CA eHealth Performance Manager r6.1.2 (Product Code EHDVCP990) Security Target

Version 1.1
April 7, 2010

Prepared for:
CA
100 Staples Drive
Framingham, MA 01702

Prepared by:
Booz Allen Hamilton
Common Criteria Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090-2950

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level (EAL) 2 augmented with ASE_TSS.2.

1.1.1 ST Identification

ST Title:	CA eHealth Performance Manager r6.1.2 (Product Code EHDVCP990) Security Target
ST Version:	1.1
ST Publication Date:	April 7, 2010
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this ST provides identifying information for the CA eHealth Suite Version 6.1.2 ST. It includes an ST Introduction, ST Reference, ST Identification, TOE Reference, TOE Overview, and TOE Type.

Chapter 2 describes the TOE Description, which includes the physical and logical boundaries.

Chapter 3 describes the Conformance Claims made by this ST.

Chapter 4 describes the Security Problem Definition as it relates to Threats, Operational Security Policies, and Assumptions met by the TOE.

Chapter 5 identifies the Security Objectives of the TOE and of the Operational Environment.

Chapter 6 describes the Extended Security Functional Requirements.

Chapter 7 describes the Security Functional Requirements (SFRs).

Chapter 8 describes the Security Assurance Requirements (SARs).

Chapter 9 is the TOE Summary Specification (TSS), a description of the functions provided by CA eHealth Suite Version 6.1.2 to satisfy the Security Functional Requirements (SFRs) and the Security Assurance Requirements (SARs).

Chapter 10 provides a rationale, or pointers to a rationale, for security objectives, assumptions, threats, requirements, dependencies, and PP claims.

1.1.3 Terminology

The terminology used throughout this ST is defined in Table 1-1: Customer Defined Terminology and in Table 1-2: CC Defined Terminology. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Term	Definition
Administrator	The eHealth Administrator is empowered to configure the eHealth Suite, monitor deployment, user accounts and settings, and reporting options within the software. The eHealth Administrator is created during the initial installation and setup of the eHealth server. Note: The eHealth r6.1 guides refer to a System Administrator, Web Administrator and eHealth Administrator. The System Administrator is the OS administrator on the machine the TOE is installed on. In the evaluated configuration, the eHealth administrator who manages the OneClick for eHealth interface is also the administrator of the eHealth Web user interface. The term "Administrator" is used throughout this ST to refer to a user with one or more of these administrative privileges.
Discover key	A discover key is used to uniquely identify an element.
Discover Policy	In a Discover Policy, Administrators specify the types of devices to find and the specific configuration parameters associated with the element type to be monitored. New discover policies can be created on-the-fly by using the OneClick for eHealth interface.
Discovery	Discovery is the process by which real-world entities found on a network are recognized, and for which an element representation is then constructed.
Element	An element is a resource that eHealth polls and for which it collects data. eHealth polls two types of elements: statistics elements and conversation elements.
End User	An eHealth end user refers to the individuals for whom web accounts have been set up on the eHealth Suite by the eHealth Administrator. These users can view network node system settings, generate reports, and view other settings dependent upon the privileges assigned to them by the eHealth Administrator. Note: Once an end user has been given access to the OneClickEH interface, that end user becomes an Administrator.
Poller Configuration	Defines the information for each element such as the name, a polling rate (the frequency with which eHealth polls the element), and the agent type (the type of element that eHealth discovered) stored in the database.
Polling	Polling is the process of collecting statistics on network, system, and application data.
User	Used to identify end users and administrators of the TOE
User Policy	The User Policy is the policy by which the TOE allows or denies access to the functions in the Web user interface and the OneClickEH interface. Administrators must modify the permissions on the individual end user accounts accordingly. The User Policy is based on a Discretionary Access Control policy which is based on privileges assigned to users.

Table 1-1: Customer Specific Terminology

Term	Definition
Authorized user	A user who may, in accordance with the TSP, perform an operation.

Term	Definition
External IT entity	Any IT product or system, un-trusted or trusted, outside of the TOE that interacts with 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.

Table 1-2: CC Specific Terminology

Keywords: Network Analysis, Network Topology Management, Network Performance Management, TOE Overview, System and Application Management, Application Performance Management, End-to-End Infrastructure Management.

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-4: Acronym Definitions. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CGI	Common Gateway Interface
CLI	Command Line Interface
CPU	Central Processing Unit
CVAR	Custom Variable
DB	Database
DCI	Database Configuration Information
EAL	Evaluation Assurance Level
FR	Frame Relay
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MB	Megabytes
MIB	Management Information Base
OneClickEH	One-Click for eHealth
OS	Operating System
PVC	Permanent Virtual Circuit
RMON	Remote Network Monitoring
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
ST	Security Target
TSC	TOE Scope of Control
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
WAN	Wide Area Network

Table 1-3: Acronym Definitions

1.1.5 References

- CA eHealth Administration Guide r6.1
- CA eHealth Overview Guide r6.1
- CA eHealth Installation Guide r6.1
- CA eHealth Release Notes r6.1
- CA eHealth Reports User and Administration Guide r6.1
- Evaluated Configuration for eHealth Suite 6.1.2 version 1.0

1.2 TOE Reference

1.2.1 TOE Identification

CA eHealth Performance Manager r6.1.2 (Product Code EHDVCP990). This is specifically the Common Criteria version of eHealth, which includes a security hotfix and a set of supplemental instructions for configuring the TOE in accordance with its CC evaluated configuration. These supplemental instructions are included in a separate document, entitled “Evaluated Configuration for CA eHealth 6.1.2” and dated April 7, 2010.

The product code for the evaluated version of the TOE is **EHDVCP990**.

1.3 TOE Overview

The TOE is the CA eHealth Network Performance Manager 6.1.2 software which is a System, Application and Network Analysis and Reporting system developed by CA. The product consists of one server component (eHealth Server for enterprise infrastructure analysis) with three other integrated operational environmental components as follows:

- Oracle 10g Database for storage of system and report critical information (Operational Environment)
- Apache Web Server for user web and GUI interface (TOE)
- eHealth OS, Solaris 2.10, to provide access to resources (e.g., CPU, memory, disk, network) (Operational Environment)

During operation, the TOE is accessed via a web interface which allows the following functions to be performed:

- Design a gateway page as a portal to the site

- Design customized report pages for individual users
- Customize the eHealth Web site
- Access the OneClick for eHealth user interface
- View scheduled reports, including MyHealth reports.
- Run and view reports on demand.
- Perform policy-based discoveries of resources
- Manage polling errors
- Create and manage element groups and grouplist
- Control user access to reports, administrative functions, elements, groups, Live Health applications
- Add and manage scheduled discover jobs, as well as modify scheduled default system jobs
- Monitor and manage all eHealth systems
- Manage user accounts
- View the element hierarchy
- Discover elements
- Manage discover policies
- Manage Database Configuration Information (DCI) rules for use in Discover
- View discover logs
- Run reports

During initial setup of the TOE, a local command line interface is used to perform the following tasks:

- Start and stop the server
- Enable SSL communications

There are two mechanisms by which the eHealth web interface can be accessed: a standard web browser and the OneClick for eHealth component (OneClickEH). Using a web browser provides access to the TOE's ability to generate and display reports. The OneClickEH component adds the ability to manage user accounts and privileges, view audit data, and configure what devices the TOE monitors and how to poll them. The OneClickEH component is an IE-based executable for Windows that is used to send HTTPS requests to the TOE and display HTTP data. While it is downloaded from the eHealth server and required for interaction with the TOE, it is not considered to be a trusted application due to its ability to be decompiled and modified. As a result, the eHealth server does not place any trust in OneClick; similar to how a web browser is used, all authorizations are made on the server side.

Note: In the evaluated configuration, only the eHealth Web User Interface and the OneClick for eHealth (OneClickEH) interfaces are used. During configuration, the command line interface is used to start the server and enable SSL communications. Once this has been performed, it is not used operationally.

The eHealth Server is used to acquire, warehouse, analyze, display, and report on data from various nodes across a network. This allows the TOE to provide information to the Administrator for verification that client networks are online and functional. The eHealth Suite allows users to manage multiple IT platforms and architectures, and manage network services.

The TOE:

- Runs the discover process to find the elements to manage
- Uses discover logs to interpret discover results
- Manages the configuration information that eHealth stores about managed resources
- Organizes resources into groups to associate related resources for monitoring
- Generates eHealth reports to obtain information about the recent performance of resources on the network
- Uses eHealth reports and tools to determine the current status of resources and identify changes
- Provides customized eHealth reporting tools
- Adds and manages scheduled jobs for generating reports, running discover processes, and managing the database
- Manages the amount of space that the eHealth database uses to ensure that eHealth can continue to collect data and generate reports
- Monitors itself and determine if critical processes are running or if certain events have occurred on the eHealth system

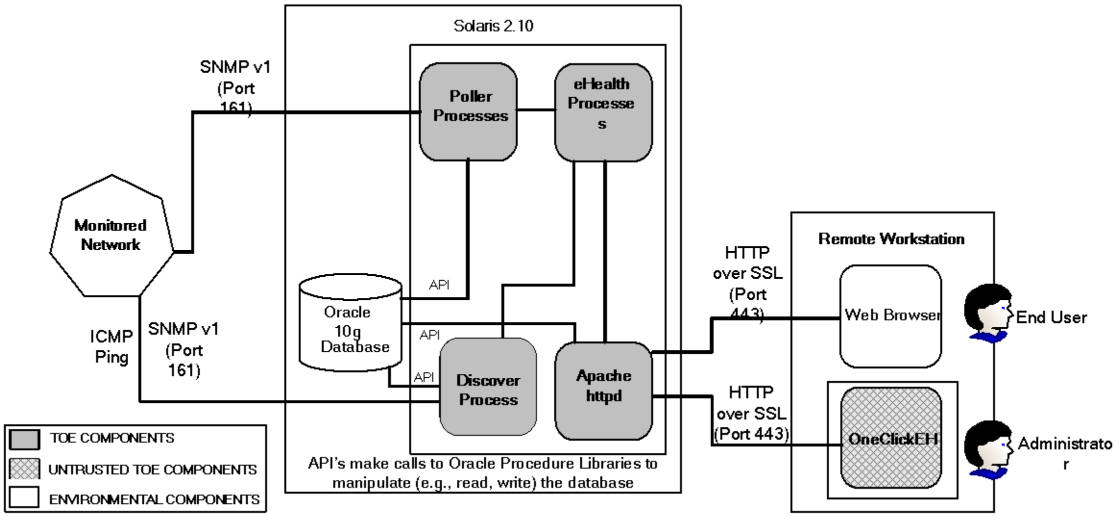


Figure 1 – TOE Boundary

As shown in Figure 1, Administrators and end users access the TOE remotely through a secure connection using HTTP over SSL through port 443. Both types of users must supply a username and password to the Apache web server v2.2.3 in order to access the TOE. The Web interface lets Administrators and end users view eHealth reports and other features from a remote system using a web browser. End users can see only those functions or pages of the Web interface that they are permitted to use. This is determined by the User Policy, which is described in Section 2.4.3. The eHealth Administrator controls access to the Web interface with Web user accounts and access settings, specifying which functions each end user can access.

Administrators use the web browser to launch the OneClick for eHealth (OneClickEH) component, which acts as the main administrative interface to the eHealth system. Once the OneClickEH component is launched, the web browser is no longer needed to perform administrative functions on the TOE. This component resides on the administrator's client machine, similar to a web browser. It uses HTTPS to interact with the TOE. Because it resides on a client machine, it is not considered to be a trusted executable. All requests initiated using the OneClickEH interface are therefore validated by the TOE once the requests have been communicated to the server. Once end users are given access to the OneClickEH interface, they are then considered Administrators. Through the OneClickEH interface, eHealth allows Administrators to monitor and manage the performance of networks, systems, and applications. These are done through polling and discover processes, which are described below.

Polling is the process of collecting statistics on network, system, and application data. An element is a resource that eHealth polls and for which it collects data. eHealth polls two types of elements: statistics elements and conversation elements. Statistics elements are devices and interfaces within the network. Conversation elements monitor traffic flow among nodes and applications using the network. Using the OneClick for eHealth interface, Administrators can view and manage all elements that eHealth is monitoring.

Discovery is the process by which real-world entities found on a network are recognized, and for which an element representation is then constructed. During the discover process, eHealth searches for resources with Simple Network Management Protocol (SNMP) agents at Internet Protocol (IP) addresses that Administrators specify. It then obtains information from the management information base (MIB) of each device and creates elements based on that information. Whenever possible, the discover process uses a discover key to uniquely identify an element. eHealth creates discover keys for newly discovered elements based on information that it obtains from the MIB at the device. When the discover process finds an element, it compares the discover key for the new element to the discover key for elements that are already in the database to determine whether the element is new.

When the Administrator saves the discover process results, eHealth stores element information in its poller configuration in the database. The poller configuration in the database information includes a name, IP address, SNMP index numbers, and other information needed to uniquely identify the element, poll it, and report on it. After installation, the discovery process can be scheduled to run at regular times to update information in the poller configuration in the database. The eHealth poller automatically collects data for any element in the eHealth database. When the TOE discovers an element, eHealth creates an entry for it in the poller configuration in the database. Each entry contains the element name, the configuration information that eHealth obtained, a polling rate, and the eHealth agent type. The polling rate specifies the frequency with which eHealth polls the element. eHealth has several polling rates. The default rate is five minutes. The eHealth agent type classifies the type of element that eHealth discovered. All collected data is stored in the Oracle 10g database.

eHealth records the results of the discover process in comparison to the existing poller configuration in the database in a log file. This discover log lists unresolved element changes to alert the Administrator to edit the elements in the database to prevent the loss of historical data and avoid polling the same element more than once.

Administrators use the OneClickEH interface to control the discover program, and for displaying the results. Administrators can also check on the status of the network by running reports such as At-a-Glance, Top N and Trend.

1.4 TOE Type

The TOE type for CA eHealth Suite Version 6.1.2 is Network Management. Network Management is defined by CC as follows: “Technology that helps to protect networks against malicious attacks that might deny access or use of the network. For example, the technology used to control access to network management centers and to protect network management transactions from various kinds of attacks.”

