/Cancel	Publisher queue
	View	Job queue for assigned projects
	View/Cancel	Job schedule for assigned projects
	Create, activate, edit, reset, move, backup, restore	Projects
	View, edit, copy, delete, replace, view status, configure status	Tasks
	Configure	Conditional workflow to task (customize tasks), customize project roles,
	View, mark as completed, attach artifact to, create, copy, edit, replace, delete	Process steps
	Create, edit, view, copy, filter, delete, attach to process steps	Artifacts for assigned projects
	Connect to AM to submit one time Task	Submitted Tasks (scans or script execution) identified in task.
	Schedule AE to Connect to AM to obtain results on a periodic bases	Results for previously identified task

User Security Role	Operations	TSF data
	Create, edit, import, export, push to Asset Manager, assign labels	Scripts
	Publish, configure, format, view	Documents
	Digitally sign	Documents
	Digitally sign	Reports
	Import	Certificates
	Configure own profile	Reset own password, notification settings, stored backups, inbox, set default page.
Security Administrator	View	Artifacts
	Configure, view, export, clear	Audit Logs
	View	Backup files
	View	Document
	View	Folder's projects
	View	Folders
	View	Job queue
	View	Job schedule
	View	Online users
	Change	Own Password
	View	Password Policy settings
	View	Process steps
	View	Projects
	View	Publisher queue
	View	Reports
	View	Scan jobs
	View	Scan job results
	View	Scripts
	View	System settings
	View	Task's chain of approval
	View	Task's history
	View	Task's state
	View	Tasks
	View	Template folders
	View	Templates
	View	Vulnerability alerts
	View	Assessment Engine Database
	View	Assessment Engine settings
	View	Assessment Engine user accounts
Executive	View	User Accounts
	View	Publisher queue
	View	Job schedule
	View	Job queue
	View	Online users
	View	Folders
	View	Projects
	View	Templates
	View	Tasks
	View	Task's chain of approval
	View	Process steps
	View	Subprocesses

User Security Role	Operations	TSF data
	View	Artifacts
	View	Backup files
	View	Document
	View	Reports
	Configure own profile	Reset own password, notification settings, stored backups, inbox, set default page.
Power User (Management functions limited to assigned projects)	Create, edit, view, copy, filter, delete, attach to process steps	Artifacts for assigned projects
	Add	Conditional workflow to task for assigned projects
	Publish, configure, format, view, download	Documents for assigned projects
	Digitally sign	Documents for assigned projects
	View	Job queue for assigned projects
	View	Job schedule for assigned projects
	Change	Own Password
	View, mark as completed, attach artifact to, create, copy, edit, replace, delete	Process steps for assigned projects
	Implement	Project controls for assigned projects
	Review, accept	Project registration requests for assigned projects
	Add, edit, copy, replace, delete	Project role for projects assigned projects
	Assign	Project to a user account assigned projects
	Create, activate, edit, reset, move, backup, restore	Assigned projects
	Link	Assigned projects
	View	Publisher queue for assigned projects
	View, generate, save	Reports for assigned projects
	Digitally sign	Reports for assigned projects
	Create, configure, add to project, delete, schedule, monitor, run on command	Scan jobs for assigned projects
	View	Scan job results for assigned projects
	Create, edit, import, export, push to Asset Manager	Scripts for assigned projects
	Configure	Security classification markings for assigned projects *
	Configure	Task's chain of approval for assigned projects
	View	Task's history for assigned projects
	View, change	Task's state for assigned projects
	View, edit, copy, delete, replace	Tasks for assigned projects
	Import, view, create, activate, edit, reset, move, assign user to, backup, restore	Templates for assigned projects
	Assign	User account to project role for assigned projects

User Security Role	Operations	TSF data
User (Management functions limited to those functions allowed by the project role to which they have been assigned for a project in an assigned folder)	Create, edit, view, copy, filter, delete, attach to process steps	Artifacts if allowed by assigned project role
	Add	Conditional workflow to task if allowed by assigned project role
	Publish, configure, format, view, download	Documents if allowed by assigned project role
	Digitally sign	Documents if allowed by assigned project role
	View	Job queue if allowed by assigned project role
	View	Job schedule if allowed by assigned project role
	Change	Own Password
	View, mark as completed, attach artifact to, create, copy, edit, replace, delete	Process steps if allowed by assigned project role
	Implement	Project controls if allowed by assigned project role
	Create, activate, edit, reset, move, backup, restore	Projects if allowed by assigned project role
	Link	Projects if allowed by assigned project role
	View	Publisher queue if allowed by assigned project role
	View, generate, save	Reports if allowed by assigned project role
	Digitally sign	Reports if allowed by assigned project role
	Create, configure, add to project, delete, schedule, monitor, run on command	Scan jobs if allowed by assigned project role
	View	Scan job results if allowed by assigned project role
	Create, edit, import, export, push to Asset Manager	Scripts if allowed by assigned project role
	Configure	Security classification markings if allowed by assigned project role *
	Configure	Task's chain of approval if allowed by assigned project role
	View	Task's history if allowed by assigned project role
	View, change	Task's state if allowed by assigned project role
	View, edit, copy, delete, replace	Tasks if allowed by assigned project role
	Import, view, create, activate, edit, reset, move, backup, restore	Templates if allowed by assigned project role

**Application Note: The security classification markings for projects and documents are for advisory purposes only. The TOE and its underlying databases are single-level applications that do not separate data based on any label or classification.*

Table 6-6: Management of TSF Data (Asset Manager)

User Security Role	Operations	TSF data
Master Administrator	Configure	SCAP Content Update parameters
	View, edit	Asset inventories
	Configure	Asset Manager Database
	Configure	Asset Manager system settings
	Create, modify, delete	Asset Manager user accounts
	View	Asset test results
	View, export, clear, configure	Audit Logs
	Disable/enable	Certificate revocation check
	Import	Certificates
	Download from Xacta website	Scripts
	Download from external (NIST or MITRE)	CVE and CCE and CPR dictionaries SCAP Scripts
	Export	Detect Server certificates
	Configure	Detect Server connections
	Synchronize	Detect Servers
	Create, modify	Equipment matching rules
	Configure	Execution of digitally signed scripts only
	Configure	HostInfo agent properties
	Define	IP ranges
	Configure	LDAP user authentication
	Create, modify, delete	Login warnings
	Configure	Password Policy parameters
	Configure	PKI user authentication
	Disable/enable	Remote login for Asset Manager Master Administrator accounts
	View, generate, save	Reports
	Create	Scan job
	Disable/enable	Script library retrieval
	Configure	Script-based asset testing (tasks)
	Digitally sign	Scripts
	View, edit, import, export	Scripts
	Configure	Security classification markings *
	Configure	SNMP settings
	Configure	Windows Domain authentication
Administrator	View	Asset test results
	Create, modify, delete	Asset Manager user accounts
	Import	Certificates
	Download from Xacta website	CVE and CCE data (SCAP Content)
	Export	Detect Server certificates
	Configure	Detect Server connections
	Synchronize	Detect Servers
	Create, modify	Equipment matching rules
	Configure	HostInfo agent POC properties
	Define	IP ranges
	View, generate, save	Reports
	Create	Scan job
	Configure	Script-based asset testing (tasks)
	Digitally sign	Scripts (if given permission)

User Security Role	Operations	TSF data
	View, edit, import, export	Scripts
	Modify	Own password
Security Administrator	View	Asset inventories
	View	Asset test results
	View	Asset Manager Database
	View	Asset Manager system settings
	View	Asset Manager user accounts
	View, export, clear	Audit Logs (no logs)
	View	CVE and CCE data (SCAP Content)
	View	Detect Server connections
	View	Equipment matching rules
	View	HostInfo agent properties
	View	IP ranges
	View	Login warnings
	Modify	Own password
	View	Asset inventory, export plans
	View	Password Policy parameters
	View	Reports
	View	Scan jobs
	View	Scripts
User	View Export	Asset inventories equipment list/plans
	View	Asset test results
	Modify	Own password
	View/Generate	Reports on Asset and Test

**Application Note: The security classification markings for projects and documents are for advisory purposes only. The TOE and its underlying databases are single-level applications that do not separate data based on any label or classification.*

Table 6-7: Management of TSF Data (Detect Server)

User Security Role	Operations	TSF data
Master Administrator	Configure/View Application settings	Maintenance Time, Verbosity, how enter key behaves, define LDAP server connection
	Configure/View Audit settings	Enable/Disable audit, set record limit, syslog configuration
	Configure/View Security Policy settings	Password Policy parameters, master admin remote login restriction, preventing multiple logins, restrict non-PKI to local, enable/disable/configure certificate revocation checking.
	Configure/View Database settings	Detect Server Database (name, IP, database, credentials, port, SSL mode, # connections)
	Configure/View Support Services settings	Enable/Disable email support to either Xacta or local.
	Configure/View Login Warning	Warning Banner
	Select Security Markings	Security classification markings *
	Configure Security Markings	Customize default labels hierarchy, create new labels
	Configure/View Server Configuration	IP range restrictions, Asset Manager URL, Asset Manager Cert, Socket and Session Timeouts, # open handles, Agent Data age, enable/disable Legacy testing and support
	Configure SNMP settings	Enable/Disable SNMP Agent
	Create, modify, delete User Accounts, reset password history	Detect user security attributes: Account Name, Authentication Type, Active/Inactive State, and Password. Role automatically set to master admin.
	View Known Agents	HostInfo agent status
	View Test Scripts	Test scripts names and results
	View and delete Scan Jobs	Detect Server sessions (scans)
	View Sessions	Detect Server job schedules
	View and export Logs	Process log for Detect Server
	View, export, and clear Audit	Audit log for Detect Server

6.1.5.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[operations as specified in Tables 6-5, 6-6, and 6-7].***

6.1.5.3 FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles ***[***

Assessment Engine Security Roles:

- ***Master Administrator***
- ***Administrator***
- ***Security Administrator***
- ***Executive***
- ***User * (Privileges can be assigned to a user to create two special categories of Users. They are as follows)***
  - ***Project Administrator***
  - ***Power User***

Asset Manager Security Roles:

- ***Master Administrator***
- ***Administrator***
- ***Security Administrator***
- ***User ****

Detect Server Security Roles:

- ***Master Administrator***

].

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

Application Note: Although the Vendor uses the term "User" for administrative roles in their documentation, all of these "users" have access to selected management functions and TSF data. No user controlled data is created.