Network Management is the most appropriate designation given to the TOE from the list of TOE types made available by CCEVS. By managing the performance and behavior of network devices and looking for abnormalities, it is possible for the TOE to detect when devices are operating beyond their expected parameters, which could be evidence of compromise or attack.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

The scope and requirements for the evaluated configuration are summarized as follows: The eHealth Suite Version 6.1.2 software (i.e., the TOE) will be installed on the eHealth Server machine with the Solaris 2.10 operating system installed. The TOE will be installed on a physical machine (as opposed to a virtual one).

The Oracle 10g Database, base version 10.2.0.3, will communicate with the eHealth Suite Version 6.1.2 software and will be installed on the eHealth Server machine. Patches to this database will not be applied from Oracle—instead, the vendor will release their own database patches once internal testing ensures that Oracle updates are compatible with the TOE.

The installation and configuration process will be consistent with the Common Criteria supplemental installation guidance which is included with the distribution of the TOE.

The evaluated components of eHealth Suite Version 6.1.2 are identified below:

- Apache Web Server v2.2.3
- eHealth Processes
- Poller Processes
- OneClickEH interface
- Web user interface
- Discover Process

The TOE is expected to be installed in accordance with the "Evaluated Configuration for eHealth Suite version 6.1.2" that is included with the distribution of the TOE.

Table 2-1: Component Definitions defines each component of CA eHealth Suite Version 6.1.2.

Component	Definition
Apache Web Server v2.2.3	eHealth automatically installs an Apache web server and software to enable authorized users and Administrators to view eHealth reports and other features from any remote system using a web browser. The Apache Web Server v2.2.3 serves multiple purposes within the eHealth Suite. Primarily it serves as the platform upon which the web user interface and OneClickEH interfaces run. Administrators may log in to the OneClickEH interface and set up End User accounts as well as manage the TOE. User login information is encrypted in a configuration file and is stored and protected by the host Operating System on the eHealth Server. The Apache Web Server facilitates End

Component	Definition
	User access to eHealth reporting functionality to analyze data stored in the Oracle 10g Database. The Apache Web Server acts as the interface with the client machine and creates an instance of a program called nhWeb on the eHealth Server through the utilization of a Common Gateway Interface (CGI) script. The nhWeb invocation then serves as the link between the Apache Web Server and the Oracle 10g Database. It serves to translate form input values into parsed input for equivalent CLI commands.
eHealth Processes	eHealth Processes provides an interface to the information stored within the Oracle 10g Database. These processes are used to facilitate interactions with the eHealth Server received from remote workstations through the Apache Web Server component.
Poller Processes	eHealth Poller Processes provides the data collection for monitored devices. Information is collected a variety of different ways through the Poller Processes via the SNMP v1 protocol. The information is then stored by the Poller Processes to the Oracle 10g Database for future use.
OneClickEH Interface	The OneClick for eHealth (OneClickEH) interface acts as the main administrative interface to the eHealth system. The OneClickEH console, which interfaces with this interface, is launched from a web browser. The OneClickEH component displays a tree structure on the left with access to the administrative functions. On the right, it displays a high-level status summary. Note that the OneClickEH component is considered an evaluated component of the TOE because it is a required mechanism for administrative access that is distributed with the TOE, cannot be substituted for any other application, and because its interface to the server is a TSF interface. Similar to a web browser, the OneClickEH component is installed onto a client machine. The TSF has no ability to enforce the integrity of this client, so there is no way of verifiying its integrity save for re-installation.
Web User Interface	From the various tabs of the web interface, Administrators and authorized users can perform administrative functions, generate eHealth reports, and access numerous eHealth products.
Discover Process	During the discover process, eHealth searches for resources with Simple Network Management Protocol (SNMP v1) agents at Internet Protocol (IP) addresses that TOE administrators specify during installation.

Table 2-1: Component Definitions

2.2 Excluded from the TSF

The following optional products and components can be integrated with eHealth but are NOT included in the evaluated configuration. They provide no added security related functionality. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.2.1 Installed but Requires a Separate License

These components are installed with eHealth Suite v6.1.2, but they require a separate license and are therefore not included in the TOE boundary.

- **eHealth AdvantEDGE View** - eHealth AdvantEDGE View is the Web-based graphical user interface and element manager for use with SystemEDGE agents. eHealth AdvantEDGE View and SystemEDGE can be used separately or with eHealth for integrated performance and availability management across an infrastructure.

- **SystemEDGE** - SystemEDGE operates on a client or server system, continuously monitoring changing conditions and providing detailed information about the system's configuration, status, performance, users, applications, file systems, and other critical resources. SystemEDGE can be used as a stand-alone solution to monitor critical systems and applications or it can be used as part of an integrated eHealth solution. Features of SystemEDGE include Automatic Notification and Action, Top Processes, Asset Tracking, Integration and Small Footprint and Scalability. SystemEDGE agents can be deployed, licensed and managed with eHealth AdvantEDGE View, a graphical user interface and element manager.

- **SystemEDGE Agents** - The eHealth SystemEDGE agent operates autonomously. It lets Administrators offload the task of routine system monitoring from IT personnel to the systems where problems occur.

- **Distributed eHealth** - Distributed eHealth is a highly scalable solution for managing large infrastructures using a single integrated view across multiple eHealth systems. It lets Administrators monitor and manage up to one million elements across a worldwide network.

- **Integration Modules** - Integration modules help eHealth do either or both of the following:
    - Import configuration and performance data about network components from other software solutions. This data is then used by eHealth reports and Live Health.

    - Export intelligent alarms from Live Health to network management systems, letting Network Operations Center (NOC) administrators troubleshoot problems using the workflow with which they are familiar. In some cases, administrators can drill down from the network management system to eHealth reports to investigate the source of an alarm.

- **Live Health** - Live Health is a software solution that provides real-time fault, performance, and availability management for any of the eHealth components that have been purchased. When used with all components, Live Health provides real-time management capabilities across an entire IT infrastructure. It monitors the network, systems, and applications to detect faults, potential outages, and delays that can cause downtime and service degradation.
- **Remote Polling** - As an alternative to Distributed eHealth, a remote polling environment can be used. With remote polling, eHealth is installed on remote systems (called remote sites) and each site is set up to poll a set of elements. The database at each site contains data for the elements it is polling, and Administrators can manage those elements using eHealth. A central eHealth system retrieves information and performance data from the remote eHealth systems and periodically merges the data into one central eHealth database. From this central database, reports can be run for all elements. The central site can support up to 100,000 elements, depending on the system configuration and the reports that are run.

- **TrapEXPLODER** - CA eHealth TrapEXPLODER is a Simple Network Management Protocol (SNMP) management application that receives and filters SNMP trap messages and forwards them to other management applications on other hosts and ports. With CA eHealth TrapEXPLODER, Administrators can configure all devices to send traps to a central machine that can “explode” (forward) the traps to other management stations. TrapEXPLODER is an integrated part of Live Health and AdvantEDGE View.

2.2.2 Installed but Untrusted

These components are installed with eHealth Suite v6.1.2, but they are not part of the TSF because they are not trusted components.

- **OneClick for eHealth (OneClickEH) component** – The OneClickEH component is a proprietary executable binary that is downloaded from the eHealth server using the web user interface and is used to operate the TOE. It is not considered to be part of the TSF because the eHealth server does not grant it the ability to validate security operations on the client side. However, since it is necessary to use the OneClickEH component in order to perform operations on the TOE, it is still considered to be within the TOE boundary. It is untrusted because as a client application, it can be subjected to modification that cannot be detected or prevented by the TSF.

- **Command Line Interface** – The CLI is used to start the server and enable SSL communications. Once this has been done, it is the expectation that the TOE will be managed remotely using one of the graphical utilities. This is untrusted because it does not perform any security-relevant functionality while the TOE is operationally deployed. As a result, the CC guidance explicitly recommends against its operational use.

- **Motif Console** – The Motif console requires access to the OS account used to install the TOE, increasing the risk that the TOE can be modified out of band by a careless or malicious local user. All functionality of the Motif console which is security-relevant is replicated in the OneClick for eHealth interface. This is untrusted because it does not perform any security-relevant functionality while the TOE is operationally deployed. As a result, the CC guidance explicitly recommends against its operational use.

- **Reports Center** – Reports can be created through the Web User Interface. The Reports Center is not needed for this functionality. This is untrusted because it is out of scope of the TSF and was such was not tested.

- **Reports Scheduler** – This is accessed through the Motif console, which is not included in the evaluated configuration. This is untrusted because it is out of scope of the TSF and was such was not tested.

- **High Availability configuration** – High availability (HA) is a system implementation based on levels of redundancy that helps ensure a system or application can quickly come back online in the event of a failure. Highly available systems are often characterized by the ability of their components to fail over to backup systems in the event of a failure. This is untrusted because it is out of scope of the TSF and was such was not tested.

- **Disaster Recovery configuration** - An eHealth environment can be configured to integrate with the DR replication software CA XOsoft Replication. The replication software copies all eHealth, Oracle, and eHealth database files over the network from the active eHealth system to a standby system, often in another physical location. When an update is made to a file or directory on the active system, the changes are automatically replicated to the standby system. When there is a critical failure (data file corruption) or a disaster (hurricane, earthquake) on the active system, a manual failover to the standby system occurs, which then becomes the active system. This is untrusted because it is out of scope of the TSF and was such was not tested.

2.2.3 Not installed

These components are not installed with eHealth Suite v6.1.2 and are therefore not included in the TSF.

- **Traffic Accountant** - Traffic Accountant is an eHealth product that provides network traffic analysis and reporting for use with RMON2 probes, Cisco NetFlow and IPFIX.

- **Application Response** - eHealth Application Response measures actual, observed response time from the end user’s point-of-view.

- **Application Response Agents** - eHealth Application Response agents are installed on Windows-based client systems or terminal servers (such as servers for Citrix MetaFrame or Microsoft Windows Terminal Services). These agents measure the actual response times of transactions performed by end users for the monitored applications. The agents then aggregate this data into an average response time for each application. eHealth Application Response can also track response times for individual transactions and groups of transactions.

- **NSM Agents** – Unicenter Network and Systems Management (NSM) agents monitor critical business systems, helping to check for consistent performance and enhance system management. The eHealth suite of software can be used to poll these agents for performance data. eHealth provides Administrators with the ability to perform trend analysis, capacity planning, and proactive, real-time self-management.

- **Service Availability** – eHealth Service Availability is a plug-in module for the SystemEDGE agent. It manages and monitors response time and availability of Internet services such as Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP3), Domain Name System (DNS), Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), Packet internetwork groper (PING), TCP-connect, Active Directory, Dynamic Host Configuration Protocol (DHCP), File I/O, Internet Message Access Protocol (IMAP), Lightweight Directory Access Protocol (LDAP), Messaging Application Programming Interface (MAPI), Network Information Service (NIS), Simple Network Management Protocol (SNMP), SQL Query, Trivial File Transfer Protocol (TFTP), Virtual User, Generic and Custom.

- **Cisco IOS IP SLAs** - Cisco IP Service Level Agreement is bundled with equipment from Cisco Systems, Inc. This agent enhances the management and measurement of enterprise and service provider networks by testing service and response from Cisco routers to critical resources. When Cisco IP SLA is configured with eHealth, the Cisco router generates traffic to specified network resources, and measures the availability of the resource and response time between the router and that resource. Cisco IP SLA can also measure important metrics such as latency, packet loss, and jitter (the variation in delay between two successive packets in a simulated real-time voice or video data flow). These metrics are then stored in the eHealth database.

- **Juniper Real-Time Performance Monitoring (RPM)** - The Juniper real-time performance monitoring (RPM) feature monitors network performance between a Juniper router and a remote device. RPM sends probes between two network endpoints, and measures performance information including availability, packet response time and jitter.

- **Application Insight Modules -** eHealth Application Insight Modules (AIMs) are application-specific plug-in components for the SystemEDGE agent. With AIMs, SystemEDGE can provide more detailed monitoring and management of business-critical applications that reside on the target system.

- **SMTP Integration** - an SMTP server is used to send notifications when Live Health is being used. Since this component has been excluded, SMTP integration is also excluded.

2.3 Physical Boundary

The TOE includes the following components:

- Apache Web Server v2.2.3
- eHealth Processes
- Poller Processes
- OneClickEH component
- Web User Interface
- Discover Process

The TOE runs on a machine running Solaris 2.10 that meets or exceeds the physical hardware requirements as outlined in section 2.3.1. The physical boundary of the TOE includes the eHealth Suite Version 6.1.2 server software as depicted in Figure 1 and is responsible for implementing the TOE's security functional requirement components. As seen below, the Oracle 10g database is an environment component installed on the same physical server before the eHealth TOE is installed. The TOE interface to Oracle used to manipulate the database is done via an API that performs Oracle Procedure Library calls. The Oracle listener is required to be active in order for the TOE to function, but its potential risk to security can be mitigated through correct configuration. The evaluated configuration document that accompanies the CC-certified version of the TOE contains instructions on how to accomplish this.

2.3.1 Hardware Components

The following table identifies eHealth's hardware components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
Environment	eHealth Server UNIX Platform	Machine running Solaris 2.10 8 GB – Swap Space 4 GB – RAM 23 GB – Free Disk Space 250 Mhz - CPU

		Other: 100baseTX Network Interface Controller
Environment	Remote Workstation Platform	Windows 2000 or later

Table 2-2: eHealth Suite Version 6.1.2 Hardware Components

2.3.2 Software Components

The following table identifies eHealth's software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	eHealth Suite Version 6.1.2	Software package installed includes all TOE items listed below: Poller Processes eHealth Processes Apache Web Server v2.2.3 with mod_SSL OneClickEH Interface Web User Interface Discover Process
Environment	Solaris 2.10	eHealth Operating System
Environment	Oracle 10g Database	Oracle Database, update 10.2.0.3
Environment	Web Browser	Remote Web Browser with JavaScript enabled Windows systems: Internet Explorer version 7 or later Firefox 3.5 or later

Table 2-3: eHealth Suite Version 6.1.2 Software Components

2.3.3 Network

The eHealth Server receives information from various nodes on the network depending on how the eHealth Administrator configures the TOE to operate. In the evaluated configuration, communications traverse between network nodes and the eHealth Server via the IETF Standard SNMP protocol version 1. eHealth will work with any SNMP v1 manageable device that has defined MIB support which can be certified and supported with eHealth. The SNMP v1 management devices are listed at http://support.concord.com/devices /.

2.3.4 Solaris 2.10

eHealth relies on the OS to provide access to resources (e.g., CPU, memory, disk, and network). Prior to the installation of eHealth, the underlying OS (i.e., Solaris 2.10) is configured. All external interfaces to the TOE are disabled with the exception of the HTTP over SSL v3.0, Oracle API's, SNMP v1 and ICMP PING interfaces as shown in Figure 1 above. Physical access to the TOE is initially required for installation but once the TOE is in its operational state no further direct access to the TOE is required. Users of the TOE will interact through the HTTP over SSL v3.0 interface (web user interface) via a remote workstation. Administrators of the TOE will interact through the HTTP over SSL v3.0 interface (OneClickEH interface) via a remote workstation.

2.3.5 Oracle 10g (Environment)

eHealth includes an integrated database, which in Release 6.1.2 is the Oracle10g database. (This database is a product that was developed by the Oracle Corporation and not part of the TOE). The evaluated version of Oracle 10g is installed on the Solaris platform before the eHealth Suite is installed. Once installed properly, direct user access to Oracle 10g is not required. Users interact directly with the TOE and the TOE accesses the Oracle 10g database as required to perform its functions. The Oracle listener is required to be active on the eHealth server in order for the TOE to function. However, when the TOE is configured in accordance with the CC installation guidance provided with the validated product, the server is resistant to known attacks that utilize the listener as a vector.

The TOE interface to Oracle used to manipulate the database is done via an API that performs Oracle Procedure Library calls. eHealth uses the database to save all of its element information, polled data (the report data that it collects from critical resources on the network), and poller configuration settings. When the TOE saves the results of a discover process, eHealth creates an entry in the database for each element that the discover process found. After each poll, eHealth saves the data it collected for each discovered element in the database.

2.3.6 IPv6

Support for IP addresses in compliance with IPv4 standard has been extended in eHealth Suite Version 6.1.2 to addresses in compliance with the IPv6 standard. eHealth Suite Version 6.1.2 can discover, poll, store, display, and report on either or both IPv4 or IPv6 addresses. The network that eHealth 6.1.2 resides on must be capable of routing both IPv4 and IPv6 addressed packets.

For more information on IPv6 support and limitations, see page 28 of the CA eHealth Installation Guide r6.1.

2.3.7 Remote Workstations

Users of the eHealth Suite interact with the product through the use of HTTP over SSL v3.0 with a web browser which uses HTML and/or the OneClickEH component. The GUIs then connect directly to the Apache Web Server v2.2.3.

2.4 Logical Boundary

The logical boundary of the TOE includes the eHealth Suite Version 6.1.2 Server software. This component enforces the Identification and Authentication, Audit, Data Protection, Security Management, and Encrypted Communications. Security Functions as described in the following subsections.

2.4.1 Identification and Authentication

Remote access is the only allowed access for authentication to the operational TOE. The remote workstation uses an authorized web browser to interact with the TOE via the SSL v3.0 Web interface port 443 to the Apache Web Server v2.2.3. A username and password request is issued by the web server. The user provides a username and password to the web server which is passed to the eHealth server via an industry standard web browser (see Section 2.3.2 for the supported web browsers). The Apache web server will validate the user's claimed credentials against password information and usernames stored in a web server configuration file stored on the local file system. The TOE will return the success or failure of the authentication process. If properly authenticated, the web server provides the username that has been authenticated to the eHealth application. TOE passwords are stored locally on the operating system in their encrypted form (MD5 hash). When a user presents his password to the TOE it is hashed with MD5 and the two hashes are compared. If the hash matches, access to the TOE is allowed.

Access privileges granted to users are managed by eHealth. eHealth stores the user privilege information in a CSV file on the operating system where eHealth runs. When a user requests content from the eHealth application, eHealth validates the authorization to this content by comparing the validated username provided by the web server with the list of access rights on the Authorization database (CSV). For database access, the eHealth application verifies that the OS user has access to the Oracle database and grants it DBA rights. Additional accounts are granted read only access rights. All files that eHealth requires are owned by the account used to install the TOE and are read-only except by the owner.

The eHealth Administrator has the privileges associated with the eHealth account created and maintained by the underlying Operating System (i.e., Solaris 2.10). This account will have access to the various files used by the TOE and stored and protected by the underlying OS.

eHealth protects the server resources from unauthorized access. An End User's capability of accessing pages and files, and running applications or reports are controlled by the corresponding User Policy.

2.4.2 Audit

The TOE generates audit records for selected security events. Events are tracked based on occurrence and who triggered them. Results are recorded to a local log text file on the eHealth Server that is stored and protected by the host Operating System. The event results contained in the local log text file are recorded in a human-readable format. Logins can be audited via log files prepared by the web server, and displayed to the privileged user (administrative user) via the web interface. This login log file is also protected and stored on the host Operating System. As a result, the eHealth Administrator can utilize the contents of the log files for further processing. A web browser in the TOE environment is required to read the audit records. The eHealth Administrator interacts with the TOE from a remote workstation. Administrators are required to successfully identify and authenticate themselves to the TOE before being granted permission to review the generated audit information.

Reports are also considered to be an auditing function. When the TOE polls discovered SNMP elements, statistical information about these elements are stored in the database. Based on this information, reports can be generated which show these statistics over time. Statistics include a variety of metrics on system and network performance such as CPU utilization and bandwidth throughput.

2.4.3 Data Protection

The access control features of the underlying operating system protect all TOE data. Local access is not permitted by any user other than an authorized Operational Environment administrator that has an account on the local machine. End Users log on to the machine via a remote workstation, and are not permitted to edit any of the information stored on the eHealth Server except for their own password. The User Policy is a Discretionary Access Control policy by which the TOE allows or denies access to the functions in the Web user interface and the OneClickEH interface. Administrators must modify the permissions on the individual end user accounts accordingly. Individual users can be allowed or denied access to different screens on the web interface, different types of reports to be run, and different groups of elements to view.

2.4.4 Security Management

eHealth maintains two types of roles – end users and Administrators. Security Management is handled by an authorized eHealth Administrator via the OneClickEH interface. Access to the security management functions is secured by the web server authentication scheme and user based permissions. Administrators are permitted to edit user account attributes and access permissions while end users are denied these privileges. Beyond this distinction, individual End Users and Administrators may have differing levels of privilege based on what elements, element groups, and report types they are allowed to access.

2.4.5 Encrypted Communications

The TOE uses an Apache web server v2.2.3 to support protection of external TOE communication with the users by performing SSL v3.0 encryption through Apache’s OpenSSL-based cryptographic module (mod_SSL). The TOE uses openssl 0.9.8.d. The protocol for transport is HTTP over the Secure Socket Layer protocol, referred to as "HTTPS" or "HTTP over SSL." HTTP over SSL is used as the secure communication between the eHealth server and the remote workstation. The use of SSL ensures that all traffic to and from the TOE via the remote administration interface is protected from unauthorized disclosure. The eHealth server relies on the user’s web browser in the environment to process self-signed certificates for authenticating the end points of the communication channel and to encrypt the data. User passwords are not sent in the clear but use an MD5 hash for comparison to a shared secret on the TOE. All SSL v3.0 data is encrypted with 3DES-EDE-CBC and RSA is used for symmetric key exchange. All keys are destroyed using the overwrite method once they are no longer needed. The correctness of the cryptography is asserted by the vendor. The CC evaluation simply verified that cryptography has been implemented.

Note that the OneClickEH component runs as an additional graphical layer on top of Internet Explorer. Its sole responsibility is to translate between GUI elements and commands sent by IE to the eHealth server. As a result, it depends on the existing version of IE on the client machine to perform encryption over the OneClickEH interface.

3 Conformance Claims

3.1 CC Version

This ST is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2007-09-004, Version 3.1 Revision 2, September 2007.

3.2 CC Part 2 Extended

This ST and Target of Evaluation (TOE) is Part 2 extended for EAL2 to include all applicable NIAP and International interpretations through 27 April 2009.

3.3 CC Part 3 Augmented

This ST and Target of Evaluation (TOE) is Part 3 augmented for EAL2, to include all applicable NIAP and International interpretations through 27 April 2009.

3.4 PP Claims

This ST does not claim Protection Profile (PP) conformance.

3.5 Package Claims

This TOE has a package claim of EAL2.

3.6 Package Name Conformant or Package Name Augmented

This ST and Target of Evaluation (TOE) is conformant to EAL package claims augmented with ASE_TSS.2**.**

3.7 Conformance Claim Rationale

There is no Conformance Claim rationale for this ST.

4 Security Problem Definition

4.1 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated. The following are threats addressed by the TOE.

T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or performs operations for which no access rights have been granted, via user error, system error, or other actions.

T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded; thus masking a user's action.

T.MODIFY Users, whether they be malicious or non-malicious, could attempt to misconfigure or modify their user accounts in an attempt to tamper with TOE resources or modify security information relative to the TOE.

T.MASK Users whether they be malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.

T.DOS Users or network services, whether they be malicious or non-malicious, could attempt to disable or degrade the performance of networks, systems, or applications in the network.

T.EAVESDROPPING A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.

T.CRYPTO_COMPROMISE A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.

4.2 Organizational Security Policies

There are no Organizational Security Policies that apply to the TOE.

4.3 Secure Usage Assumptions

The specific conditions listed in this section are assumed to exist in the TOE environment. These assumptions are necessary as a result of practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

4.3.1 Personnel Assumptions

A.ADMIN One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.

A.CLIENT It is assumed that Administrators who download the OneClickEH component regularly ensure that their client machine has up-to-date patches, is scanned for viruses/malware, and periodically re-downloads the OneClickEH component from the web interface to ensure its integrity.

A.NOEVIL Users and administrators of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.

A.PATCHES Administrators exercise due diligence to patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.

A.PASSWORD It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data.

4.3.2 Connectivity Assumptions

A.LOCATE The network the TOE monitors is isolated from untrusted networks. The SNMP v1 monitored traffic is limited to a trusted network, (either physically isolated or protected by appropriate network boundary devices).

4.3.3 Physical Assumptions

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

5 Security Objectives

This chapter provides a listing of security objectives to ensure that all of the security threats listed in Chapter 3 have been countered. The security objectives are divided into Security Objectives for the TOE (Section 5.1) and Security Objectives for the Operational Environment (Section 5.2).

5.1 Security Objectives for the TOE

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

O.ACCESS The TOE will provide measures to authorize End Users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the eHealth Administrator of the TOE.

O.AUDIT The TOE will provide measures for recording security-relevant events that will assist the eHealth Administrators in detecting misuse of the TOE and/or its security features, or in detecting events that would compromise the integrity of the TOE and violate the security objectives of the TOE.

O.IDEN The TOE will provide measures to uniquely identify End Users and will authenticate the claimed identity prior to granting a user access to the TOE.

O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.

O.MANAGE The TOE will provide eHealth Administrators with the resources to manage and monitor user accounts, resources and security information relative to the TOE.

O.MONITOR The TOE will collect and analyze critical data for network devices, systems, and applications and report on the performance, capacity, availability, and response of these resources.

O.CRYPTOGRAPHIC_FUNCTIONS The TOE shall provide cryptographic functions for its own use, including encryption/decryption and secure hash. This will assist authorized users in preventing unauthorized monitoring of networks or information systems that would compromise the integrity of the TOE and violate the security objectives of the TOE.

5.2 Security Objectives for the Operational Environment

The following security objectives for the Operational environment of the TOE must be satisfied in order for the TOE to fulfill its security objectives.

OE.ADMIN One or more eHealth Administrators will be assigned to install, patch, configure and manage the TOE and the security of the information it contains.

OE.CLIENT Administrators who download the OneClickEH component will regularly ensure that their client machine has up-to-date patches, is scanned for viruses/malware, and periodically re-downloads the OneClickEH component from the web interface to ensure its integrity.

OE.LOCATE The TOE will be located on a trusted network whose boundary is protected from other networks.

OE.NOEVIL Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.

OE.PASSWORD Users of the TOE shall ensure that they choose strong passwords and that they protect their authentication data as instructed by the administrator guidance.

OE.PROTECT The parts of the TOE critical to security policy enforcement will be protected from unauthorized physical modification.

6 Extended Security Functional Requirements

6.1 Extended Security Functional Requirements for the TOE

The Table below contains the extended Security Functional Requirements for the TOE:

Security Functional Class	Security Functional Component
Security audit (FAU)	FAU_GEN_EXT.1(1) Discover log Generation
	FAU_GEN_EXT.1(2) Poller Audit Log Generation
	FAU_GEN_EXT.1(3) Message Log Generation
	FAU_GEN_EXT.1(4) Report Generation
	FAU_SAR_EXT.1 Audit Review

Table 6-1: Extended Security Functional Requirements for the TOE

6.1.1 Security audit (FAU)

The FAU_GEN_EXT family defines requirements for recording the occurrence of security relevant events that take place in the Operational Environment but are observed by the TSF. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types. The FAU_GEN.1 requirements are extended because these extended requirements govern the auditing of data which occurs on remote environmental systems and the environmental OS on which the TOE is installed. The generation of these types of records is specific to the TOE and does not refer to the generic audit record generation as described in CC Part 2.

FAU_GEN_EXT.1.1 The TSF shall be able to generate **[*assignment: type of log file*]** based on the following logical or physical elements: **[*assignment: list of logical or physical elements outside the TOE boundary for which the TOE is capable of logging data.*]**

FAU_GEN_EXT.1.2 The TSF shall record within each **[*assignment: type of log file*]** at least the following information: [***assignment: list of attributes pertaining to elements outside the TOE boundary for which the TOE is capable of logging data***].