6.1.6 Class FTA: TOE access

6.1.6.1 FTA_SSL_EXT.1 TSF-initiated session locking

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL_EXT.1.1 The TSF shall lock an interactive session after ***[Master defined time interval of user inactivity]*** by disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL_EXT.1.2 The TSF shall require the following events to occur prior to unlocking the session: ***[user re-authentication].***

6.1.6.2 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components

Dependencies: No dependencies

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.1.7 Class FTP: Trusted path/channels

6.1.7.1 FTP_ITC_EXT.1 Partial Intra-TSF trusted channel among distributed TOE components

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC_EXT.1.1 The TSF shall invoke the Operational Environment to establish a trusted communication channel among its distributed component applications that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure using the encryption and certificate services from the Operational Environment.

FTP_ITC_EXT.1.2 The TSF shall use this trusted channel for all communication among its distributed application components.

6.1.8 Class RCA: Risk and compliance assessment

6.1.8.1 RCA_COL_EXT.1 Asset data collection

Hierarchical to: No other components

Dependencies: No dependencies

RCA_COL_EXT.1.1 The TSF shall be able to collect configuration information from the IT network assets on the target network via the following methods:

[

- ***Collect scans performed by the HostInfo Agents***
- ***Test scripts run by the HostInfo Agents***
- ***Detect scans performed by the Detect Servers***
- ***Importation of information from third-party asset discovery/vulnerability scanners***
- ***Importation of information from third-party enterprise management databases***

].

RCA_COL_EXT.1.2 At a minimum, the TSF shall collect and record the following information:

[

- ***date and time of the collection***
- ***HostInfo-generated host ID***
- ***computer name***
- ***network adapter configuration (MAC address, IP address)***
- ***computer model and serial number***
- ***operating system version***
- ***the outcome (success or failure) of the collection***
- ***administratively defined list of asset information***

].

6.1.8.2 RCA_EVL_EXT.1 Risk and compliance evaluation

Hierarchical to: No other components

Dependencies: RCA_COL_EXT.1

RCA_EVL_EXT.1.1 The TSF shall be capable of performing the following evaluation function(s) on the collected IT network asset data:

[

- ***Compliance assessment***
- ***Calculate risk levels based on number and severity of test script failures***
- ***Update and/or create Database Records based on Equipment Matching Rules***
- ***Automatically answer a Criteria Question by using an expression to compare collected data to a requirement***
- ***Link collected inventory data to applicable security requirements***

].

6.1.8.3 RCA_NOT_EXT.1 Asset security notifications

Hierarchical to: No other components

Dependencies: RCA_EVL_EXT.1

RCA_NOT_EXT.1.1 The TSF shall send a notification to ***[the user assigned to a project role that has been configured to receive notifications for an event(s) listed in Table 6-8]*** when ***[the event(s) listed in Table 6-8]*** occurs during the risk and compliance assessment process.

Table 6-8: Security Notifications

Event	Description
New Equipment Found or Existing Equipment Updated	a scan finds new equipment or when equipment in the database is updated
Software Collected	a scan retrieves software information
OS Collected	a scan retrieves operating system information
Risk Level Changed	a project's risk level changes
Document Publishing Finished	a document is published successfully
Subscription Notice	the subscription license for a project is about to expire
Test Result(s) Expired	a test result(s) expires
Assessment Status Changed	a project's assessment status has changed
Project Status Changed	a project's status has changed
Protection Level Changed	a project's protection level has changed
Assessment Status Expiration	a project's assessment/certification expires

6.2 Security Assurance Requirements for the TOE

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2 and taken from Part 3 of the

Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 6-9.

Table 6-9: EAL2 Assurance Components

Item	Class	Component	Component Title
1	ADV: Development	ADV_ARC.1	Security architecture description
2		ADV_FSP.2	Security-enforcing functional specification
3		ADV_TDS.1	Basic design
4	AGD: Guidance documents	AGD_OPE.1	Operational user guidance
5		AGD_PRE.1	Preparative procedures
6	ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
7		ALC_CMS.2	Parts of the TOE CM coverage
8		ALC_DEL.1	Delivery procedures
9		ALC_FLR.2	Flaw reporting procedures
10	ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
11		ASE_ECD.1	Extended components definition
12		ASE_INT.1	ST introduction
13		ASE_OBJ.2	Security objectives
14		ASE_REQ.2	Derived security requirements
15		ASE_SPD.1	Security problem definition
16		ASE_TSS.1	TOE summary specification
17	ATE: Tests	ATE_COV.1	Evidence of coverage
18		ATE_FUN.1	Functional testing
19		ATE_IND.2	Independent testing – sample
20	AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6.3 Security Requirements Rationale

6.3.1 Dependencies Satisfied

Table 6-10 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 6-10: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	Operational Environment*
2	FAU_GEN.2	User identity association	FAU_GEN.1	1
			FIA_UID.1	17 (H)
3	FAU_SAR.1	Audit review	FAU_GEN.1	1
4	FAU_SAR.2	Restricted audit review	FAU_SAR.1	3

Item	SFR ID	SFR Title	Dependencies	Item Reference
5	FAU_SAR.3	Selectable audit review	FAU_SAR.1	3
6	FCO_SIG_EXT.1-1	Generation of digital signatures (documents and reports)	FIA_UID.1	17 (H)
7	FCO_SIG_EXT.1-2	Generation of digital signatures (scripts)	FIA_UID.1	17 (H)
8	FCS_CKM.1	Cryptographic key generation	FCS_COP.1	10
			FCS_CKM.4	9
9	FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1	8
10	FCS_COP.1	Cryptographic operation	FCS_CKM.1	8
			FCS_CKM.4	9
11	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	14 (H)
12	FIA_ATD.1	User attribute definition	None	N/A
13	FIA_SOS.1	Verification of secrets	None	N/A
14	FIA_UAU_EXT.2	TSF user authentication before any action	FIA_UID.1	17 (H)
15	FIA_UAU.6	Re-authenticating	None	N/A
16	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	14 (H)
17	FIA_UID.2	User identification before any action	None	N/A
18	FMT_MTD.1	Management of TSF data	FMT_SMF.1	19
			FMT_SMR.1	20
19	FMT_SMF.1	Specification of Management Functions	None	N/A
20	FMT_SMR.1	Security roles	FIA_UID.1	17 (H)
21	FTA_SSL_EXT.1	TSF-initiated session locking	FIA_UAU.1	14 (H)
22	FTA_TAB.1	Default TOE access banners	None	N/A
23	FTP_ITC_EXT.1	Partial Intra-TSF trusted channel among distributed TOE components	None	N/A
24	RCA_COL_EXT.1	Asset data collection	None	N/A
25	RCA_EVL_EXT.1	Risk and compliance evaluation	RCA_COL_EXT.1	24
26	RCA_NOT_EXT.1	Asset security notifications	RCA_EVL_EXT.1	25

** Note: Reliable timestamps are provided by the hardware and OS of the platforms that host the TOE components. See OE.Time as defined in Table 4-2: Security Objectives for the Operational Environment.*

6.3.2 Functional Requirements

Table 6-11 traces each SFR back to the security objectives for the TOE.

Table 6-11: Mapping of TOE SFRs to TOE Security Objectives

Item	SFR ID	TOE Security Objective
1	FAU_GEN.1 Audit data generation	O.AuditGeneration The TOE will provide the capability to selectively create records of security-relevant events and associate these events with the user who caused the event.

Item	SFR ID	TOE Security Objective
2	FAU_GEN.2 User identity association	O.AuditGeneration The TOE will provide the capability to selectively create records of security-relevant events and associate these events with the user who caused the event.
3	FAU_SAR.1 Audit review	O.AuditReview The TOE will provide the capability for review of the audit information to authorized users via the TOE interfaces.
4	FAU_SAR.2 Restricted audit review	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.
5	FAU_SAR.3 Selectable audit review	O.AuditReview The TOE will provide the capability for review of the audit information to authorized users via the TOE interfaces.
6	FCO_SIG_EXT.1-1 Generation of digital signatures (documents and reports)	O.Sign The TOE will provide mechanisms to allow digital signing of files to prove the origin of the information contained within them.
7	FCO_SIG_EXT.1-2 Generation of digital signatures (scripts)	O.Sign The TOE will provide mechanisms to allow digital signing of files to prove the origin of the information contained within them.
8	FCS_CKM.1 Cryptographic key generation	O.CryptoComm The TOE will provide cryptographic functions for secure communications between TOE components
9	FCS_CKM.4 Cryptographic key destruction	O.CryptoComm The TOE will provide cryptographic functions for secure communications between TOE components
10	FCS_COP.1 Cryptographic operation	O.CryptoComm The TOE will provide cryptographic functions for secure communications between TOE components
11	FIA_AFL.1 Authentication failure handling	O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.
12	FIA_ATD.1 User attribute definition	O.Attributes The TOE will be able to store and maintain user attributes.
13	FIA_SOS.1 Verification of secrets	O.Password The TOE will be able to support an administrator defined password policy.
14	FIA_UAU_EXT.2 TSF user authentication before any action	O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.
15	FIA_UAU.6 Re-authenticating	O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.
16	FIA_UAU.7 Protected authentication feedback	O.ProtectAuth The TOE will provide protected authentication feedback.
17	FIA_UID.2 User identification before any action	O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.

Item	SFR ID	TOE Security Objective
18	FMT_MTD.1 Management of TSF data	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.
19	FMT_SMF.1 Specification of Management Functions	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.
20	FMT_SMR.1 Security roles	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.
21	FTA_SSL_EXT.1 TSF-initiated session locking	O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.
22	FTA_TAB.1 Default TOE access banners	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.
23	FTP_ITC_EXT.1 Partial Intra-TSF trusted channel among distributed TOE components	O.TransProtect The TOE will invoke the Operational Environment to provide a trusted communications path that provides for the protection of the data from modification or disclosure while being exchanged between TOE components.
24	RCA_COL_EXT.1 Asset data collection	O.Collect The TOE will collect configuration data from the IT network assets.
25	RCA_EVL_EXT.1 Risk and compliance evaluation	O.Analyze The TOE will be capable of analyzing the collected asset data to derive conclusions about risks and compliance of the IT network assets.
26	RCA_NOT_EXT.1 Asset security notifications	O.Notify The TOE will notify responsible personnel when designated events occur in the assessment process.

Table 6-12 demonstrates that the SFRs meet all security objectives for the TOE. Rationale for each objective is included in the table.

Table 6-12: All TOE Objectives Met by Security Functional Requirements

Item	Objective ID	SFR ID/Title	Rationale
1	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate	FAU_SAR.2 Restricted audit review	FAU_SAR.2 limits access to the audit information through the administrative GUIs.
		FMT_MTD.1 Management of TSF data	FMT_MTD.1 specifies the administrative functions and the TSF data on which they operate as they are available to each of the defined administrative (security) roles for each of the administrative interfaces of the TOE.

Item	Objective ID	SFR ID/Title	Rationale
	security attributes via the TOE interfaces.	FMT_SMR.1 Security roles	FMT_SMR.1 requires that the TSF maintain multiple administrative roles. The TSF is able to associate a human user with one or more administrative roles and these roles are used to restrict access to the administrative functions and TSF data.
		FTA_TAB.1 Default TOE access banners	FTA_TAB.1 requires that before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.
2	O.Analyze The TOE will be capable of analyzing the collected asset data to derive conclusions about risks and compliance of the IT network assets.	RCA_EVL_EXT.1 Risk and compliance evaluation	RCA_EVL_EXT.1 defines the evaluation functions that are performed by the TOE to analyze the collected asset data.
3	O.Attributes The TOE will be able to store and maintain user attributes.	FIA_ATD.1 User attribute definition	FIA_ATD.1 defines the attributes of users, including the username that is used by the TOE to determine a user's identity, the password used for authentication, the account type that determines a user's administrative role and the folders and projects assigned to that user which define the TSF data a user may access.
4	O.AuditGeneration The TOE will provide the capability to selectively create records of security-relevant events and associate these events with the user who caused the event.	FAU_GEN.1 Audit data generation	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that an administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event.
		FAU_GEN.2 User identity association	FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event.
5	O.AuditReview The TOE will provide the capability for review of the audit information to authorized users via the TOE interfaces.	FAU_SAR.1 Audit review	FAU_SAR.1 provides for the audit information to be able to be interpreted by the appropriate personnel.
		FAU_SAR.3 Selectable audit review	FAU_SAR.3 provides the functionality to make the interpretation of the audit information easier for the user.

Item	Objective ID	SFR ID/Title	Rationale
6	O.Collect The TOE will collect configuration data from the IT network assets.	RCA_COL_EXT.1 Asset data collection	RCA_COL_EXT.1 defines the information collected from the IT network assets and the methods by which it is collected.
7	O.CryptoComm The TOE will provide cryptographic functions for secure communications between TOE components.	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 defines the key generation parameters for the cryptographic operations used for secure communications
		FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 defines the method of destroying the keys used in the cryptographic operations used for secure communications
		FCS_COP.1 Cryptographic operation	FCS_COP.1 defines the parameters of the cryptographic operations used by the TOE for secure communications
8	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.	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 requires the TSF be capable of performing the specified security management functions.
9	O.Password The TOE will be able to support an administrator defined password policy.	FIA_SOS.1 Verification of secrets	FIA_SOS.1 defines the TOE's password policy including each parameter that can be configured by the administrator.
10	O.ProtectAuth The TOE will provide protected authentication feedback.	FIA_UAU.7 Protected authentication feedback	FIA_UAU.7 specifies that the user's password will be masked on input.
11	O.Notify The TOE will notify responsible personnel when designated events occur in the assessment process.	RCA_NOT_EXT.1 Asset security notifications	RCA_NOT_EXT.1 defines the events that generate notifications during the collection and analysis of the asset data and also defines the users to whom the notifications are sent.
12	O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.	FIA_AFL.1 Authentication failure handling	FIA_AFL.1 specifies that a user account will be disabled after a defined number of invalid login attempts thus preventing brute force attacks.
		FIA_UAU_EXT.2 TSF user authentication before any action	FIA_UAU_EXT.2 requires that all TOE users authenticate themselves to the TOE either through the TSF's authentication mechanism or by a mechanism in the Operational Environment that has been invoked by the TSF before being able to access any TOE functionality or data.

Item	Objective ID	SFR ID/Title	Rationale
		FIA_UAU.6 Re-authenticating	FIA_UAU.6 specifies the conditions under which a user must be re-authenticated.
		FIA_UID.2 User identification before any action	FIA_UID.2 ensures that every user is identified before the TOE performs any mediated functions.
		FTA_SSL_EXT.1 TSF-initiated session locking	FTA_SSL_EXT.1 specifies that a user session will be locked after a defined period of user inactivity.
13	O.Sign The TOE will provide mechanisms to allow digital signing of files to prove the origin of the information contained within them.	FCO_SIG_EXT.1-1 Generation of digital signatures (documents and reports)	FCO_ SIG_EXP.1-1 specifies how the TOE provides proof of origin via digital signatures for published documents and reports that it generates
		FCO_ SIG_EXP.1-2 Generation of digital signatures (scripts)	FCO_ SIG_EXP.1-2 specifies how the TOE provides proof of origin via digital signatures for scripts that it generates
14	O.TransProtect The TOE will invoke the Operational Environment to provide a trusted communications path that provides for the protection of the data from modification or disclosure while being exchanged between TOE components.	FTP_ITC_EXT.1 Partial Intra-TSF trusted channel among distributed TOE components	FTP_ITC_EXT.1 defines the TOE's role in secure communications between TOE components. The TOE invokes the Operational Environment to establish a secure channel that relies on encryption and certificate services provided by the Operational Environment. The TOE then uses only this logically distinct and trusted channel for component to component data transmissions.

6.3.3 Assurance Rationale

Evaluation Assurance Level EAL2 was chosen to provide a moderate level of assurance due to the low level threat of malicious attacks.

7 TOE Summary Specification

7.1 IT Security Functions

Section 7.1 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.11: Logical Scope of the TOE .

The following sub-sections describe how the TOE meets each SFR listed in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Functions	Sub-Functions	SFRs
Security Audit	SA-1 Audit Generation	FAU_GEN.1
		FAU_GEN.2
	SA-2 Audit Review	FAU_SAR.1
		FAU_SAR.2
		FAU_SAR.3
Proof of Origin	PO-1 Generation of digital signatures	FCO_ SIG_EXP.1-1
		FCO_ SIG_EXP.1-2
User I&A	IA-1 User Login Security	FIA_AFL.1
		FIA_SOS.1
		FIA_UAU.7
		FTA_TAB.1
	IA-2 User Security Attributes	FIA_ATD.1
	IA-3 User Identification & Authentication	FIA_UAU_EXT.2
		FIA_UID.2
	IA-4 User Re-authentication	FIA_UAU.6
		FTA_SSL_EXT.1
Security Management	SM-1 Management Functions	FMT_SMF.1
	SM-2 Management Security Roles	FMT_SMR.1
	SM-3 Management Access Control	FIA_ATD.1
		FAU_SAR.2
		FMT_MTD.1
		FMT_SMR.1
Trusted Channels	TC-1 Trusted Communications	FCS_CKM.1
		FCS_CKM.4
		FCS_COP.1
		FTP_ITC_EXT.1
Risk and Compliance Assessment	RC-1 Asset Data Collection	RCA_COL_EXT.1
	RC-2 Risk and Compliance Evaluation	RCA_EVL_EXT.1
	RC-3 Asset Notifications	RCA_NOT_EXT.1

7.1.1 Security Audit Functions

7.1.1.1 SA-1: Audit Generation

(FAU_GEN.1, FAU_GEN.2)

The TOE generates audit records of security significant events and associates each auditable event with the identity of the TOE user account that caused the event. The TOE provides a decentralized auditing functionality. The Assessment Engine, the Asset Manager and each Detect Server generate its own audit records which are stored in the database associated with each of these components and subsystems. The events recorded for each TOE component are listed in Table 6-2: Auditable Events.

The TOE will audit the creation, deletion and modification of database records for the database objects listed in the following table. The database objects that are relevant for these audit events also depend on the TOE component and subsystem.

Table 7-2: Object List (for Database Create, Update and Delete Events)

Component (Subsystem)	Database Object		
Assessment Engine	Account	EquipmentImportRule	RequirementParameter.Answer
	Acronym	EquipmentImportSetGroupRule	RiskElement
	Alert	Folder	RiskLevel
	Alert.Associated	Help	RiskSnapshot
	Appendix	Location	Role (project role)
	Application	Location.SET_Threats	SampleDoc
	Application.Alias	Lookup	Scan
	Assignment	Milestone	ScriptData
	AutomatedTest	OptionList	SecurityDataCategory
	Barrel	Os	SecurityDataType
	Bucket	Os.Alias	SiteArtifact
	CheckList	Permission	Software
	CheckListEntry	PersistentSchedule	SSAA
	CheckListGroup	POAItem	SysDataFlow
	CheckListQuestion	Prereq	SysInterface
	CheckListQuestion.Answer	Project	SystemUser
	ChoiceOption	ProjectArtifact	Task
	Content	ProjectArtifact.Link	Task.SET_Psteps
	Criteria	ProjectAttributes.Data	TaskState
	Criteria.Status	ProjectHead	Test
	Definition	ProjectPersonnel	TestProc
	Document	PStep	TestProc.SET_Lookup
	DocumentFigure	Reference	TestResult.class
	DocumentIncluded	Regulation	Threat
	DocumentReference	RemoteServer	Vulnerability
	Equipment	ReqCriteria	
	Equipment.Property	Requirement	
	Equipment.SET_Application	Requirement.SET_Tests	

Component (Subsystem)	Database Object		
	EquipmentGroup	Requirement.Status	
	EquipmentImportMatchRule	RequirementParameter	
Continuous Assessment (Asset Manager)	Account (Wrapper for the User object)		
	GenericServer (A Virtual Detect Server)		
	Help		
	PersistentSchedule (Schedulable objects such as ScriptExecutionTask and Scanner)		
	Scanner (i.e. the object type that includes Detect Discovery, 3rd Party Discovery/Vulnerability Scanner Interfaces)		
	Server (A Detect Server)		
	User (Contains personal User attributes)		
Continuous Assessment (Detect Server)	Account (Wrapper for the User object)		
	Help		
	PersistentSchedule (Schedulable objects such as ScriptExecutionTask and Scanner)		
	Scanner (i.e. the object type that includes Detect Discovery, 3rd Party Discovery/Vulnerability Scanner Interfaces)		
	Self (A Detect Server)		
	User (Contains personal User attributes)		

The Audit Policy Settings page of the administrative GUIs lets Master Administrators and Security Administrators manage each of these audit logs. Enabling the audit logs allows viewing of all application activity by clicking on the Administration> Audit link. Each of the three types of audit logs mentioned above may be configured differently through the appropriate administrative GUI. That is, the Assessment Engine audit log is managed through the Dashboard and the Asset Manager and each Detect Server log is managed through the corresponding GUI.