Management: FAU_GEN_EXT.1

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

a) Invoke the discover process
b) Define the polling interval
c) Define report templates and elements to be reported

Audit: FAU_GEN_EXT.1

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

a) Not specified: Execution of data collection process

Dependencies: None

The FAU_SAR_EXT family defines the requirements for audit tools that should be available to authorized users to assist in the review of audit data that is collected for the behavior of the Operational Environment. The FAU_SAR.1 requirement is extended because it refers to the review of data generated in the Operational Environment and collected by the TOE as opposed to being generated by the TSF. The viewing of these types of records is specific to the TOE and does not refer to the generic audit record review as described in CC Part 2.

FAU_SAR_EXT.1.1 The TSF shall provide **[*assignment: list of authorized users*]** with the capability to read **[*selection: (all information), (assignment: subset of attributes listed in FAU_GEN_EXT.1.2)*]** collected from the [***assignment: list of log files maintained by the TOE***].

Application Note: *The selection is present to allow the PP/ST author to choose whether the reviewable data includes all audited data or if only some subset of the data is reviewable.*

Management: FAU_SAR_EXT.1

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

a) Define what report types are available to individual users
b) Define report types and format for myHealth reports

Audit: FAU_SAR_EXT.1

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

a) Not specified: Failed attempt to view log data

Dependencies: FAU_GEN_EXT.1

6.1.2 FAU_GEN_EXT.1 (1) Discover log Generation

Hierarchical to: No other components.

FAU_GEN_EXT.1.1 (1)The TSF shall be able to generate **[*a discover log*]** based on the following logical or physical elements:
[*Audit: Device [system name, unique device ID, IP address*]
Audit: Agent [MTF, SNMP port, enterprise ID]
***Audit: Element [LAN/WAN Elements, Router/Switch Elements, Application, Modem Pool and Remote Access Server, Response, QoS]*]**

FAU_GEN_EXT.1.2 (1)The TSF shall record within each **[*discover log*]** at least the following information:
[***Host, Discover Methods, IP Addresses, and IP Exclusion File***].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: *The discover logs probe a range of network IP addresses set by the administrator during installation through discover rules. The discovery process is run periodically after installation. Element field changes and new elements found are stored in this log file. After installation, the discovery process can be scheduled to run at regular times or run manually from the OneClickEH interface to update information in the database.*

6.1.3 FAU_GEN_EXT.1 (2) Poller Audit Log Generation

Hierarchical to: No other components.

FAU_GEN_EXT.1.1 (2)The TSF shall be able to generate **[*a poller audit log*]** based on the following logical or physical elements: [***collected MIB information from devices on the network***]

FAU_GEN_EXT.1.2(2)The TSF shall record within each **[*entry of the poller audit log*]** at least the following information: [***the exact time the change is made, the user id for the user who makes the change, the type of change made and the name of the device and whether the change operation is successful or not***].

Dependencies: FPT_STM.1 Reliable time stamps

Application note: *Devices are a set of supported products as specified in [Certified Device List, updated quarterly]*

Application Note: *During installation, the Poller component of the TOE populates the Oracle database with information on devices that eHealth monitors in database objects called "elements." Poller audit logs track changes made to these elements. The Poller interface to Oracle is done via an API that performs Oracle Procedure Library calls. These API calls perform inserts and updates to the database.*

6.1.4 FAU_GEN_EXT.1 (3) Message Log generation

Hierarchical to: No other components.

FAU_GEN_EXT.1.1 (3)The TSF shall be able to generate [***a message log*****]** based on the following logical or physical elements: [***all internal running process and program events eHealth monitors***]

FAU_GEN_EXT.1.2 (3)The TSF shall record within each **[*entry of the message log*]** at least the following information: [***the exact date and time the event occurred, the process and job id who invoked the event, the type of event and the status of the event (i.e., whether the event operation is successful or not)].***

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: *Message logs capture messages from all other internal running processes and programs in the TOE. For example, the messages contain information on jobs that are started and finished by the TOE, as well as error messages.*

6.1.5 FAU_GEN_EXT.1 (4) eHealth Reports generation

Hierarchical to: No other components.

FAU_GEN_EXT.1.1 (4)The TOE shall be able to generate [***eHealth reports***] based on the following logical and physical elements: [***statistical data stored in the Oracle 10g database generated by Poller Process.***]

FAU_GEN_EXT.1.3 (4)The TOE shall display within each **[*eHealth report record*]** the following information:
[***Date and time of the event, type of event, the element, title of the report, group the element belongs to, and the type of report that was run***]

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: *These reports pull from data generated as a result of the poller process. Specific report types are discussed in* Section 9.1.1.7. *The standard report types are trend, top N, and at-a-glance.*

Application Note: *This report list refers to the ability of the TOE to preserve a list of reports run by all users of the TOE.*

6.1.6 FAU_SAR_EXT.1 Audit review

Hierarchical to: No other components.

FAU_SAR_EXT.1.1 The TSF shall provide [***administrators and end users***] with the capability to read *[**all information***] collected from the [***discover logs, poller audit logs, message logs, and eHealth reports***].

Dependencies: FAU_GEN_EXT.1 (1) Discover log generation
FAU_GEN_EXT.1 (2) Poller audit generation
FAU_GEN_EXT.1 (3) Message log generation
FAU_GEN_EXT.1 (4) eHealth Reports generation

Application Note: *Administrators and end users can read the eHealth reports. However, only Administrators can read the discover logs, poller audit logs and message logs. Individual End Users and Administrators can be further restricted to some subset of these types of logs and reports as defined by the User Policy.*

6.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

7 Security Functional Requirements

7.1 Security Functional Requirements for the TOE

The following table provides a summary of the Security Functional Requirements implemented by the TOE.

Security Functional Class	Security Functional Component
Security audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic Key Management
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1 Cryptographic Operations
User data protection (FDP)	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
Identification and authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security Management (FMT)	FMT_MOF.1 (1) Management of security functions behavior
	FMT_MOF.1 (2) Management of security functions behavior
	FMT_MSA.3 Static Attribute Initialization
	FMT_MTD.1 (1) Management of TSF data
	FMT_MTD.1 (2) Management of TSF data
	FMT_MTD.1 (3) Management of TSF data
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Trusted Path/Channel (FTP)	FTP_TRP.1 Trusted Path

Table 7-1: Security Functional Requirements

The following subsections present the details for each of the TOE Security Functional Requirement components.

7.1.1 Security audit (FAU)

7.1.2 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [**not specified**] level of audit; and

c) [***web events: generation of reports, viewing of reports, login, and self password changes***

d) ***OneClick events: login, user creation, user modification, discovery execution, element modification, element deletion, and group and grouplist creation, modification, and deletion***].

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, [***web events: IP address of the Remote Workstation from which a page was accessed, End User account name, date and time at which the page was accessed, name of the operation that was performed, pathname of the page visited, return code, and the total amount of data (in bytes) that was transferred***].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: The audit records referred to in these SFRs are captured in the Web Server Log httpd-log and httpd-error.

7.1.3 FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

7.1.4 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [***Administrators***] with the capability to read [***the IP address of the Remote Workstation from which a page was accessed, End User account name, date***

and time at which the page was accessed, name of the operation that was performed, pathname of the page visited, return code, and the total amount of data (in bytes) that was transferred] from the audit records.

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

Dependencies: FAU_GEN.1 Audit Data Generation

7.1.5 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

Application Note: *The TOE can restrict the ability of users to see elements in various reports based on group membership of the element.*

7.1.6 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to apply [**sorting**] of audit data based on [**user identity, page type, individual statistics, time range, Remote Workstation node**].

Dependencies: FAU_SAR.1 Audit review

7.1.7 Cryptographic Support (FCS)

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.1.8 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA***] and specified cryptographic key sizes [***1024 bits***] that meet the following: [***ANSI X9.31 and ANSI X9.80***].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Application note: This SFR supports key generation for SSL.

7.1.9 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***overwrite method***] that meets the following: [***no standard***].

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]

Application note: This SFR supports key destruction for SSL.

7.1.10 FCS_COP.1 (1) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1(1) The TSF shall perform [***encryption and decryption***] in accordance with a specified cryptographic algorithm [***3DES-EDE-CBC for encryption and decryption***] and cryptographic key sizes [***168 bits for encryption and decryption***] that meet the following: [***FIPS 46-3 for encryption and decryption***].

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

Application Note: *This SFR supports the mod_ssl module used in the Apache Web Server component of the TOE.*

7.1.11 FCS_COP.1 (2) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 (2) The TSF shall perform [***password hashing***] in accordance with a specified cryptographic algorithm [***MD5***] and cryptographic key sizes [***64 bit***] that meet the following: [RFC 1321].

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

Application Note: *This SFR supports the mod_auth_digest module used in the Apache Web Server component of the TOE.*

7.1.12 User data protection (FDP)

7.1.13 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce [***the User Policy***] on [***users*]**

Dependencies: FDP_ACF.1 Security attribute based access control

Application Note: End users can be added to groups and are only able to see the information for the groups they have been assigned to.

7.1.14 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [***User Policy***] to objects based on the following: [***username, elements, groups, grouplists, report type, page views***]

Application Note: Elements can be assigned to groups. Grouplists are groups of groups. Users can be allowed access to all elements or only specific groups and/or grouplists. Users can also be restricted to only viewing certain types of reports and only certain pages in the user interfaces.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***users are assigned access to groups, report types, and page views***].

See Application Note for FDP_ACF.1.1 for more information.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***the Apache server allows an Administrator to use the OneClick interface***].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [***no rules***].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

7.1.15 Identification and authentication (FIA)

7.1.16 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***username, password, groups, grouplists***].

Dependencies: No dependencies.

See Application Note for FDP_ACF.1.1 for more information.

7.1.17 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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

Dependencies: FIA_UID.1 Timing of identification

7.1.18 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies

7.1.19 Security Management (FMT)

7.1.20 FMT_MOF.1 (1) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 (1) The TSF shall restrict the ability to [**determine the behavior of, disable, enable, modify the behavior of**] the functions [***modify system settings, modify user settings***] to [***the Administrators granted access to those pages within OneClick by the Apache server***].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application Note: *The user and system settings are explicitly defined in FMT_SMF.1.*

7.1.21 FMT_MOF.1 (2) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 (2) The TSF shall restrict the ability to [**enable**] the functions [***generate views of the Elements stored in Oracle 10g***] to [***Administrators and authorized end users***].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application Note: *A user can only view (i.e., read, or create reports based on the view) the Elements stored in the Oracle 10g database for which his group matches a group associated with the Element. Administrators can view and create reports on any Elements in the database. See the application note for FDP_ACF.1.1 for more information.*

7.1.22 FMT_MSA.3 Static Attribute Initialization

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [***User Policy***] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [***Administrators***] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

7.1.23 FMT_MTD.1 (1) Management of TSF data

Hierarchical to:	No other components.
FMT_MTD.1.1 (1)	The TSF shall restrict the ability to [**query**] the [***eHealth reports***] to [***Administrators and authorized end users***].
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
Application Note:	*This SFR is used to restrict the ability to query eHealth reports generated by TOE users. See* Section 9.1.1.*7 for more information on eHealth Reports.*

7.1.24 FMT_MTD.1 (2) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 (2) The TSF shall restrict the ability to [**modify**] the [***user password***] to [***the specific End User, eHealth Administrator***].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

7.1.25 FMT_MTD.1 (3) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 (3) The TSF shall restrict the ability to [**modify**] the [***User Policy***] to [***Administrators***].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application Note: The user policy is used by the administrators to set users permissions, change passwords, and restrict access to various eHealth reports.

7.1.26 FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

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

- ***set or change the password of a user and force a user to change his or her own password;***
- ***Define Custom Reports***
- ***Invoke the Discover Program***
- ***Schedule Tasks***
- ***View the message logs***
- ***Add, delete, view, and Modify users and user Attributes (including passwords)***
- ***View User Attributes (administrators only)***
- ***Create, Modify or Delete Grouplists***
- ***Create New or Modify Groups***
- ***Run eHealth Reports (At-A-Glance, Top N, and Trend)***
- ***Query eHealth Reports (At-A-Glance, Top N, and Trend)***
- ***View the Web Access Logs***
- ***View list of eHealth reports generated by any authorized user of the TOE***]

Dependencies: No dependencies.

Application Note: These functions are accomplished via the Web interface and through access by the administrators to One-Click.

7.1.27 FMT_SMR.1.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [***End User and Administrator***].

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

Dependencies: FIA_UID.1 Timing of identification

7.1.28 Trusted Path/Channel (FTP)

7.1.29 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**disclosure**].

Application Note: This SFR is included to capture SSL encryption functionality.

FTP_TRP.1.2 The TSF shall permit [**remote users**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**initial user authentication**].

Dependencies: No dependencies

7.2 Operations Defined

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. All of the components in this ST are taken directly from Part 2 of the CC except the ones noted with "_EXT" in the component name. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, selection, and refinement to be performed on functional requirements. These operations are defined in Common Criteria, Part 1 as:

7.2.1 Assignments Made

An assignment allows the specification of parameters and is specified by the ST author in [***italicized bold text***].

7.2.2 Iterations Made

An iteration allows a component to be used more than once with varying operations and is identified with the iteration number within parentheses after the short family name (e.g. FAU_GEN.1 (1), FAU_GEN.1 (2)).

7.2.3 Selections Made

A selection allows the specification of one or more items from a list and is specified by the ST author in [**bold text**].

7.2.4 Refinements Made

A refinement allows the addition of details and is identified with "Refinement:" right after the short name. ~~The old text is shown with a strikethrough~~ and <u>***the new text is specified by italicized bold and underlined text***</u>.

8 Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL2 augmented with ASE_TSS.2.

8.1 Security Architecture

8.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D: The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D: The developer shall design and implement the TSF so that it is able to protect itself from tampering by un-trusted active entities.

ADV_ARC.1.3D: The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C: The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C: The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C: The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C: The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C: The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

8.1.2 Functional Specification with Complete Summary (ADV_FSP.2)

ADV_FSP.2.1D: The developer shall provide a functional specification.