The following fields are recorded in the Assessment Engine, Asset Manager and Detect Server audit logs:

- **Timestamp** (date and time of the event)
- **Subject Identity** (username and administrative role – if applicable)
- **Remote Address** (address of remote terminal - if applicable)
- **Folder Name** (if applicable)
- **Customer ID** (for subscription/license based projects - if applicable)
- **Project Name** (if applicable)
    - **Type of Event** (event name)
- **Event Description** (includes additional details about the event:
    - o event outcome
    - o name of the application settings field that has been modified, and the new value to which the field has been set – for change of security settings events
    - o name of user who signed scripts, date signed, which scripts were signed and the distinguished name within the certificate – for script signing events)

Audit Records Limit sets the maximum number of log entries. By default, this is set to 10,000, the recommended maximum. If the limit is exceeded, all excessive records (oldest first) will be

written to a zipped Microsoft Excel file stored on the application server's file system the next time the application's housekeeper feature runs. Excessive records will be deleted from the Application Database after the housekeeper runs. Audit logs are stored under

\\Program Files\Xacta\Applications\App\engine\ webapps\xacta\logs

in an Excel file which is zipped and named

"AutoAuditLogBackup<MM_dd_ yyyy_hh_mm_ss_a>.zip".

Changes to the audit records limit will only take effect after Housekeeping has run.

Only Master Administrators and Security Administrators can clear the audit logs. Clearing an audit log cannot be undone. To save the information in an audit log, it must be first exported to an Excel file before clearing. Another means of exporting the audit trail is to enable Write Audit to Syslog which sends audit records to a specified system log host, allowing access to the audit information outside the scope of the TOE. Configuring the Audit Records limit, enabling/disabling the Write audit to Syslog feature, exporting and clearing the audit logs is done through the management functions of the Dashboard and the Asset Manager and Detect Server GUIs.

Note: The administrator is responsible to perform periodic backups of the audit data to prevent loss of data.

Operational Environment Support

SA-1: Audit Generation is supported by the Operational Environment through:

- Protection of the stored Audit Records through the RDBMS interfaces
- Protection of log files through the operating system interfaces
- Logging to an optional Centralized Syslog Server or the local Server's Syslog
- Viewing Syslog
- Reliable timestamps for the audit records

7.1.1.2 SA-2: Audit Review

(FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

The TOE allows only Master Administrators and Security Administrators to view all events recorded in the Assessment Engine, Asset Manager and Detect Server audit logs. The View Logs page of the corresponding administrative GUI (Dashboard, Asset Manager GUI or Detect Server GUI) displays the significant application and server events for each of the TOE components and subsystems listed above. Each log can be filtered to display only administratively specified information and can also be exported to a Microsoft Excel file.

The audit logs can be filtered by User Name, Project Name, Event Name, Time span (Start Date, End Date), or a Relevant Term (Description) that is entered through the appropriate administrative GUI.

The audit logs also have advanced filter options for criteria-specific searches. One or more of the following parameters can be entered for a detailed search. The available search parameters are:

- **User Name** - The user filter box is a drop-down list that displays a list of all the TOE user accounts present in the application. This parameter instructs the audit log to display only the activities and events that relate to the selected account.
- **Project Name** - The project filter box is a drop-down list that displays all the projects in the application. This parameter instructs the audit log to display all project-related events.
- **Start Date and End Date** - (mm/dd/yyyy or text, e.g. June 21, 2006). These parameters instruct the audit log to display only the activities and events that occurred on or between the dates entered.
- **Description** – A keyword or phrase for an event. The audit log will use this to retrieve and display all events that have matching text in their title or description contents.

The audit records are presented in a spreadsheet format. Each column has a header cell that when selected (left mouse click) orders the audit log alphabetically based on the columns record field.

7.1.2 Proof of Origin Functions

7.1.2.1 PO-1: Generation of digital signatures

(FCO_ SIG_EXP.1-1, FCO_ SIG_EXP.1-2)

The TOE provides digital signature functionality to supply proof of origin for published documents (.pdf), reports (.pdf) and scripts. Acrobat Reader is used only to view documents and display the signature in the Signature field. Acrobat Reader is not required for the TOE to apply signatures to a .pdf document, .pdf report, or script.

Digitally Signing Documents and Reports:

This feature is available only at the Published Documents process step and is applicable only to PDF documents. This feature provides users the ability to sign PDF documents that are either published by the Assessment Engine or generated as one of its reports. Signing adds additional security to files - not just for copyright protection, but for the end users to see that the content of the document hasn't been altered. End users can monitor the signer of the PDF document using Adobe Acrobat or any capable PDF viewer.

Published documents and reports in PDF format can be signed using the Dashboard. Users have the option of displaying the signature field in the document generated. A PDF document with a signed status is still open for signing and modification, though these activities are monitored using a PDF viewer such as Acrobat. A PDF document with a certified status does not allow further changes on the document.

A signature field, if selected as visible, will appear on the bottom left of the generated PDF document. If a PDF document is signed, the Signature Panel of Acrobat will always display details about the digital signature even if the signature field is not visible.

Document signing is constrained by the signing capabilities of PDF's "binary" file format which allows creation of digital signatures only by either Common Access Card (CAC) signing (PKCS11) or signing via the PKCS12 format, i.e. .pfx or .p12 file format. The cryptographic functionality used for document signing is asymmetric-key encryption using SHA1WithDSA, SHA1WithRSA and is provided by either a CAC hardware module or a Browser cryptographic module. The CAC hardware module and drivers and/or the Browser crypto modules used are in the operational environment

Digitally Signing Scripts:

Signing scripts involves generating a digital signature and associating that signature with the script it signs. By signing a script, the administrator certifies that the script is valid and poses no security risk, and that the script was not modified before reaching the end user or HostInfo agents.

By default, Asset Manager is configured to prevent unsigned scripts from being executed. Unsigned scripts will not be passed on to HostInfo agents. This is a security measure designed to support non-repudiation (i.e., the concept of binding data to a person via their digital signature), an important aspect of security. Asset Manager can be configured to allow both signed and unsigned scripts, but doing so poses a potential security risk, so use caution.

Note: Individual HostInfo agents can also be configured to restrict usage to signed scripts only. If an agent is configured this way, then it will not execute unsigned scripts, even if Asset Manager is configured to allow them. Since Asset Manager is configured by default to disallow unsigned scripts and never send them to HostInfo agents, the agents are not configured to disallow them. Although this may seem contrary to the Asset Manager setting, it allows agents to be more easily managed and tailored, should your organization opt to allow unsigned script execution.

Only master administrators and administrators that have been given the privilege by the master administrator may sign scripts.

This privilege is specified in the account's properties, and includes the method that may be used to sign scripts.

Script signing supports signing via a soft certificate private key PKCS8 format, which is stored in a Java Keystore (JVS) file. Script signing (i.e. "plain-test" signing) also supports CAC (PKCS11) and the Personal Information Exchange (PKCS12) formats. The cryptographic functionality for script signing is asymmetric-key encryption using SHA1WithDSA, SHA1WithRSA and is provided by either a CAC hardware module or a Browser cryptographic module.

A user must provide a PIN or pass phrase to access his or her private key within Asset Manager's script-signing applet to sign one or more scripts. When a signature is saved, the certificate distribution process is automatically initiated and the script is updated in the Asset Manager Database. At this point the scripts will only reside in Asset Manager and will not be replicated to Detect until the "Apply Changes" button on Asset Manager's Script Library page is clicked.

If a signed script is modified in any way, its digital signature will be removed and it will be listed as unsigned. This is a security measure designed to ensure that any script changes are reviewed and officially approved before use. The fact that a script is signed confirms that it has been unchanged since the time it was signed.

See Table 1-5: TOE Cryptographic Functionality in Section 1.4.6 for references to the documents that describe the PKCS formats.

Operational Environment Support

PO-1: Generation of digital signatures is supported by the Operational Environment through:

- Use of PKI Infrastructure
- Use of an optional CAC as a security provider (This includes hardware and drivers that must be pre-installed)
- Adobe Acrobat digital signing functionality

7.1.3 User I&A Functions

7.1.3.1 IA-1: User Login Security

(FIA_AFL.1, FIA_SOS.1, FIA_UAU.7, FTA_TAB.1)

The TOE uses multiple means to ensure login security.

The TOE controls the strength of authentication passwords and authentication failure handling through the parameters in the Xacta password policy specified in Table 6-4: Xacta Password Policy Rules. These parameters control user access to the TOE's administrative graphical user interfaces.

The Master Administrators can manage the policies and settings for login, passwords, inactivity time-out, remote login, and PKI authentication using the Security Policy subsystem via the Dashboard and the Asset Manager and Detect Server GUIs. The following parameters may be set:

Maximum Failed Login Attempts sets the number of unsuccessful login attempts that may be made before the login account is disabled. The account becomes disabled if the failed login attempt count reaches the specified value. For example, a value of 3 is entered, then after three unsuccessful login attempts the account will be disabled. Disabled accounts can be reactivated only by an Administrator. If a value of zero is entered, the account will never be disabled. However, for security reasons, this is not recommended. This lockout feature does not apply to the Master Administrator accessing the TOE via the Console directly. Master Administrator access to the TOE via remote access is disabled via this mechanism. The default value is 3.

Failed Login Time Frame sets the time frame allowed for unsuccessful login attempts. An account will be disabled when the maximum failed login limit is met within the specified time frame. For example, the time frame set is 30 seconds and 3 maximum failed login attempts are allowed. If an individual logs in unsuccessfully 3 times within 30 seconds, his or her account is disabled. However, if the account holder does not use up the allowed number of failed login attempts (3, in the example) within the specified time frame, the failed login attempt counter is reset. That is, the individual is again allowed 3 unsuccessful login attempts. The default value is 30 seconds.

Note: Login at the console cannot be disabled for the Master Administrator account.

The following password policy parameters may be set to control access to the Dashboard and the Asset Manager and Detect Server GUIs when user authentication is performed by the TSF. The following do not apply for authentication by an external LDAP Server.

Prevent Multiple Logins is disabled by default. Enabling this feature prevents people from logging into the Assessment Engine using the same username and password, via multiple browser windows. This feature safeguards against duplicate login attempts and notifies the appropriate personnel about the violation. This feature can be set to notify the individual attempting to login with the username, the account holder who is currently logged in with the username, or both.

Password Expiration sets the maximum number of days before a password must be changed. If a value of zero is entered, the application will force the account holder to create a new password each time he or she logs in. The default value is 30 days.

Note: All account holders will be forced to change their passwords when they login for the first time.

Password History Cycle sets the number of new passwords that must be used before a previously used password can be reused. If a value of zero is entered, the application will allow an account holder to reuse the same password indefinitely. However, for security reasons, this is not recommended. The default value is 3.

Minimum Password Length sets the minimum number of characters required in all passwords. A password must consist of at least one character, and the default value is 8. For security reasons, it is recommended that the default number not be changed.

Password Character Classes determines complexity requirements for passwords. This setting requires passwords to contain characters from the specified number of character classes. The default value is 3. This means passwords must contain characters from at least three of the four available character classes. For security reasons, it is recommended that the default value not be changed to a lower value. The character classes include:

- Uppercase characters (A through Z)
- Lowercase characters (a through z)
- Digits (0 through 9)
- Special characters (e.g., @, &, !,;,+)

Password Class Counter is also used to determine complexity requirements for passwords. The default value is 1. This means passwords must contain at least 1 character from each of the specified number of character classes. For example, if *password character classes* was set to 3 and *password class counter* was set to 1, a valid password would be “Aa123456” because it contains at least three classes (an uppercase character, a lowercase character, and digits) and contains at least one of each class.

Passwords are hashed by the application server, using the SHA-1 Hash Algorithm and are stored in the RDBMS.

Master Administrator Access is used to disable remote login for Master Administrator accounts. By default unrestricted access is enabled. Although remote login can be disabled, the Master Administrator can never be disabled from logging in at the console.

Validate CSP applies only if PKI authentication is to be used to access the application. (See Section 7.1.3.3) The CSP (Cryptography Service Provided) Implementation is used by government agencies that require specific patches of Microsoft Internet Explorer. When set to "Yes", the TOE components will check whether those patches are properly installed and will deny a user's access if they are not.

Restrict Non-PKI logon to Console Only restricts non-PKI logon to console only. The default is disabled.

In addition to the use of the policy parameters defined above, the TOE enhances user authentication security by masking the password upon input for username/password authentication. For PKI authentication no password is shown, only a non-editable display of the CAC subject (TOE user account name). The TOE can also display a warning message at login. Master Administrators can select the warning message to display on the login page from a list of pre-defined warnings or create a new warning message using the Login Warning page of the administrative GUIs.

Operational Environment Support

IA-1: User Login Security is supported by the Operational Environment through:

- Use of PKI Infrastructure including keystore
- Protection of the stored password through the RDBMS interfaces
- Encryption support

7.1.3.2 IA-2: User Security Attributes

(FIA_ATD.1)

The TSF maintains the following security attributes for TOE user accounts (Users of the Dashboard, Asset Manager and Detect Server GUIs for access to administrative functions and TSF Data).

- **Account Name** (Login Name / Username)
- **Account Type** (Administrative Role / Security Role) – See Section 7.1.4.2)
- **Authentication Type** (Password and/or PKI)
- **Active/Inactive State** (Inactive accounts cannot access the system)
- **Account Disabled Date** (When this date has past, the account will become inactive and the account holder will not be able to logon to the system until a Master Administrator reactivates the account.)
- **Password**
- **Password Expiration** (Number of days before the current password will expire)
- **Password History**
- **Assigned Folder** (if any)
- **Assigned Project(s)** (if any)
- **IP Range** (if any)

The User Accounts page of the Dashboard and the Asset Manager and Detect Server GUIs is used to create and modify all accounts. The content of this page varies depending on the Security Role assigned to the account. Master Administrators can see all accounts, while all others can only see accounts with administrative rights equal to or lower than their own.

7.1.3.3 IA-3: User Identification & Authentication

(FIA_UAU_EXT.2, FIA_UID.2)

Each individual must be successfully identified and authenticated with a username and password by the TSF or by an authentication service in the Operational Environment that has been invoked by the TSF before access is allowed to the TOE's administrative interfaces access is allowed to the TOE administrative functions (via the Dashboard, Asset Manager GUI and Detect Server GUI) and TSF data.

User accounts can be created via the Dashboard and the Asset Manager and Detect Server GUIs or may be imported from an external LDAP (Lightweight Directory Access Protocol) or Active Directory server. A user account must be created for each of the AE, AM, and DS servers individually. An account on one of the servers does provide access to the other servers.

Note: The LDAP or Active Directory server is not included in the TOE.

The TOE only enforces the requirement on the Dashboard, Asset Manager GUI, and Detect Server GUI. Any utility (Win32 or HostInfo Utility) requires an OS I&A for access.

For accounts created through the administrative GUIs, account authentication can be via Password and/or PKI (Public Key Infrastructure).

Password Authentication

If Password Authentication is selected, the parameters of the password policy as described in Section 7.1.3.1 IA-1: User Login Security apply. The credentials are passed through the secure SSL tunnel. A hash (using the SHA-1 algorithm) of the password is stored in the appropriate TOE component's and subsystem's database and is used as the reference for validating the entered password whenever an individual authenticates to the Assessment Engine, Asset Manager or Detect Server.

PKI Authentication

To enable basic PKI Authentication, the certificates of the Certificate Authorities are placed within the application's Tomcat keystore signifying it as trusted. These imported certificates are used by the application to establish that the certificate was signed by a trusted source. The CRL portion of the TOE user authentication process is separate and optional.

Individual accounts that have been created by an administrator must have their properties set to use PKI authentication in order to make use of this feature. Individuals with accounts configured to use PKI authentication must first configure their browser to use the required certificate. In Microsoft Internet Explorer, this is found under Tools > Internet Options > Content tab > Certificates. For Netscape, it is found under Edit > Preferences > Privacy and Security > Certificates. For account holders with PKI authentication set, the CAC subject (account name) from the certificate information will be displayed in the login box. For PKI authentication, no password is displayed and the account name is not editable upon user login.

Note: The certificates and keystores generated for one TOE component cannot be used for any other component. For example: certificates for the Assessment Engine can only be used for the Assessment Engine.

Importing User Accounts

User accounts may be imported from an external authentication server on the User Account Page of the Dashboard and the Asset Manager and Detect Server GUIs. The administrator uses a drop down menu to determine the type of authentication server they wish to use to import accounts (LDAP or Windows Active Directory). Administrators enter a username, password, and a search string to connect to and search the server. After searching, a dialog box displays users that match the search string, as well as the functionality for importing and creating a user for this external authentication server account.

An authorized administrator has to import the user account for each or the 3 main TOE component interfaces separately. LDAP or Active Directory can be a single source for controlling a user/password. (LDAP./ Active Directory maintains one account for a user). However, the user account (if the user has access to all 3 components) would have to be imported 3 times (once for AE, once for AM, once for DC).

LDAP Authentication

LDAP authentication allows the Assessment Engine, Asset Manager and Detect Servers to authenticate the imported account holders via Public Key Infrastructure (PKI) certificates, rather than by requiring them to enter a username and password. LDAP is not necessarily required for PKI Authentication, although it can be used to support Certificate Revocation List (CRL) checking. In both cases, accounts imported from an external authentication server and accounts created by an Administrator, the PKI infrastructure used for authentication is outside of TOE Boundary.

Active Directory Authentication

If the TOE has been enabled to use Active Directory authentication, users can login to the TOE using their domain account and password. For users with Active Directory accounts that have been imported into the Application Database, the user first logs on to the domain, then launches the TOE application (Assessment Engine or Asset Manager) from a browser. The user will see the TOE application's login page with the login name field containing the domain name grayed out (disabled) and the password field omitted. At that point the user just clicks the 'Login' button. The TOE will then check the user's domain credentials against the accounts in each subsystem's database. If the user exists in the database he is granted access to the TOE.

Both password and PKI authentication can be enabled simultaneously for a single user account. If this is the case, upon login, users will first be tested against PKI, and then against Windows Active Directory. If neither of these options is enabled they will be skipped. Users will finally be given a username/password login prompt if neither PKI nor Active Directory authentication was successful.

Any user authentication information stored in the TOE databases is either encrypted or hashed using the SHA-1 algorithm. This includes all passwords for local authentication; data used for authentication by an optional external authentication server (LDAP, Active Directory); and any passwords needed for access to the optional third-party Asset Discovery/Vulnerability Scanners and/or Enterprise Management Databases. The TOE does not store any passwords for the tested or monitored network assets

Operational Environment Support

IA-3: User Identification & Authentication is supported by the Operational Environment through:

- Use of an optional LDAP or Active Directory Server
- Use of PKI Infrastructure
- Protection of the stored password through the RDBMS interfaces
- Trusted communications implementation

7.1.3.4 IA-4: User Re-authentication

(FIA_UAU.6, FTA_SSL_EXT.1)

The Security Policy Settings of the Dashboard and the Asset Manager and Detect Server GUIs allows the Administrators to manage policies and settings for login, passwords, and inactivity time-out.

The Inactivity time-out enables a Master Administrator to enter the length of time before an account holder's session times out, due to a period of inactivity. After this time-out, the TSF will require the account holder to re-authenticate through the standard login procedures before being allowed any access to the TOE.

Note: This requirement is only enforced on the Dashboard, Asset Manager GUI, and Detect Server GUI. The users of the installation and maintenance utilities are not considered TOE Users and therefore are not subject to this requirement.

7.1.4 Security Management Functions

7.1.4.1 SM-1: Management Functions

(FMT_SMF.1)

The TOE is capable of performing the security management functions as defined in Table 6-5: Management of TSF Data (Assessment Engine), Table 6-6: Management of TSF Data (Asset Manager), and Table 6-7: Management of TSF Data (Detect Server) a (See Section 6.1.5.1 FMT_MTD.1 Management of TSF data).

The management functions for the Assessment Engine are accessible through the Dashboard. The management functions for the Asset Manager and the Detect Server(s) are available through the specific GUI for each subsystem.

All management functions provided by the Dashboard, Asset Manager GUI and Detect Server GUI are limited to the administrative roles as defined in Section 7.1.4.2 SM-2: Management Security Roles below. These interfaces required identification and authentication of the user by the TOE.

Operational Environment Support

SM-1: Management Functions is supported by the Operational Environment through:

- Trusted communication between the TOE and external servers.

7.1.4.2 SM-2: Management Security Roles

(FMT_SMR.1)

The TOE maintains administrative roles that determine the access an account holder has to the management functions and TSF data. All users of the TOE have access to management functions and TSF data and are considered administrators. The administrative role is determined by the account type attribute of an individual's account. The folder(s), project(s) and IP Range(s) assigned to the account also determine the account holder's permissions to the functions and data.

The access control procedures for the management functions and TSF data are described further in Section 7.1.4.3 SM-3: Management Access Control .