ADV_FSP.2.2D: The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C: The functional specification shall completely represent the TSF.

ADV_FSP.2.2C: The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C: The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C: For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C: For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C: The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

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

ADV_FSP.2.2E: The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

8.1.3 Architectural Design (ADV_TDS.1)

ADV_TDS.1.1D: The developer shall provide the design of the TOE.

ADV_TDS.1.2D: The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C: The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C: The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C: The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C: The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C: The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C: The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.1.2E: The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

8.2 Guidance Documents

8.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

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

8.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

8.3 Lifecycle Support

8.3.1 Authorization Controls (ALC_CMC.2)

ALC_CMC.2.1D: The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D: The developer shall provide the CM documentation.

ALC_CMC.2.3D: The developer shall use a CM system. ALC_CMC.2.1C: The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C: The CM system shall uniquely identify all configuration items.

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

8.3.2 CM Scope (ALC_CMS.2)

ALC_CMS.2.1D: The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C: The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

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

8.3.3 Delivery Procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

8.4 Security Target Evaluation

8.4.1 Conformance Claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

8.4.2 Extended Components Definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

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

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

8.4.3 ST Introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.
ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

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

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

8.4.4 Security Objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

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

8.4.5 Security Requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.10C The statement of security requirements shall be internally consistent.

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

8.4.6 Security Problem Definition (ASE_SPD.1)

ASE_SPD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

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

8.4.7 TOE Summary Specification (ASE_TSS.2)

ASE_TSS.2.1D The developer shall provide a TOE summary specification.

ASE_TSS.2.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.2.2C The TOE summary specification shall describe how the TOE protects itself against interference and logical tampering.

ASE_TSS.2.3C The TOE summary specification shall describe how the TOE protects itself against bypass.

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

ASE_TSS.2.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

8.5 Tests

8.5.1 Analysis of Coverage (ATE_COV.1)

ATE_COV.1.1D: The developer shall provide evidence of the test coverage.

ATE_COV.1.1C: The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

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

8.5.2 Functional Tests (ATE_FUN.1)

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

ATE_FUN.1.2D The developer shall provide test documentation

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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

8.5.3 Independent Testing (ATE_IND.2)

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

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

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

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

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

8.6 Vulnerability Assessment

8.6.1 Vulnerability Analysis (AVA_VAN.2)

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

AVA_VAN.2.1C The TOE shall be suitable for testing.

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

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, and TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

9 TOE Summary Specification

9.1 TOE Security Functions

This section describes the security functions provided by the TOE. The OneClickEH component is part of the TOE but it does not provide any security functions; instead, it translates administrator input into requests that are sent to the web server and validated by the server. When the requests are processed by the server, they are returned to the OneClickEH component as XML. This XML is then parsed by the OneClickEH component in a matter suitable for display to the administrator.

9.1.1 Audit

9.1.1.1 eHealth Processes

eHealth Processes provides an interface to the information stored within the Oracle 10g Database. These processes are used to facilitate interactions with the eHealth Server received from remote workstations through the Apache Web Server component. Administrators can monitor the eHealth system processes by accessing the Tasks and Information, System Information, Server Processes tree of the OneClickEH component. Any issues with the system processes will be recorded in the system message log.

9.1.1.2 eHealth Poller Processes

Polling is the process of collecting statistics about network, system, and applications data directly from elements. The eHealth poller automatically collects data for any element defined by the poller configuration in the eHealth database. The poller configuration defines the information for each element such as the name, a polling rate (the frequency with which eHealth polls the element), and the agent type (the type of element that eHealth discovered). The polling rates are discussed below:

- Conversation Poll Rate - The conversation poll rate is the speed at which eHealth collects data on the probes and other devices that are being used in a network to collect traffic data. The default poll rate for conversation data is 30 minutes, but Administrators can set it to 15, 45, or 60 minutes.

- Statistics Poll Rate - The speed at which eHealth polls statistics elements.

- Normal Polling Rate - By default, eHealth assigns the Normal polling rate to newly discovered statistics elements. It polls elements every 5 minutes and saves the data to the poller configuration in the database during the poll.

- Slow Polling Rate - eHealth polls elements every 30 minutes and saves the data in the poller configuration in the database during the poll. Administrators can change the default interval to 10, 15 or 60 minutes.

- Fast Polling Rate - eHealth aggregates the data from five 1-minute polls into one 5-minute average sample before saving it to the poller configuration in the database. This process maintains consistent data samples. Administrators can change the default interval to 30 seconds, 2.5 minutes, or 5 minutes.

- Fast Store Polling Rate - eHealth collects data at the Fast rate and stores the 30 seconds or 1-minute samples in the poller configuration in the database without aggregating them.

The Polling schedule and rates are managed through the Setup tree of the OneClickEH component.

9.1.1.3 Elements

An element is a resource that eHealth polls and for which it collects data. eHealth polls two types of elements, as follows:

Conversation elements - monitor traffic flow among nodes and applications using the network. Conversation elements include devices that use Remote Network Monitoring (RMON) or similar agents to monitor traffic, and Cisco NetFlow collectors. RMON v2 is a type of device that collects network management information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that have occurred. A probe is an example of an RMON device. For more information, refer to RFC 2021.

Statistics elements--devices and interfaces within the network. Statistics elements include the following:

- Local area network (LAN) and wide area network (WAN) interfaces
- Quality of Service (QoS)
- Routers, their central processing units (CPUs), and interfaces
- Mobile wireless and wireless interfaces
- Systems, their disks, interfaces, partitions, CPUs, and process sets
- Remote access server (RAS) devices, modem pools, modems, and Integrated Services Digital Network (ISDN) interfaces
- Application services and their process sets
- Response sources, destinations, and paths
- Synchronous Optical Network (SONET) interfaces
- Storage area networks (SANs)
- Digital subscriber line (DSL) interfaces and cable modems
- Voice over IP (VoIP) features such as call managers, voice line quality, and services

9.1.1.4 Element Properties

The poller configuration in the database defines properties for each element including the name, agent type, alias, community string, discovered values, interface speed, parent name, and SNMP v1 index as described below. Administrators can modify most of these element properties by using the OneClick for eHealth interface.

- Agent Type - The agent type specifies the type of element such as Router or System.
- Alias - An alias can be defined for a specific element by an administrator if the full element name is not intuitive.
- Community String - The community string is used by Administrators to grant read and write access to various device MIBs. eHealth typically uses a read-only community string to poll devices.
- Discovered Information - The Discovered Information values are the values that eHealth obtains from the element agent during a discover.
- Element Name - The element name is the name that eHealth automatically assigns to a resource after it discovers it within an infrastructure.
- Interface Speed - During the first poll, eHealth obtains the speed of LAN elements, and both the incoming and outgoing speeds of full-duplex interface elements as configured at the device.
- Parent - A parent is the top-level element in a hierarchy of elements (such as a router, system, modem pool, or remote access server). For example, a router will have several elements because each LAN/WAN interface is an individual element.
- SNMP v1 Index - The SNMP v1 index is a unique identifier for similar elements of a device (for example, all interfaces of a router).

9.1.1.5 Finding and Selecting Elements

The OneClickEH interface can be used to view all elements that are being monitored and their associated configuration. An Administrator or authorized user can view element configuration by accessing the Managed Resources, Elements tree in the left pane of the OneClickEH component. By default, the OneClickEH component immediately shows all of the elements there. If matching criteria is specified in the Filter table by field at the top of the screen, it filters the list as a user types. An administrator or authorized user has the ability to customize the element display. Additionally, searches can be performed on elements based on a specific name, alias or IP address:

- If Alias is selected from the list, a portion of the element’s alias name can be specified using wildcards (for example, *testSystems*).

- If Name is selected from the list, a portion of the element's name can be specified using wildcards (for example, *boston*).

One or more IP address octets can be searched using wildcards.

9.1.1.6 Discover

Discovery is the process of locating resources and creating elements for them. To find the resources, eHealth uses Simple Network Management Protocol (SNMP v1) to search for agents at the IP addresses that are specified by Administrators during installation. eHealth first tests each address via a simple PING and SNMP v1 request to ascertain the probable existence of an agent at that address. It then obtains information from the management information base (MIB) on each agent and creates elements based on that information. When the Administrator saves the discover process results, eHealth stores element information in its poller configuration with its database. Once the initial address range is set by the Administrators the discovery process is complete. After installation, the discovery process can be scheduled to run at regular times to update information in the poller configuration in the database. The poller configuration in the database information includes a name, IP address, SNMP v1 index numbers, and other information needed to uniquely identify the element, poll it, and report on it.

Administrators can create discover policies to specify the types of devices and specific configuration parameters associated with the element type that they want to monitor. Administrators can create new discover policies on-the-fly by accessing the Tasks and Information, Resource Discovery, Interactive Discover tree of the OneClickEH interface.

9.1.1.7 Discover Rules

The Database Configuration Information (DCI) rules file can include or exclude elements based on certain element attributes, create groups, create associations, or modify element attributes. The results of a Discover operation can be filtered and transformed using DCI rules and the elements can be saved to named groups. Many options of the discover process are controlled by the Discover Policy parameter settings, which can be defined and edited using the eHealth for OneClick interface.

Each element can only be associated with a single policy. If no policy is specified for a discover run, the command uses the existing environment settings to remain backwards compatible with previously scheduled discover jobs or old scripts.

9.1.1.8 Agents

eHealth uses SNMPv1 agents to collect data about an infrastructure to provide the information that is needed for troubleshooting, analysis, and planning. Section 2.2 provides a description of the agents that are not included in the evaluated configuration. To monitor the network, eHealth relies on SNMPv1 agents embedded in the network devices that are being monitored. eHealth discovers these devices through SNMPv1, polls the statistics collected by each device’s MIB at user-defined intervals, and collects the information into a database.

9.1.1.9 Audit Records

The TOE generates audit records (i.e., access logs) to track all end users’ interaction with the TOE through the Web Server component of the TOE, including password changes, generation of reports, and viewing reports. In the case where a user causes the event (such as a password change), the TOE is able to associate the event (password change) with the user that caused the event. These logs include the start-up and shutdown of the audit functions. The audit records must include the date and time of the event, subject identity, and the outcome of the event. For each event type, the following information must be captured in the audit records: IP address of the remote workstation that accessed a page, end user account name, date and time when the page was accessed, name of the operation performed, pathname of the page visited, return code, and the total amount of data (in bytes) that was transferred. Administrators have the ability to read this information from the audit records. All end users are prohibited from accessing the audit records. Only the Administrators are able to read this information from the audit records. Additionally, Administrators can sort the data in the audit records based on user identity, page type, individual statistics, time range and remote workstation node.

During installation, a discovery process is run to baseline the network resources. Once the discovery process has populated the database, the TOE uses the poller process to collect historical data on the various elements in the database.

The TOE relies upon the underlying OS to store the audit data generated by the TOE and to provide reliable timestamps for use by the TOE. The TOE creates the following logs to monitor the actions described above:

- Poller Audit Logs – This log is generated based on the collected MIB information from devices on the network. Log new element additions, element deletions, and changes to any field of any element. The pollerAudit.date.time log captures the following information: the time of change, username for the user who made the change, type of change made, the name of the device, and the outcome of the change operation.

- Discover Log – This log describes the results of an element merge operation detailing what elements matched, the quality of the match, and field changes and any new elements found. For all devices, the following information is captured: system name, unique device ID and IP address. For all agents, the following information is captured: MTF, SNMP v1 port and enterprise ID. For all Elements, the following information is captured: LAN/WAN elements, router/switch elements, Application, modem pool and remote access server, response, QoS. For server object discover logs, the following information is captured: host, discover methods, IP address and IP exclusion file.

- Message Log – This log is generated based on all internal running process and program events monitored by eHealth. The information captured in this log includes the following: date and time the event occurred, the process and job ID who invoked the event, type of event and the outcome of event. Statistics Polling static window messages are stored on the underlying OS in a file called messages.stats.log. On the TOE these files can reach a maximum size of 100 MB. Once the log file reaches the maximum size, eHealth moves the data to a backup log file named messagesbackup.bak and overwrites the existing backup log file, if one exists. eHealth then starts a new log file using the default file name.

9.1.1.10 Discover Log

When a discover process is run, eHealth compares attributes of the discovered elements to attributes of previously discovered elements that are stored in the database. To resolve changes, discover uses a complex matching process based on discover keys. For each discover that is run, eHealth records the results in comparison to the existing poller configuration in the database in a file named discoverInteractive.date.time.log. To access the log files, Administrators and authorized users drill down to the Log Files tab of Interactive Discover under Tasks and Information in the OneClickEH component.

Each discover log file displays a header composed of three sections: Discover Results, Network Change Summary, and Duplicate Analysis. The log includes the infrastructure changes that the discover process could resolve using existing information in the database. Discover is able to resolve an infrastructure change when it can update the poller configuration in the database with the information without duplicating an element or incorrectly changing existing information. The sections are detailed below:

- Discover Results Section - The Discover Results section of the discover log lists the time at which the discover occurred, indicates whether it was scheduled or interactive, and itemizes the options that were specified for the discovery.