The user accounts for the Assessment Engine, Asset Manager and Detect Server are separate; a single user must have an account created for each management interface in order to use it. (See Section 7.1.3.3 IA-3: User Identification & Authentication for details of importing user accounts). The values of the account types (roles) maintained by the TOE depend on the management interface being used. The Dashboard (Assessment Engine), Asset Manager GUI and Detect Server GUI each support a different set of management roles to control access to their functionality.

Assessment Engine Security Roles:

- **Master Administrator**

  A Master Administrator has full access to the entire application and is able to create additional Master Administrators as well as all other account types. Only Master Administrators have access to all of the Assessment Engine's administrative functions. A Master Administrator account can only be deleted by another Master Administrator. A new Master Administrator (username "*madmin*") account is created during the installation of the product. Upon first login the *madmin* account will be forced to change the password created during installation. The *madmin* account must be disabled after another account with madmin privileges is created.

  By default, an account with the Master Administrator role can access the Assessment Engine from any remote terminal that has access to the TOE. Due to this type of account's unlimited permissions, it is required that after installation and initial configuration of the product that the login for the Master Administrators be restricted to local access only. This forces the login by those accounts to be done only at the Application Server's console.

- **Administrator**

  Administrators have permission/restrictions to view and edit any information to which they have access. Administrator accounts should be given to those who have a need to access, edit, or configure projects, continuous assessment settings, and reports.

  These administrators are restricted to certain folders. They can only create and modify projects and accounts associated with their folders. They may assign their projects to any user that is restricted to their folders. They can only view reports related to their

folders. These administrators can be deleted only by another administrator of equal or higher type and level/restrictions.

- **Security Administrator**

Security Administrators have read-only access to everything except the Audit page (Administration > Audit) of the Dashboard. Only Security Administrators and Master Administrators can view, export and clear the audit records.

- **Executive**

Executive accounts are similar to administrators, but have read-only access. Executive accounts are intended for managers who need to monitor progress, compliance, and risk levels. The application's reporting features are especially useful to executives. The reports provide information about compliance levels, risk posture, vulnerabilities, project status, equipment and software inventory, and much more.

Executive accounts can only view project registration requests.

- **Users**

User accounts are typically given to analysts who will be performing project assessments/certifications. Users typically must be assigned to a project in order to access it. They are able to edit the process steps in their projects, but do not have administrative rights over their projects. User access to projects is also restricted to the folders they have been given access to. For example, if a user is granted access to Folder A but not Folder B, he or she cannot be given access to projects that belong to Folder B. Users can also create project registration requests. Privileges can be assigned to a user to create two special categories of Users. They are as follows:

- **Project administrators:** These are users (regardless of restrictions) who have been given administrative rights for their project(s). Project administrators can modify their project in any way. Their privileges allow them to define roles, assign users to roles, create and edit tasks and process steps, and set up connections to an Asset Manager server in order to enable equipment inventory scans and Continuous Assessment. They may assign their projects to any user that is allowed access to the project folder.
    - **Power user:** Power users are similar to users, but also have the ability to review and approve project registration requests.

Asset Manager Security Roles:

- **Master Administrator**

Master Administrators have full read/write access to all the functionality of the Asset Manager GUI, and can be given the privilege to digitally sign scripts. A Master Administrator can also give script signing privileges to other administrators. A Master Administrator account is created during installation. A Master Administrator can create additional Master Administrators as well as the other Asset Manager account types.

- **Administrator**

Administrators have full read/write access to all Asset Manager management functions except the View Logs and Audit Log pages. Administrators may digitally sign scripts if they are given the privilege by the Master Administrator

- **Security Administrator**

The Security Administrator has the ability to view, clear, and archive Audit information.

- **User**

Users have read and write access to the Task List page and Home area of the Asset Manager GUI but are limited to read-only access to the Assets and Reports areas.

Detect Server Security Roles:

- **Master Administrator**

Master Administrators have full read/write access to all the functionality of the Detect Server GUI. More than one Master Administrator account may be created.

Note: Although the Vendor uses the term "User" for administrative roles in their documentation, all of these "users" have access to selected management functions and TSF data. No user controlled data is created.

7.1.4.3 SM-3: Management Access Control

(FAU_SAR.2 FIA_ATD.1, FMT_MTD.1, FMT_SMR.1)

All users of the TOE have access to management functions and TSF data as defined in Table 6-5: Management of TSF Data (Assessment Engine), Table 6-6: Management of TSF Data (Asset Manager), and Table 6-7: Management of TSF Data (Detect Server) (See Section 6.1.5.1 FMT_MTD.1 Management of TSF data). Therefore, all TOE users are considered administrators, however, access to these management functions and TSF data is controlled by account and project attributes.

The account type attribute assigned to an individual's account determines the administrative role and the management functions that may be accessed (See Section 7.1.4.2 SM-2: Management Security Roles).

The folder(s), project(s), and IP Range(s) assigned to an individual's account (if any) restrict the TSF data that may be accessed.

Administrators fall into several categories, depending on their account type and whether or not they are restricted to an assigned folder. Administrators have permission to view and/or edit any information to which they have access.

The functions that an administrator may perform are also limited by whether or not they have been assigned to any of the project role attributes of a project. Project role assignments are attributes of a project; they are not TOE user account attributes as defined in Section 6.1.4.2 FIA_ATD.1 User attribute definition.

- Project Administrators have administrative rights for that project regardless of their assigned project role.
- Power Users are similar to users, but also have the ability to review and accept project registration requests.
- Users can only be assigned to projects that exist within the folder to which they have been assigned. Users can only access a project if they are assigned project roles associated with that project.

Project roles are used to enforce workflow and restrict the tasks and actions an administrator can take within a project. There is no limit to the number of project roles a project can have and each role can be given a different set of permissions. Projects created by the TOE include a number of pre-defined project roles with basic access permissions. Only individuals assigned to a project role with the appropriate permissions can change the state of a task. Only individuals with project roles included in a task's chain of approval may approve it.

A Master Administrator, Administrator, or User assigned to be Project Administrator can assign one or more project roles to an individual only after he/she has been assigned to the project through the Dashboard.

IP Ranges are used to control an individual's access to the Asset Manager's inventory information. For example, a Master Administrator could create a "Finance Department" IP Range, specify the IP Range of the equipment that belongs to it, and then assign it to the appropriate Project Administrators. Only those Project Administrators can then see the Finance department inventory. This ensures that data security is maintained. IP Ranges must be assigned to each individual's account, with the exception of Master Administrators, Security Administrators and Executive accounts, who have access to all information, by default.

Operational Environment Support

SM-3: Management Access Control is supported by the Operational Environment through:

- Protection of the HostInfo Agent Configuration Utility

7.1.5 Trusted Channel Functions

7.1.5.1 TC-1: Trusted Communications

(FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_ITC_EXT.1)

The TSF includes a trusted communication infrastructure that provides trusted communication channels among its distributed application components. The 'trusted communication channel' among distributed application components ensures the two end points, (i.e., two components) are authenticated, their identity is associated to the data they transfer and that the data transferred is protected from modification and disclosure.

Establishment of these trusted communications channels depend on the functionality of both the TOE (for configuration) and the Operational Environment (for implementation).

Communications between the TOE components use the Transmission Control Protocol/Internet Protocol (TCP/IP). The Assessment Engine, Asset Manager and Detect Server are designed to communicate with each other via VRMI. VRMI ("Virtual Remote Method Invocation") was developed by Telos Corporation to facilitate a secure means for application-to-application communications. VMRI uses trusted certificates to authenticate and establish a trusted communications link between TOE components The Telos VRMI package uses a combination of Java's HTTP Servlet technology, SSL encrypted communication, Output/Input streams and Java Reflection to create a client-to-server request/response model. All communication occurs over TCP/IP and specifically over HTTPS.

Each TOE component code base that has features of a VRMI server has its own VRMI package that reflects the implementation classes for the server-side. The server-side VRMI component

also defines a Client interface by which VRMI clients can make calls to servers without knowing anything about the server implementation classes.

The client stub is sent with each VRMI call/request to the server (over SSL) and from that the matching server implementation call is made on the server-side, using Java Reflection technology.

Inter-application communications between the application servers (Assessment Engine –to– Asset Manager, Asset Manager –to– Detect Server, and Detect Server –to– HostInfo Agent) is also encrypted using SSL. The TOE uses either 3DES 128 bit, AES 128 bit, or AES 256 bit encryption for inter-application communications that meet the generation and exchange of session keys as defined in SSL version 3.1 or TLS version 1 protocol.

Communications between end-user browsers and the application servers is the same as AE-to-AM component communications. TLS version 1 or SSLv3 must be enabled at the client browser; otherwise, communication will fail (i.e. not be permitted). Communications between AM-to-DS and DS-to-Agents use mutual authentications schemes.

The RC4-128 w/ MD5 Hash algorithm is only used for encryption when communicating with an Oracle Database. The TOE also supports 3DES (168 bit key) encryption and DES (56 bit key) encryption for communications with Oracle.

Application components can be configured to use PKI certificates for end-user authentication. When end-user PKI authentication is not enabled, the Dashboard GUI and the Asset Manager and Detect Server GUIs may be accessed via username and password. (See Section 7.1.3.3 IA-3: User Identification & Authentication)

See Table 1-5: TOE Cryptographic Functionality for references to the cryptograph functions.

Operational Environment Support

TC-1: Trusted Communications is supported by the Operational Environment through:

- TCP/IP protocols

7.1.6 Risk and Compliance Assessment Functions

7.1.6.1 RC-1: Asset Data Collection

(RCA_COL_EXT.1)

Automatic and manually scheduled scanning is performed by the TOE to collect network asset information. Scan jobs and job schedules are created and edited by the Asset Manager's administrative GUI for each Detect Sever. Scan jobs tell the Detect Server what type of scan to perform (discovery, collect, vulnerability) and what areas of the network to scan. There is no limit to the number of jobs that can be created, and each may be configured differently.

Note: The Job Scheduler does not enforce any security decisions. Creation of scan and discovery jobs is part of the management functions that are within the scope of the evaluation. However, the invoking of the scheduled jobs at the correct time is not covered by the evaluation. Re-occurring scans and discovery jobs were successfully scheduled and executed to supply real-time information during testing.

At a minimum, the TOE collects and records the following information:

- date and time of the collection
- HostInfo-generated host ID
- computer name
- network adapter configuration (MAC address, IP address)
- computer model and serial number
- operating system version
- the outcome (success or failure) of the collection
- administratively defined list of asset information (i.e. vulnerabilities, running applications, installed applications, etc.)