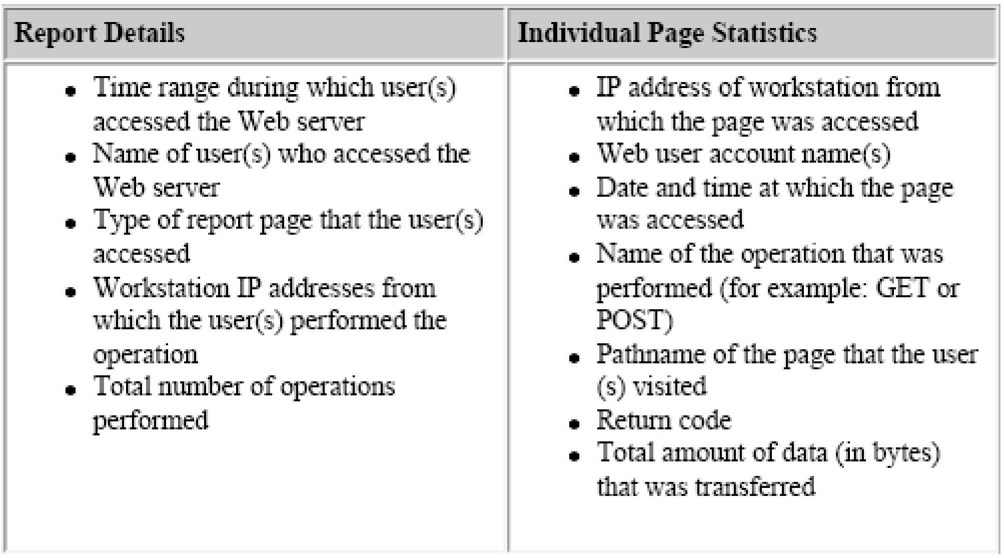
- Network Change Summary Section - The Network Change Summary section of the discover log identifies several types of elements: new, updated, unchanged, and missing. It also lists discover key changes—the unique identifiers that eHealth uses to recognize elements.

- Duplicate Analysis Section - The Duplicate Analysis section of the discover log lists the number of suspected duplicate elements, duplicate (identical) names, and duplicate keys identified in the database.

When eHealth completes the discover process, it displays the number of new elements that it discovered and the number of existing elements that it updated. It also lists updates to metadata, such as elements that have changed groups. eHealth saves these messages in the discoverResults.log file.

9.1.1.11 Web Server Access Logs

From the eHealth web user interface, Administrators can access the Access Logs under eHealth Management on the Administration page. Administrators can generate a detailed list of all connections that all or specific End Users have made to the eHealth Suite, all or specific Web pages that End Users have accessed, and a specific time and date range during which the access occurred. In addition, the eHealth Administrator can also display summary statistics of individual connections to the eHealth Suite (that is, for each report page). The following figure describes the report details and page statistics that can be obtain by generating an access log.



Report Details	Individual Page Statistics
• Time range during which user(s) accessed the Web server • Name of user(s) who accessed the Web server • Type of report page that the user(s) accessed • Workstation IP addresses from which the user(s) performed the operation • Total number of operations performed	• IP address of workstation from which the page was accessed • Web user account name(s) • Date and time at which the page was accessed • Name of the operation that was performed (for example: GET or POST) • Pathname of the page that the user (s) visited • Return code • Total amount of data (in bytes) that was transferred

Figure 2 – Access Log Attributes

These files can be viewed under the Access Logs section at the OneClickEH interface. They are synonymous with standard Apache web logs. The log files specifically are:

- Web Server Log httpd-log – Standard Apache web log of all HTTP requests, including user login, password changes, report generation, and viewing of reports.

- Web Server Log httpd-error – Standard Apache web log errors resulting from HTTP requests.

9.1.2 eHealth Reports

eHealth identifies and collects data from existing devices, agents, and management systems in the network intranet. To evaluate the health of these network resources, eHealth uses the historical data that it collects to analyze trends and calculate averages. It collects data over a period of time for various elements polled by the TOE. This data grade the performance of each element based on the utilization and numbers of errors that eHealth detects. eHealth uses upper limits for utilization and errors, referred to as Trend thresholds, to identify problem areas. Administrators and end users can generate reports on the collected data to manage network resources. eHealth reports provide an easy-to-read picture of the historical and current performance of the elements that were polled. The various reports assist users in optimizing network performance, recognizing trends, and identifying potential problems before they affect critical services. This section describes the basic reports that are available to the TOE users.

eHealth Suite Version 6.1.2 has the ability to create reports for system elements and application service elements. These reports are generated on the statistical data stored in the database generated by the poller processes. Each report contains the following information: date and time of event, type of event, element, title of report, group the element belongs to and the type of report that was run. eHealth reporting helps Administrators to assess performance, locate faults and diagnose problems on hardware devices. The agents report performance statistics related to CPU, storage (disk and partition), memory (physical and virtual), communications, processes, and systems. These statistics are used in eHealth reports.

These reports can help Administrators track the performance of groups of elements and look for situations that might require attention. They can also help summarize performance by enterprise, region, department, or business unit.

Once an Administrator identifies the system elements that he wants to manage, he can use eHealth to generate the following types of reports for systems:

- At-a-Glance
- Trend
- Top N

By default, eHealth allows Administrators and end users to run At-a-Glance, Top N, and Trend reports from the Organization page of the web user interface. These users can also generate a report list from this interface.

9.1.2.1 At-a-Glance Reports

At-a-Glance reports provide a series of charts that show the performance of critical variables for a specified element during the report period. A report period is the time range included in a report. When end users run a report, they can specify the time range. The time options vary with each report type, but the report period can consist of hours, days, weeks, or months.

At-a-Glance reports provide detailed information for all the critical performance parameters available, depending on the element reported on. At-a-Glance reports present the variables on identical time axes that allow TOE users to examine the interaction of critical performance indicators over the report period. Users can compare these charts to determine whether activity in one chart coincides with activity in other charts. For example, At-a-Glance reports can compare bandwidth utilization, bytes in & bytes out, frames in & frames out, errors in & errors out, availability, latency, etc.

9.1.2.2 At-a-Glance Reports for Applications

Administrators can use an At-a-Glance report to show the performance of an application service element during the report period. The Application Service At-a-Glance report charts show trends for important application performance variables.

If the systems were discovered using the System technology, Administrators can monitor the health and performance of the system and its resources using System At-a-Glance reports in addition to the Application Service At-a-Glance reports.
When an At-a-Glance report is run for a specific application service that was monitored, the report includes both footprint (if available) and application statistics for that application. Because the At-A-Glance reports for application service elements already contain information about the footprint variables, Administrators will not be able to run these reports for the application process set elements. To obtain data for the application process set elements alone, a Trend report must be run.

9.1.2.3 At-a-Glance Reports for Systems

An At-a-Glance report for system elements provides summary capacity statistics for the specified system, including CPU, interface, and partition utilization; disk faults and I/O; and system availability. With these reports, Administrators can isolate busy CPUs or full disks and compare groups of system.

9.1.2.4 Top N Reports

Top N reports are tabular reports that list all elements in a group, or all elements in a group that exceed or fall below the values that end users specify. For example, users can run a Top N report to show the following:

- 50 LAN/WAN elements that have a bandwidth utilization above a certain percentage
- All system partitions that have less than a certain utilization
- Some number of routers that have an average line utilization above 90%, incoming discards greater than 100 frames per second, and outgoing discards greater than 150 frames per second
- All elements in a certain group

When end users run a Top N report, they can specify the following criteria:

- Number of elements and element types to display
- Element group within which to search
- Up to six variables on which to report
- Service goal for each variable
- Filter criteria for each variable

- Ascending or descending display order
- Report period

9.1.2.5 Top N Reports for Applications

Administrators can generate a Top N report to list all application service elements in a group, or to list the elements in a group that exceed or fall below the report criteria goals that are specified.

9.1.2.6 Trend Reports

A Trend report shows the behavior of one or more performance variables for an element or a group of elements, over a specified period of time. Because of its flexibility, a Trend report can be used to reveal traffic patterns over time, as well as relationships between elements and between variables. If it indicates that two variables are correlated, then it suggests a causal relationship between them. For instance, if the bandwidth utilization and the collision rate on an Ethernet segment show a strong correlation, the high bandwidth utilization is likely causing the high rate of collisions.

9.1.2.7 Trend Reports for Systems

Administrators can use Trend reports to see the value of one or more variables for their systems over a specified report period. This helps Administrators to track the values of the variables to see when values might have changed radically or when a particular event, such as a reboot or missed poll, occurred.

The Trend variables differ for each element type. Reports can be run for the following types of systems and system components:

- CPU
- Disk
- Local Area Network (LAN)
- Process and Process Set
- User or System Partition
- Wide Area Network (WAN)

Each of these types includes specific variables on which Administrators can run reports. For example, server disk elements have variables for disk reads and writes, storage capacity, and storage utilization. Administrators can select up to ten variables at a time on which to run a Trend report.

9.1.2.8 MyHealth Reports

Administrators and authorized end users can user MyHealth reports to tailor a set of reports to meet a specific set of needs. These users can create and run multiple MyHealth reports. Each report can contain several charts that summarize critical application, system, and network information. The eHealth administrator and authorized users design MyHealth reports by specifying the report panels, titles, baseline periods, and a service profile. This information can be customized and displayed on a summary page. The eHealth Web administrator specifies whether each user can view, create, edit, or run MyHealth reports on demand.

9.1.2.9 MyHealth Reports for Systems

The MyHealth report page of the Web user interface contains a series of charts that are tailored to a user's particular interest. MyHealth provides eHealth web users with one or more customized reports on the elements and groups that they consider critical. A MyHealth report page contains one or more panels, and each panel contains a separate chart.

9.1.2.10 MyHealth Reports for Applications

Administrators and authorized end users can include charts for application service monitoring in the MyHealth reports. MyHealth provides eHealth Web users with one or more customized reports on the elements and groups that they consider critical. MyHealth reports are run from the MyHealth tab in the eHealth Web user interface.

9.1.3 Identification and Authentication

Once the Administrator has logged onto the eHealth Suite and configured end user accounts, the TOE is then setup to authenticate users from a remote workstation. An end user accesses the eHealth Server through a browser on their remote workstation. The connection is established using HTTP over SSL v3.0. Secure access to the eHealth Web server is enabled by default. Secure access requires all TOE users to identify and authenticate themselves to the Apache Web Server v2.2.3 by supplying an eHealth Web user name and password. All users must be identified and authenticated to the TOE prior to being able to perform any functions on the TOE through the browser based GUI. A policy to ensure a hard-to-guess password is specified in the administrator guidance. The TOE compares the entered user name and password with the attributes of the user account for its authentication and identification of users. These attributes (username, password, groups and grouplists) of all users are stored in the database and used by the TOE in order to confirm a user’s access to the TOE.

Users can see only those functions or pages of the web interface that they are permitted to use. The Administrator controls access to the web interface with web user accounts and access settings, specifying which functions each user can access. Administrators cannot modify the access permissions for individual users. To apply different access permissions to individual users, Administrators must modify the permissions on the individual accounts accordingly.

Access privileges granted to users are managed by the eHealth application. This protects the system resources from unauthorized access. The eHealth application stores the privilege information on a CSV file on the system where eHealth runs. When the user requests content from the eHealth application, the eHealth application will validate the authorization to this content by comparing the validated username provided by the web server with the list of access rights on the Authorization database (CSV). Users do not access the database directly, but instead can view elements within the database via reports if the user is authorized to read those elements. Users are assigned to groups to control their access to view elements. For database access, the eHealth application verifies that the OS user has access to the Oracle database and grants it DBA rights. The TOE requires administrators and end users to establish robust passwords for the use of the TOE.

If an administrator does not have the OneClickEH component on their client machine, they must first authenticate to the web interface and follow the link to download the OneClickEH component. Once the OneClickEH component has been saved to the remote workstation, the web browser is not needed for access to the OneClickEH component. Once the OneClickEH component has been downloaded, administrators must use it to authenticate to the OneClick interface if they wish to perform the functions allowed by that interface.

In the case of the Web Server Interface the user initiates authentication to the web server component of the TOE using digest authentication from Apache, specifically the Apache module mod_auth_digest controls the encryption of the passwords, and protects the TOE from replay attacks. During the I&A process the user performs the SSL v3.0 protocol handshake, is prompted with a login pop up window, and is allowed to enter I&A credentials. Authentication requires both. Note that through this interface a valid authentication attempt via SSL v3.0 and a valid certificate exchange between users is authenticated as part of the TOE (i.e., Apache Server) and the remote web browser SSL protocol handshake using an RSA key pair.

The TOE maintains user identity, authentication data (I&A credentials), and authorizations on each user of the system. These take the form of the tuplet {username, password, group}. The username and password are stored in the underlying operation system. For clarification, the password is not stored directly, but rather as an MD5 hash. The Identification and Authentication function stores the users associated role, which essentially takes the form of the couplet {username, group}.

A user must authenticate to the eHealth Suite to perform any action on the TOE. The information is sent encrypted via HTTP over SSL v3.0, as described above, from the user's web browser to the eHealth Suite where access is either granted or denied.

9.1.4 Data Protection

Access to TOE data is protected through the access control provided by the TOE and discussed in this section. In order to manipulate data, a user must successfully login via either the OneClickEH interface (as an Administrator) or the web interface . Local access is not permitted by any user other than an authorized Operational Environment administrator that has an account on the local machine. End Users are not given permission to modify anything on the system besides their personal password attributes. Data storage is handled by the underlying Operating System upon which the eHealth Suite resides and the Oracle 10g database.

9.1.4.1 Data Storage

When eHealth collects data about the performance of the monitored network, it stores the data in its database. In its raw form, this detailed performance data is called as-polled data. To reduce the amount of data it stores, saving storage capacity, eHealth aggregates the data as it ages. By default, eHealth keeps the most recent three days' worth of as-polled data in the database.

When the as-polled data becomes older than three days, eHealth aggregates it into hourly samples and retains that data for several weeks. When the hourly data ages, eHealth aggregates it into daily and weekly samples, retaining that data for many more weeks. Reports can still be run using this data, but the same level of detail will not be able to be seen that the as-polled data provides. This process of aggregating data is called database rollup. The eHealth administrator can define the database rollup schedule and change the length of time for which eHealth retains as-polled data, as well as the rolled-up hourly, daily, and weekly data.

9.1.4.2 Configuration

The TOE supports a policy that is created by the eHealth Administrator upon installation of the TOE. Once the eHealth Administrator has successfully logged in, there are several processes that are invoked to begin setting up the access, authorization, audit, data protection, and security management settings. As a part of the initial installation, a configuration process is invoked that (in conjunction with a discovery process) identifies and sets up communication channels with machines using SNMP protocol version 1. Identification information for these machines is then added to processing tables within the eHealth Suite. These processing tables enable the TOE to monitor network resources. Only machines that are on this list (using SNMP protocol version 1) are permitted to communicate with the TOE. Additionally, the initial installation of the eHealth Suite sets up an administrative account. Once the eHealth Suite Version 6.1.2 is installed, the administrator can begin to setup and configure user accounts from the web interface. The eHealth Suite r6.1.2 software provides the authenticated administrators with the ability to view audit trails according to the attributes that the administrator requested to view in the

GUI. The eHealth Suite also provides data protection and security management functionality through the GUI. Authenticated administrators are permitted to manage user accounts and to control which users have access to which data groups.

9.1.5 Encrypted Communications

The TOE uses an Apache web server v2.2.3 to support protection of external TOE communication with the users by performing SSL v3.0 encryption through Apache's OpenSSL-based cryptographic module (mod_SSL). The TOE uses openssl 0.9.8.d. The protocol for transport is HTTP over the Secure Socket Layer protocol, referred to as "HTTPS" or "HTTP over SSL." HTTP over SSL v3.0 is used as the secure communication between the eHealth server and the remote workstation.

No means are provided for the end users to physically access the TOE. The use of SSL v3.0 provides a trusted path for all remote user communication and initial user authentication between the TOE and the remote workstation. This ensures that all traffic to and from the TOE via the remote administration interface is protected from unauthorized disclosure. The eHealth server relies on the user's web browser in the Operational Environment to perform the SSL v3.0 protocol with its associated cryptography to process certificates for authenticating the end points of the communication channel and to encrypt the data. User passwords are not sent in the clear but use an MD5 hash with 64 bit key sizes for comparison to a shared secret on the TOE, the hashing is conformant to the RFC 1321 standard. All SSL v3.0 data is encrypted with 3DES-EDE-CBC keys with 168 bit sizes, this conforms to the FIPS 46-3 standard. RSA with 1024 bit keys is used for symmetric key generation; this conforms to the ANSI X9.31 and ANSI X9.8 standards. These keys are destroyed by the overwrite method. The OneClickEH component hooks into the installation of Internet Explorer installed on the client system in the Operational Environment. The implementation of SSL for communications sent across the OneClickEH interface is therefore trusted by the Operational Environment component.

The protection mechanisms employed by the TOE ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The host Operational Environment administrator can access the TOE to change the time and halt the execution of the TOE application. Because the host Operational Environment is considered to be a trusted IT entity and the interface established to change the time and halt the TOE is via a trusted path, the security domain for the Application TOE is still considered protected from interference and tampering.

9.1.6 Security Management

The TOE maintains the roles of end user and Administrator. An end user is only able to access the web user interface to perform the functions listed in table 9-1. Once an end user has been given access to the OneClickEH interface, that end user then becomes an Administrator.

9.1.6.1 Web User Interface

Administrators and end users can perform administrative functions from the Web User. End users can access this interface only after a web user account has been created for them by an Administrator. By default, a new user account does not have access to any groups, but rather must be manually added to that group by the Administrator. The web interface lets Administrators and end users view eHealth reports and other features from a remote system using a web browser. See Table 9-1 below for details on the functions that can be performed from the web user interface.

9.1.6.2 OneClickEH Interface

The OneClickEH interface acts as the main administrative interface to the eHealth system. The OneClick for eHealth (OneClickEH) interface is initially accessed via the Administration page of the web user interface. Once initially launched, the OneClickEH component can be saved to the remote workstation so future access is not dependent upon the web user interface. However, separate authentication is required for access to the OneClickEH interface. Once an end user is given access to the OneClickEH interface, that end user is then considered an Administrator of the TOE. The table below details the functions Administrators and end users can perform on the TOE:

User	Interface	Action
Administrator	Web User Interface	View/query Reports Run Reports on demand Change Password Log in to different user account Change preferences Manage server status Manage access logs Site configuration Remove reports marked for deletion View elements View advanced logging
	OneClickEH Interface	View discoveries Perform discoveries Manage discover policies Manage jobs Manage DCI rules View process sets Manage polling View all errors View system messages View job history View web activity View OneClickEH activity Schedule jobs View user accounts Create new users Delete users Modify user policy Manage server controls Manage polling controls Manage advanced logging

		View system information Manage eHealth systems View groups Create groups Add elements to groups Delete elements from groups Delete groups Modify users who can see groups Enable/disable element views Search elements not in a group Modify group settings View grouplists Create grouplists Add groups to grouplists Delete groups from grouplists Delete grouplists Search groups not in a grouplist Modify grouplist settings Manage elements Search elements Search elements not grouped Search elements by type Search elements by IP address Search elements by Interface IP address Run reports
End User	Web User Interface	View/query Reports Run Reports on demand Change Password Log in to different user account Change preferences Manage server status Manage access logs Site configuration Remove reports marked for deletion View elements View advanced logging Note: Prior to accessing the web user interface, end users must have a web user account set up by an Administrator. The ability of an end user to perform the functions listed above depends on the permissions granted by Administrators based on the User Policy.

Table 9-1: Functions performed on the TOE

The OneClickEH interface displays a tree structure on the left with access to the administrative functions listed above. On the right, it displays a high-level status summary. From this window, Administrators can access more information by drilling down to various functions. A single OneClickEH interface can manage multiple eHealth systems, even if they are mixed versions.

The Discover portion of the OneClickEH interface provides tabs that represent each aspect of the discover process, including a rules editor, policy set editor and scheduler.

Administrators have the ability to specify alternative initial values to override the default values of new users having minimum privileges when their account is first created.

9.1.6.3 Managing Groups and Grouplists

eHealth enables the Administrator, by way of the User Policy, to organize elements into groups so that related elements can be associated with one another (such as those for a specific department or customer) and generate reports for those specific element sets, or so that the Administrator can filter the elements shown in the OneClickEH interface. To organize groups, the Administrator can use grouplists. For example, Administrators can use grouplists to model larger organizations such as all of the groups for a customer, a company, geographic region, and so on. By focusing on a subset of elements—rather than all elements in the IT infrastructure—the TOE can create effective reports that address specific needs. A group can belong to multiple grouplists. Groups and grouplists can be used together to control access to reports and elements via the Web interface.

As soon as elements are discovered of a specific type, eHealth creates a default group called All that includes all discovered elements of that type. For example, if the TOE has 40,000 LAN/WAN elements, the LAN/WAN All group includes all 40,000 LAN/WAN elements. If the TOE has one system element, the System All group contains that one system element. The TOE cannot add or delete All groups.

9.1.6.4 Changing User Passwords

The Administrator can add new users and set their permissions. The Administrator can add, list, modify, and delete user and system passwords for all users. End users can add, list, modify, and delete their own passwords only.

9.1.6.5 Password Management

The eHealth Suite enables the eHealth Administrator to set up end user accounts on the eHealth Server with a default password of his/her choice. End users are permitted to change their passwords at any time following a successful login if the Administrator sets “user can change password” to ‘YES’.

9.1.6.6 Password Validation

No password complexity validation is done by eHealth Suite Version 6.1.2. It is the responsibility of the organization to ensure that end users and administrators are educated in selecting appropriate passwords.

9.1.6.7 Lost Password Management

In the event that an End User loses his or her password, the eHealth Administrator must change the password in the eHealth Suite. The End User may then login to the eHealth Server and modify their password.

9.1.6.8 Password Reset

The eHealth Administrator will reset an End User password upon request from the user. This reset will set a temporary password that the End User should be instructed to change following first login.

9.1.6.9 Providing Access to Groups and Reports

The Administrator can grant end users permissions to view and use none, some, or all groups and grouplists. The Administrator can view and use all groups and grouplists. For example, Internet Service Provider (ISP) operators need to see a grouplist that contains all of their customers. However, they would likely create a group for each customer and restrict access so that each customer views only their own activity. Groups and grouplists also restrict which eHealth reports a user can run.

To assign permissions to use groups and grouplists the Administrator logs in to the Web server, and selects the user name to modify the access permissions. For each technology type listed in the Groups and Grouplists sections, the Administrator can do one of the following:

- Select No access to prevent the user from viewing any groups, grouplists, or elements for that technology type.
- Select All elements to allow the Web user to view all groups, grouplists, and elements for that technology type.
- Select one or more groups or grouplists from each list to restrict the user to only those groups or grouplists and the elements they contain.

9.1.7 Self Protection

The self protection function is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The TOE is an application running on a dedicated device that executes all of its processes internally. It is accessible only via the defined interfaces. Only authorized users of the host Operational Environment are able to modify the functionality of the TOE. The poller interface enforces domain separation in that any data sent to this interface (which is presumed un-trusted) is logically separated from all other TOE data. It is never executed but rather is parsed for analysis. Traffic flowing through the TOE is subject to the policies as defined by the authorized users.

In the evaluated configuration, traffic can only come into the TOE via three physical interfaces: the HTTPS interface (access to which is controlled by a username and a password), the Oracle Database (which is only accessible by internal TOE processes) or the poller interface (where the traffic is monitored and analyzed by the TOE but no actions can be executed). Because HTTP-basic authentication is used for all requests, unauthorized traffic cannot bypass the identification and authentication mechanisms. In addition, all requests made by the client are validated by the server side. Replacing a client application used to interface with the TOE does not bypass the TSF because the server does not trust the client to make any authorization decisions.

Working in concert with its platform, the TOE works with the Operational Environment (OS and DB) to provide protection of its security functions through non-bypassability and domain separation. All user operations are conducted in the context of an associated session. The TOE manages these sessions to prevent one session from compromising another session. The TOE provides only well-defined interfaces to these sessions, and the sessions allocated only after successful authentication. The TOE relies on its platform to operate correctly and to prevent unauthorized access to TOE data and stored executables.

The OneClickEH component of the TOE is an executable which is downloaded from the TOE's web server. Once it has been saved to a remote client workstation, it resides outside of the self-protection boundary of the TOE. Therefore, the potential exists for a rogue application to impersonate the OneClickEH component. However, because all requests are validated by the server, a client-side modification will not be able to bypass the TSF. In order to reduce the threat of such a modification, administrators should ensure their client workstation is patched and should periodically check to make sure that their system is free of malware. If further assurance is desired, the OneClickEH component can simply be re-downloaded prior to each administrative session. It does not require installation or any other dependencies so it can be run simply by accessing the hyperlink to the executable in the web interface.

9.2 TOE Summary Specification Rationale

This section identifies the security functions provided by the TOE mapped to the security functional requirement components contained in this ST. This mapping is provided in the following table.

Security Function	Security Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_GEN_EXT.1(1) Discover log generation
	FAU_GEN_EXT.1(2) Poller audit generation
	FAU_GEN_EXT.1(3) Message log generation
	FAU_GEN_EXT.1(4) Report generation
	FAU_SAR.1 Audit Review
	FAU_SAR_EXT.1 Audit Review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic Key Management
	FCS_CKM.4 Cryptographic Key Destruction
	FCS_COP.1 Cryptographic Operations
User Data Protection (FDP)	FDP_ACC.1 Subset access control

Security Function	Security Functional Components
	FDP_ACF.1 Security attribute based access control
Identification and Authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security Management (FMT)	FMT_MOF.1 (1) Management of security functions behavior
	FMT_MOF.1 (2) Management of security functions behavior
	FMT_MSA.3 Static Attribute Definition
	FMT_MTD.1 (1) Management of TSF data
	FMT_MTD.1 (2) Management of TSF data
	FMT_MTD.1 (3) Management of TSF data
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Trusted Path	FTP_TRP.1 Trusted Path

Table 9-2: Security Functional Requirements

9.2.1 Security Audit

The audit function of the TOE enforces the FAU_GEN.1, FAU_GEN_EXT.1(1), FAU_GEN_EXT.1(2), FAU_GEN_EXT.1(3), FAU_GEN_EXT.1(4), FAU_GEN.2, FAU_SAR.1, FAU_SAR_EXT.1, FAU_SAR.2 and FAU_SAR.3 requirements.

The main functionality of the TOE is to run discover jobs to find elements in the monitored network and to poll those elements once its configuration has been stored in the Oracle 10g database. The element and poller configuration data is stored in the database and polled by the poller processes to identify attributes of the elements. The Administrator defines the events to be audited, and those events are captured in the discover log, poller audit log and message log. Statistics Polling static window messages are stored on the underlying OS in a file called messages.stats.log. On the TOE these files can reach a maximum size of 100 MB. Once the log file reaches the maximum size, eHealth moves it to a backup log file named messagesbackup.bak and overwrites the existing backup log file, if one exists. eHealth then starts a new log file using the default file name. When the TOE saves the results of a discover process, the TOE creates a pollerAudit.date.time.log file. The TOE saves a minimum of seven files for each type of discover log. It deletes files in excess of the seven files that are older than seven days. As stated in this section, only Administrators are able to view the audit records.

The attributes in the database can be used to create reports that help Administrators track the health of the network over a period of time and to manage network resources. These include Trend reports, Top N reports, At-a-Glance reports and MyHealth reports.

9.2.2 Encrypted Communications

FCS_CKM.1, FCS_CKM.4, FCS_COP.1 and FTP_TRP.1 support the Cryptographic Support and Trusted Path security functions.

The TOE implements the cryptographic key generation and destruction functions of the SSL v3.0 protocol to protect the communication channel between the TOE and remote users. HTTP over SSL v3.0 is used to create a trusted path for remote administration, end user access and initial user authentication. The eHealth server relies on the user's web browser in the Operational Environment to perform the SSL v3.0 protocol with its associated cryptography to process certificates for authenticating the end points of the communication channel and to encrypt and decrypt the data. User passwords are sent by way of an MD5 hash with 64 bit key sizes for comparison to a shared secret on the TOE. All SSL v3.0 data is encrypted with 3DES-EDE-CBC keys with 168 bit sizes. RSA with 1024 bit keys is used for symmetric key exchange. These keys are destroyed by the overwrite method. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

9.2.3 User Data Protection

The data protection function of the TOE enforces the FDP_ACC.1 and FDP_ACF.1 requirements.