Note: The correctness of the assessment scripts for the assessment task (suitability to task) is not part of this evaluation

The TOE collects information from IT network assets via the following methods:

Collect scans performed by the HostInfo Agents

A HostInfo Agent is an application that resides on a host computer. The agent is designed to collect data about its host and transmit it back to the Detect Server using encrypted Secure Sockets Layer (SSL) protocol. These agents must be configured to point to a Detect Server, provided with a trust store with the appropriate Detect Server certificate(s), and must have a polling interval specified. For Windows agents, this configuration is performed during installation; for OS X agents, configuration must be performed after installation using the HostInfo Configuration Utility.

The HostInfo Agents automatically perform Detect-Collect scans every time they check in with their Detect Server and return the results. A polling interval defines how often the agent should check-in with the Detect Server to see if it requires any information. Detect-Collect scans are used to gather information about a device, such as its configuration and software.

The HostInfo Utility can be used to manually retrieve host information from machines that are inaccessible to the Detect Server, or if HostInfo Agents cannot be installed due to a security policy. To use the HostInfo Utility, it must be executed directly from the network asset. It can be copied to a floppy disk/portable storage device or accessed from a shared network location and then executed on each network asset. The collected data would then be imported to the Assessment Engine.

Test scripts run by the HostInfo Agents

The Asset Manager subsystem has the capability to test the IT network assets. Asset testing allows for the automatic collection of data to be used in the evaluation process of a project task.

Asset Manager uses a library of customizable JavaScript scripts to test for host configuration. The script library contains scripts used to gather equipment information and perform automated testing. These scripts can be executed as part of an automated test or scan designed to collect equipment configuration and vulnerability information.

Scripts can be created or imported from other sources. Scripts can be written in JavaScript. The proprietary Xacta Automated Script Language (XASL) is being deprecated. Therefore, XASL is not included in the evaluation. Instructions for writing test scripts can be found in the product guidance.

The TOE supports all the standard JavaScript variables, objects, properties and methods except those related to internet browsing or dynamic HTML. JavaScript as used by the HostInfo Agents has been augmented by Xacta added extensions to simplify the creation of the test scripts by TOE users. The objects and variables in the extensions were created specifically allow the HostInfo Agents to collect the needed data for risk and compliance assessment. The new variables and objects implemented for the Xacta extensions are summarized in the tables below. Please see the user guidance *document Xacta® JavaScript Extensions Reference Manual for Version 4.0, Service Pack 8,* for details about these objects and their use.

Table 7-3: Xacta JavaScript Extensions – Variables

Variable	Description
host	The global variable host refers to the Host object.
log	The global variable log can be used to print messages for debugging purposes.
Result	This global variable represents the script result. It must be set to an object of type of TestResult. This object is transferred to the server as a result of the script execution.
agent	The global variable agent provides several methods and properties to configure the agent itself. Changes made by the methods are stored permanently to the agent's configuration file agent.properties.
OS_X	This global variable provides several methods unique to agents running under Mac OS X.

Table 7-4: Xacta JavaScript Extensions - Objects

Object	Description	Host Platform Requirements for Use
Application	Represents an installed application.	Microsoft Windows, Mac OS X 10.3 or above
CertificateInfo	Provides access to attributes of an X.509 certificate.	Supported on all platforms where Xacta HostInfo can be installed
Cpu	Represents a CPU.	Microsoft Windows NT 4.0 or above, Mac OS X 10.3 or above. On different platforms different properties of Cpu can be set.
Dictionary	Represents an object that maps keys to values. It cannot contain duplicate keys; each key can map to at most one value.	Supported on all platforms.
DiskPartition	Represents information about one disk partition in a disk partition table.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
DiskPartitionTable	Represents a basic disk partition table.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows 2000 Professional, Windows NT Server, Windows NT Workstation.

Object	Description	Host Platform Requirements for Use
DownloadFiles	Used to download files from remote servers to a local temporary folder. Its main purpose is to download and run programs.	Supported on all platforms.
EffectiveSubcategoryAuditPolicy	Provides access to the computed effective audit policy for all subcategories for the specified security principal. The effective audit policy is computed by combining system audit policy with per-user policy.	Microsoft Windows Vista, Windows 2008.
Exec	Allows execution of external programs. Exec objects are only available in scripts sent by Distribution Manager.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation, Mac OS X 10, Linux, Solaris.
EnvironmentVariable	Represents an operating system environment variable.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation, Mac OS X 10, Linux, Solaris.
FileInfo	Provides information about a file.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation, Mac OS X 10, Linux, Solaris.
FileStat	Provides information obtainable with stat(2) system call.	Linux, Solaris, Mac OS X.
Firmware	Represents the version attributes of the computer system's basic input/output services (BIOS) or firmware that is installed on the computer.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation, Mac OS X 10. Note. Under Mac OS X only version property is set.
GptPartition	Represents information about a GPT-style disk partition.	Microsoft Windows Vista, Windows XP, Windows Server 2003.
GptPartitionTable	Specifies partition information specific to GPT-formatted disks.	Microsoft Windows Vista, Windows XP, Windows Server 2003.
Host	Represents a computer connected to a network.	Microsoft Windows, Mac OS X 10, Linux, Solaris. Note. Property Windows is supported only for Microsoft Windows platforms.
MbrPartition	Represents information about one MBR (Master Boot Record) disk partition	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows 2000 Professional, Windows NT Server, Windows NT Workstation.
MntEntry	Specifies mounted file systems	Linux, Solaris, Mac OS X 10.
NetAdapter	Contains information about a particular network adapter on the local computer. One object is assigned per IP address and per MAC address	Microsoft Windows, Mac OS X 10, Linux, Solaris.

Object	Description	Host Platform Requirements for Use
OpenIpPort	Contains information about an open (for sending and receiving User Datagram Protocol (UDP) datagrams) port or active TCP connection.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
OS	Contains host operating system information.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation, Mac OS X 10, Linux, Solaris.
OsXApplication	Represents an installed application.	Mac OS X 10.3 or above.
OsXFramework	Represents a Mac OS X framework.	Mac OS X 10.3 or above.
OsXExtension	Represents a Mac OS X kernel extension.	Mac OS X 10.3 or above.
OsXProperty	Represents one property from a property list.	Mac OS X 10.2 or above.
OsXPropertyList	Represents Property Lists (frequently referred to as “plists” or Preferences) - files storingconfiguration settings for Mac OS X applications such as /Library/Preferences/com.apple.AppleFileServer.plist.	Mac OS X 10.2 or above.
OsXStartupItem	Represents a Mac OS X startup item.	Mac OS X 10.3 or above.
OsXVolume	Represents a mounted volume.	Mac OS X.
PhysicalDrive	Specifies information about a physical drive connected to the local computer.	Microsoft Windows, Mac OS X 10.
PointOfContact	Contact information stored by HostInfo on the computer about the person who can correct issues with this computer.	Supported on all platforms.
Product	Represents product information such as a model and a serial number.	Microsoft Windows, Mac OS X 10.3 or above.
PropertyFile	Allows the interpretation of a file as a set of key/value pairs which can be used for analyzing configuration files.	Supported on all platforms.
Sid	Represents Security ID (SID) - a structure of variable length that uniquely identifies a user or group on all Windows NT Implementations.	Microsoft Windows.
TestResult	Defines the results of script execution.	Supported on all platforms.
TextFile	Used to search a text file for a particular line(s). Once the object is created the file can be opened, lines matched by a regular expression can be read from the file, and the file can be closed.	Supported on all platforms.
Version	A utility class that compares versions represented by strings.	Supported on all platforms.

Object	Description	Host Platform Requirements for Use
Volume	Represents a volume on the computer.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows 2000 Professional.
Windows	Returns information about Windows OS.	Microsoft Windows.
WindowsAccountLockoutPolicy	Contains lockout information for users and global groups in the security database, which is the security accounts manager (SAM) database or, in the case of domain controllers, the Active Directory.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation
WindowsACE	Contains a set of access rights and a security identifier (SID) that identifies a trustee (user account or group account) for whom the rights are granted, denied, or audited.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsAudit	Analyzes the Windows operating system's auditing rules.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsAuditSubcategory	Specifies a security event type and when to audit that type.	Microsoft Windows Vista, Windows 2008.
WindowsExecutableImage	Represents a Windows image file.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsFileVersion	Contains version information strings.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsNetworkGroup	Represents data related to the computer network group or domain.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation
WindowsObjectRights	Contains rights assigned or revoked to/from Windows accounts for the Windows object such as a file or a share. It specifies the access particular users or groups can have to the object.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsPasswordPolicy	Contains data about the password policy set on the host computer.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsRegistryFile	Represents Windows system registry settings	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.

Object	Description	Host Platform Requirements for Use
WindowsRegistryKey	Represents the Windows registry key. It retrieves a list of subkeys and list of names of values of the key.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsRegistryValue	Used to get a Windows registry value	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsService	Represents current information about a Windows service.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsSystemAuditSubcategories	Allows retrieval of the system audit policy for all audit-policy subcategories	Microsoft Windows Vista, Windows 2008.
WindowsShare	Contains information about the shared Windows resource.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsUserAccount	Represents Windows user account information.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WindowsUserRight	Specifies user right assignments, accounts in an LSA object's database that hold a specified privilege or an account right.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation.
WMIQuery	Makes it possible to execute WQL queries to evaluate data from Windows WMI class instances such as Win32_BIOS.	Microsoft Windows Vista, Windows XP, Windows Server 2003, Windows 2000 Server, Windows NT Server, Windows 2000 Professional, Windows NT Workstation
UnixUserAccount	Provides information about a Unix user account found in /etc/passwd and /etc/shadow.	Linux, Solaris, Mac OS X 10.
UnixUserGroup	Provides information about a Unix user group found in /etc/group.	Linux, Solaris, Mac OS X 10.
UserSubcategoryAuditPolicy	Provides access to per-user audit policy in all audit-policy subcategories for the specified principal Method host.	Microsoft Windows Vista, Windows 2008.

The product supports both signed and unsigned scripts to be run (the default is to execute digitally signed scripts only). For this evaluation, script execution will be restricted to only digitally signed scripts to prevent the running of rogue scripts.

The Task List page of the Dashboard is used to create and manage automated testing tasks. When a testing task is created in the Asset Manager, it is sent to the Detect Server along with the appropriate test scripts. When a HostInfo Agent in the appropriate IP Range checks in with

its Detect Server, and a task is scheduled to run, the agent will execute the appropriate scripts and return the results.

Note: If HostInfo Agents cannot be installed due to network connection restrictions or security policies, the HostInfo Utility can be used to run the test scripts manually.

HostInfo SCAP Support

Security Content Automation Protocol (SCAP) (http://nvd.nist.gov/scap.cfm) is a government multi-agency initiative to enable automation and standardization of technical security operations, such as policy compliance checking. SCAP is based on several evolving standards: XCCDF, CCE, CVE, CPE, CVSS and OVAL.

Xacta HostInfo supports compliance checking by executing rules provided in SCAP-based checklists and saving results in XCCDF format.

Note: Currently, SCAP support is provided only for Windows.

Extensible Configuration Checklist Description Format (XCCDF) (http://nvd.nist.gov/xccdf.cfm) specification defines the format for exchanging security configuration information. XCCDF documents are used for describing configuration issues and vulnerabilities, including automatic compliance checking.

XCCDF is based on XML format. SCAP checklists that are described in XCCDF format are called benchmarks. Results of automatic compliance checking are stored in XCCDF format, as well. HostInfo can process an XCCDF benchmark document, apply the specified profile, and perform compliance checking in accordance with the rules in the XCCDF document. HostInfo can also include the input benchmark XCCDF with the resulting XCCDF document.

The XCCDF specification allows the use of different checking systems for automatic checks. HostInfo supports two checking systems: OVAL and Xacta HostInfo JavaScript (described above). This enables the use of two checking systems in the same XCCDF document.

Open Vulnerability and Assessment Language (OVAL) is an XML-based language for writing automatic tests or checks, called definitions. FDCC SCAP checklists include OVAL Definition documents. Definitions from the OVAL documents are referred from the XCCDF document rules to be used for automatic compliance checking. The CPE dictionary that is part of the SCAP checklist includes references to OVAL definitions that are able to verify that a particular product is installed. HostInfo executes OVAL definitions that are used in FDCC checklists for Windows.

FDCC SCAP checklists can be downloaded from http://nvd.nist.gov/fdcc/download_fdcc.cfm.

FDCC SCAP content for Windows XP and Windows Vista consists of one XCCDF file (fdcc-winxp-xccdf.xml), three OVAL definition files (fdcc-winxp-cpe-oval.xml, fdcc-winxp-oval.xml, fdcc-winxp-patches.xml), and the CPE dictionary (fdcc-winxp-cpe-dictionary.xml).

The following product components have received NIST SCAP validation:

- Xacta IA Manager: Continuous Assessment, Version 4.0 SP8 (SCAP Website lists as 4.8), Validation Date: June 5th, 2009
- Xacta IA Manager (Xacta HostInfo), Version 4.0 SP8 (SCAP Website lists as 4.8), Validation Date: March 19th, 2009

Information about the SCAP validation is available at: http://nvd.nist.gov/validation_telos.cfm

Note: While Xacta IA Manager: Continuous Assessment and Xacta HostInfo have themselves been SCAP validated, the product itself does not do SCAP validation. It provides support for commercial and government compliance to the customer.

Detect scans performed by the Detect Servers

Discovery - Detect scans are used to discover devices on the network and retrieve high-level information about each device, such as host name, IP address, and operating system. They are performed by the Detect Server(s) and do not require HostInfo Agents.

Optionally, the Detect Server can be directed to send SNMP requests to the equipment and devices in its specified IP range and SNMP "community string". These scan results are used to help determine the type of devices on the network. SNMP discovery scans are enabled through the Asset Manager administrative GUI by creating a Discovery Scan job. By default SNMP scans are disabled.

Importation of information from third-party asset discovery/vulnerability scanners

Vulnerability scans are used to search the network assets for vulnerabilities. The TOE via the Detect Server can collect the scan results for the following third-party asset discovery/vulnerability scanners:

- ISS Internet Scanner: a vulnerability scan that uses an ISS Internet Scanner database as the vulnerability source.
- ISS Site Protector: a vulnerability scan that uses an ISS Site Protector database as the vulnerability source.
- Nessus: a vulnerability scan using Nessus. A scan request will be submitted to the Nessus server, which will perform the scan and return the results.
- eEye Retina: a vulnerability scan that uses an eEye REM database as the vulnerability source.

The third-party scans are configured and controlled outside of the TOE. The scans results are pulled by the Detect Server from a scan repository.

Importation of information from third-party enterprise management databases

The TOE via the Detect Server can collect information from a third-party enterprise management software database such as Microsoft SMS or IBM Tivoli.

Operational Environment Support

RC-1: Asset Data Collection is supported by the Operational Environment through:

- Use of an optional third-party asset discovery/vulnerability scanner
- Use of an optional third-party enterprise management database
- Use of PKI Infrastructure
- Protection of data and script files through the operating system interfaces
- Trusted communications implementation
- Proper configuration of the platforms on which the HostInfo Agent is installed

7.1.6.2 RC-2: Risk and Compliance Evaluation

(RCA_EVL_EXT.1)

The compliance assessment performed by the TOE is based on the regulations that are selected (a standards template). The compliance functions only assess the regulation items that are applicable to the project. The compliance rating calculated by the TOE is strictly a ratio:

# of passed controls (derived from the test results mapped to the controls) /

# of relevant controls (based on the Template selected)

Example:

An administrator starts a project and selects a template for DIACAP which uses the 8500.2 requirement. There may be 100 different controls within that requirement but due to the environment only 50 of the controls are relevant. These 50 controls are mapped to 2 test scripts per control. Typically the first script checks for existence (i.e. does it have the control?) and the second script checks for content (i.e. identifies what the control contains). The tests are run. If 4 tests report a failure (typically there are only three responses: “Pass”, “Failure”, and “Failed to Execute”) and these four tests map back to 2 controls, the compliance rating would be 48 out of 50. If the four tests mapped back to 4 controls then the compliance rating would be 46 out of 50.

The TOE performs the following evaluation functions on the collected IT network asset data:

Calculation of risk levels based on number and severity of test script failures

Risk elements are derived from tests that have not been executed and from test failures. The risk elements are grouped so that a single element represents all of the failures within a specific security category, and lists individual failures. The application calculates a risk level for each element (i.e., high, medium-high, medium, medium-low, or low), based on the number and severity of the test script failures.

The update and/or creation of database records based on Equipment Matching Rules

Equipment Matching Rules prevent duplicate records from being created by determining whether the equipment to be imported is new or already exists in the Assessment Engine’s database records. If an imported piece of equipment is new, a new record is created for it. If it matches already existing equipment, the administrator can specify whether Assessment Engine should ignore the new equipment information or update the existing record with the new information.

Automatic answering of a Criteria Question by using an expression to compare collected data to a requirement

One or more Criteria Questions are associated with an individual requirement. The response for each Criteria Question(s) determines the method (manual or automatic) of establishing applicability. The “manual” method uses the response to the Criteria Question (i.e., yes or no) to determine whether or not the associated requirement is applicable to the project. The “automatic” method uses an expression to determine applicability by comparing a predefined value against the information collected.

Linking of collected inventory data to applicable security requirements

The lookup lists define the universe of hardware components, operating systems, and software applications that are displayed within a project. The definition of these elements helps the application link the system inventory collected from the network assets to specific security requirements and test procedures. This allows an administrator to customize three categories of information: equipment classes, operating systems, and software applications. Information within each category is hierarchical and allows the universe of known elements to be defined with as much or as little granularity as desired.

For example, the underlying Operating Systems definitions are used to link the project's equipment to the applicable security requirements and associated test procedures. Operating systems could be defined at a high level (e.g., Windows and Unix), or at a more granular level, (e.g., Windows could be subdivided into Windows 9x and Windows NT). Windows NT could be further divided into several different versions: Windows NT 3.51, Windows NT 4.0, Windows 2000, and Windows XP. Windows 9x could contain similar sub-elements: Windows 95, Windows 98, and Windows ME.

7.1.6.3 RC-3: Asset Notifications

(RCA_NOT_EXT.1)

Project roles can be configured to receive notifications when a significant event in the risk and compliance assessment process occurs, such as a change to the project or the completion of an asset scan. When these events occur, the account holder that has been assigned to the project role will receive notifications via their Inbox (which is available on the home page of the administrative GUIs) or e-mail, depending on how his/her preferences have been configured. The events that trigger the notifications are listed in Table 6-8: Security Notifications (See Section 6.1.8.3).

If email notifications are desired, an SMTP server must be available in the Operational Environment.

Operational Environment Support

RC-3: Asset Notifications is supported by the Operational Environment through:

- Use of an optional SMTP Server

7.2 TOE Protection against Interference and Logical Tampering

The TSF when invoked by the underlying host OS maintains a security domain that protects it from interference and tampering by untrusted subjects in the TOE's Scope of Control. The TOE's protected domain includes all TOE software components.

Access to system configuration data and management functions is controlled by an access control policy which is based on the TOE user's assigned security attributes.

An underlying assumption regarding the operation of the TOE is that it is maintained in a physically secure environment.

Because the TOE is a software-only TOE, it relies on the security functionality of the Operational Environment to provide complete protection.

The TOE relies on the Operating Systems of the TOE components host platforms to provide file access control and process separation at the OS level. It also relies on third-party RDBMS to protect the data stored in the Application and Continuous Assessment Databases. The Operational Environment is also used to ensure secure communications between TOE components and remote users via the SSL implementation, encryption of communications, and certificate authentication.

The administrator guidance provides information for the secure configuration of the TOE and its Operational Environment.

7.3 TOE Protection against Bypass of Security Functions

The TSF when invoked by the underlying host OS ensures that TOE Security Policy enforcement functions are invoked and succeed before each function within the TOE's Scope of Control is allowed to proceed. All TOE user operations are conducted in the context of an associated TOE user session. This session is allocated only after successful identification and authentication by the TSF or the TSF and Operational Environment working together. The TOE enforces a password policy if native password authentication is being used. The TOE can optionally invoke an external mechanism for user authentication (i.e. LDAP or Active Directory).The TOE also supports authentication failure handling and session termination after a designated period of inactivity. The TOE user session is destroyed when the corresponding TOE user logs out of that session.

Access to management functions and TSF data is controlled by a TOE user's assigned security attributes. Authorized TOE users can only view TSF data through the administrative interfaces and only after successfully identifying and authenticating themselves. Operations on TSF data are checked for conformance to the granted level of access, and rejected if not conformant based on the TOE user's security attributes.

TOE components use trusted communication for all transmissions whether components are installed in the standalone or the standard network (distributed) deployments. The trusted communications include communication to and from the agents.

In the CC configuration the agents are configured to only execute signed scripts. These signed scripts follow the AM to DS to Agent path where the signature must be applied at the AM. The signed scripts are never stored on the hard drive of the agent to prevent any script tampering or introduction of non-authorized scripts.