As defined in Section 2.4.3, the User Policy is the policy by which the TOE allows or denies access to the functions in the Web user interface and the OneClickEH interface. Administrators must modify the permissions on the individual end user accounts accordingly. End users are only able to access the web user interface once a web user account is set up for them by an Administrator. End users can only access the sections of the web interface that they have been given permission for based on the User Policy. Once an end user has been given access to the OneClickEH interface, that end user is then considered an Administrator. By default, End Users are not given permission to modify anything on the system besides their personal password attributes.

Administrators must successfully login via the remote workstation in order to manipulate data. Administrators can access all objects on the TOE regardless of privileges. Local access is not permitted by any user other than an authorized Operational Environment administrator that has an account on the local machine. Data storage is handled by the underlying Operating System upon which the eHealth Suite resides and the Oracle 10g database.

9.2.4 Identification and Authentication

The Identification and Authentication function of the TOE enforces the FIA_ATD.1, FIA_UAU.2 and FIA_UID.2 requirements.

Authentication is the process of determining the user's true identity. Administrators and end users accesses the eHealth Server through a browser on their remote workstation. The connection is established using HTTP over SSL v3.0. Administrators and end users must authenticate to the eHealth Suite when challenged by providing a valid eHealth username and password. The information is sent encrypted from the user's web browser to the eHealth Server where access is either granted or denied by the eHealth Suite, which maintains the user ID, password, groups and grouplists for comparison. User authentication is meaningful only if there is an extremely low probability of success for random attempts to authenticate as an authorized user. The requirement ensures that the secret authentication data is computationally difficult to guess randomly.

9.2.5 Security Management

The Security Management function of the TOE enforces the FMT_MOF.1(1), FMT_MOF.1(2), FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1 and FMT_SMR.1 requirements.

The TOE maintains the roles of end users and Administrators. Both users access the TOE from a remote workstation. End users only have access to the web user interface after a web user account has been set up for them by an Administrator. Once they have access to the web user interface, end users are only allowed to access the pages that an Administrator has given them access to view. Administrators can perform functions from the web user interface and the OneClickEH itnerface. Once an end user has been given access to the OneClickEH interface, he is then considered an Administrator. Once authenticated, the Administrator is able to perform functions such as modify system settings, modify the User Policy, modify passwords, provide restrictive default values for security attributes, specify alternative initial values to override those default values and define reports.

10 Rationale

10.1 Security Objectives Rationale

The following tables provide a mapping with rationale to identify the security objectives that address the stated assumptions and threats.

Assumption	Objective	Rationale
A.ADMIN One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.	OE.ADMIN One or more eHealth Administrators will be assigned to install, patch, configure and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A.ADMIN in order to ensure that eHealth Administrators install, manage and operate the Operational Environment in a manner that maintains its security objectives.
A.PATCHES Administrators exercise due diligence to patch the Operational Environment (e.g., OS and database) so they are not susceptible to network	OE.ADMIN One or more eHealth Administrators will be assigned to install, patch, configure and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A.PATCHES in order to ensure that eHealth Administrators properly patch the Operational Environment

Assumption	Objective	Rationale
attacks.		in a manner that maintains its security objectives.
A.NOEVIL Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.	OE.NOEVIL Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.	OE.NOEVIL directly maps to A.NOEVIL and ensures that all users of the TOE are properly trained in the configuration and usage of the TOE and will follow the guidance provided.
A.LOCATE The network the TOE monitors is isolated from untrusted networks. The SNMP v1 monitored traffic is limited to a trusted network, (either physically isolated or protected by appropriate network boundary devices).	OE.LOCATE The TOE will be located on a trusted network whose boundary is protected from other networks.	OE.LOCATE directly maps to A.LOCATE to ensure that the monitored network is isolated and safe from interference by other networks.
A.PROTECT The parts of the TOE critical to security policy enforcement will be protected from unauthorized physical modification.	OE.PROTECT The parts of the TOE critical to security policy enforcement will be protected from unauthorized physical modification.	OE.PROTECT directly maps to A.PROTECT to ensure that those responsible for the TOE must ensure that the TOE hardware and software critical to security policy are protected from physical attack and unauthorized physical modification, which might compromise the TOE security objectives.
A.PASSWORD It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data.	OE.PASSWORD ensures that users of the TOE shall be instructed by the administrator guidance to choose strong passwords in accordance with the documented password policy and to protect their authentication data.	OE.PASSWORD directly maps to A.PASSWORD to ensure that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data
A.CLIENT It is assumed that Administrators who download the OneClickEH component regularly ensure that their client machine has up-to-date patches, is scanned for viruses/malware, and periodically re-downloads the OneClickEH component from the web interface to ensure its integrity.	OE.CLIENT Administrators who download the OneClickEH component will regularly ensure that their client machine has up-to-date patches, is scanned for viruses/malware, and periodically re-downloads the OneClickEH component from the web interface to ensure its integrity.	OE.CLIENT directly maps to A.CLIENT to ensure that remote workstations used to access the TOE are free of any malicious additions or modifications of the OneClickEH component.

Table 10-1: Assumption to Objective Mapping

Threat	Objective	Rationale
T.ACCESS A	O.ACCESS The TOE will provide	O.ACCESS (FDP_ACC.1, FDP_ACF.1,

Threat	Objective	Rationale
legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or performs operations for which no access rights have been granted, via user error, system error, or other actions.	measures to authorize End Users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the eHealth Administrator of the TOE.	FIA_ATD.1) addresses T.ACCESS by providing the eHealth Administrator with the capability to specify access restrictions on the protected TOE resources to End Users.
T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.	O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management. O.MANAGE The TOE will provide eHealth Administrators with the resources to manage and monitor user accounts, resources and security information relative to the TOE.	O.ROBUST_ADMIN_GUIDANCE (ALC_DEL.1, AGD_PRE.1, AGD_OPE.1) helps to mitigate T.ADMIN_ERROR by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner and to provide the administrator with instructions to ensure the TOE was not corrupted during the delivery process. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure. O.MANAGE (FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1) addresses T.ADMIN_ERROR by ensuring that only eHealth Administrators can use the provided resources for managing and monitoring user accounts, TOE resources and security information relative to the TOE.
T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.AUDIT The TOE will provide measures for recording security-relevant events that will assist the eHealth Administrators in detecting misuse of the TOE and/or its security features, or in detecting events that would compromise the integrity of the TOE and violate the security objectives of the TOE.	O.AUDIT (FAU_GEN.1, FAU_GEN_EXT.1(1), FAU_GEN_EXT.1(2), FAU_GEN_EXT.1(3), FAU_GEN_EXT.1(4), FAU_GEN.2, FAU_SAR.1, FAU_SAR_EXT.1, FAU_SAR.2, FAU_SAR.3 addresses T.AUDIT_COMPROMISE actually creating the audit records to be protected by the operational environment and ensuring that only Administrators have the ability to review the audit data.
T.MASK Users whether they be	O.AUDIT The TOE will provide measures for recording security	O.AUDIT (FAU_GEN.1, FAU_GEN_EXT.1(1),

Threat	Objective	Rationale
malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.	relevant events that will assist the eHealth Administrators in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE. O.IDEN The TOE will provide measures to uniquely identify End Users and will authenticate the claimed identity prior to granting a user access to the TOE.	FAU_GEN_EXT.1(2), FAU_GEN_EXT.1(3), FAU_GEN_EXT.1(4), FAU_GEN.2, FAU_SAR.1, FAU_SAR_EXT.1, FAU_SAR.2, FAU_SAR.3 addresses T.MASK by providing the eHealth Administrators with tools necessary to monitor user activity to ensure that misuse of the TOE does not occur. O.IDEN (FIA_ATD.1, FIA_UAU.2, and FIA_UID.2) addresses T.MASK by providing measures to uniquely identify and authenticate End Users through successful login via username and password to the Apache Web Server through HTTP over SSL v3.0. The TOE maintains user ID and password for users and groups and grouplists for elements.
T.MODIFY Users, whether they be malicious or non-malicious, could attempt to misconfigure or modify their user accounts in an attempt to tamper with TOE resources or modify security information relative to the TOE.	O.MANAGE The TOE will provide eHealth Administrators with the resources to manage and monitor user accounts, resources and security information relative to the TOE.	O.MANAGE (FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1) addresses T.MODIFY by ensuring that only eHealth Administrators can use the provided resources for managing and monitoring user accounts, TOE resources and security information relative to the TOE.
T.DOS Users or network services, whether they be malicious or non-malicious, could attempt to disable or degrade the performance of networks, systems, or applications in the network.	O.MONITOR The TOE will collect and analyze critical data for network devices, systems, and applications and report on the performance, capacity, availability, and response of these resources.	O.MONITOR (FAU_GEN_EXT.1(1), (FAU_GEN_EXT.1(2), (FAU_GEN_EXT.1(3), (FAU_GEN_EXT.1(4), FAU_SAR_EXT.1 mitigates this threat by having the TOE auditing the health and status of network devices
T.CRYPTO_COMPROMISE A malicious user or process may cause key, data or executable code associated with the cryptographic	O.CRYPTOGRAPHIC FUNCTIONS The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signatures. O.ROBUST_ADMIN_GUIDANCE The TOE will ensure that any	O.CRYPTOGRAPHIC_FUNCTIONS (FCS_CKM.1, FCS_CKM.4, FCS_COP.1, and FTP_TRP.1) mitigates the possibility of malicious users or processes from gaining inappropriate access to cryptographic data, including keys. This objective ensures that the cryptographic data does not reside in a resource that has been used by the

Threat	Objective	Rationale
functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.	information contained in a protected resource is not released when the resource is reallocated.	cryptographic module and then reallocated to another process. O.ROBUST_ADMIN_GUIDANCE (ALC_DEL.1, AGD_PRE.1, and AGD_OPE.1) helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner and to provide the administrator with instructions to ensure the TOE was not corrupted during the delivery process. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure.
T.EAVESDROPPING A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	O.CRYPTOGRAPHIC FUNCTIONS The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signatures.	O. CRYPTOGRAPHIC FUNCTIONS (FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_TRP.1) mitigates T.EAVESDROPPING by ensuring that all communication to and from the TOE are not sent unless they are encrypted.

Table 10-2: Threat to Objective Mapping

10.2 TOE Security Assurance Measures

This section identifies the assurance measures provided by the developer in order to meet the security assurance requirement components for EAL2. These measures are identified in the following table.

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Description	TOE Design v1.0, BAH	This document describes the security architecture of the TOE.
ADV_FSP.2 Functional Specification with complete summary	Functional Specification v1.0, BAH	This document describes the functional specification of the TOE with complete summary.
ADV_TDS.1 Architectural Design	TOE Design v1.0, BAH	This document describes the architectural design of the TOE.

Component	Document(s)	Rationale
AGD_OPE.1 Operational User Guidance	• CA eHealth Administration Guide r6.1, CA • CA eHealth Overview Guide r6.1, CA • CA eHealth Reports User and Administration Guide r6.1, CA • Evaluated Configuration for CA eHealth Suite Version 6.1.2, BAH	These documents describe the operational user guidance for CA eHealth Suite Version 6.1.2.
AGD_PRE.1 Preparative Procedures	• CA eHealth Installation Guide r6.1, CA • CA eHealth Command and Environment Variables Reference Guide r6.1, CA • CA eHealth Release Notes r6.1, CA • Concord Communications Software Delivery Procedures, CA (formerly Concord Communications) • Evaluated Configuration for CA eHealth 6.1.2 version 1.0, BAH	These documents describe the preparative procedures that need to be done prior to installing CA eHealth Suite Version 6.1.2.
ALC_CMC.2 Configuration Management	• eHealth CM build process, CA • eHealth CM process, CA • New eHealth Checkin Process Rollout, CA • Introduction to eHealth Development, CA • NVM Source Code Best Practices, CA • NVM IT Backup Strategy, CA	These documents describe the authorization controls for the TOE.
ALC_CMS.2 CM Scope	Configuration Item List 6.1.2, CA	This document describes the CM scope of the TOE.
ALC_DEL.1 Delivery Procedures	• Concord Communications Software Delivery Procedures, CA (formerly Concord Communications)	This document describes product delivery for CA eHealth and a description of all procedures used to ensure objectives are not compromised in the delivery process.
ASE_CCL.1 Conformance Claims	Security Target v1.1, BAH	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	Security Target v1.1, BAH	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	Security Target v1.1, BAH	This document describes the Introduction of the Security Target.

Component	Document(s)	Rationale
ASE_OBJ.2 Security Objectives	Security Target v1.1, BAH	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Security Requirements	Security Target v1.1, BAH	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	Security Target v1.1, BAH	This document describes the security problem definition of the Security Target.
ASE_TSS.2 TOE Summary Specification	Security Target v1.1, BAH	This document describes the TSS section of the Security Target.
ATE_COV.1 Analysis of Coverage	ATE coverage matrix, BAH	This document provides evidence of the test coverage based on the functional test plan.
ATE_FUN.1 Functional Tests	• Test Plan for eHealth Security Version 6.1.2, CA • Prism results matrix, CA	These documents provide a description of the vendor functional tests which were executed and evidence that all tests were completed successfully.
ATE_IND.2 Independent Testing	Evaluation Team Test Plan for CA eHealth v6.1.2 v1.0, BAH	This document describes the independent testing for the TOE.
AVA_VAN.2 Vulnerability Analysis	Vulnerability Analysis v1.0, BAH	This document describes the vulnerability analysis of the TOE.

Table 10-3: Assurance Requirements Evidence

10.3 EAL Justification

The threats that were chosen are consistent with attacker of low attack potential, therefore EAL2 was chosen for this ST.

10.4 Requirement Dependency Rationale

All Security Functional Requirement component dependencies have been met by the TOE with the exception of FPT_STM.1 and FMT_MSA.1. FPT_STM.1, Reliable Time Stamps is a dependency on FAU_GEN.1, which is met by the Operational Environment. The underlying Operating System will be available to the TOE for use in determining the timestamp for the audit trail. FMT_MSA.1 is a dependency of FMT_MSA.3. FMT_MSA.3 states that the User Policy provides restrictive default values for security attributes, and the Administrators can specify alternative initial values to override those default values. FMT_MSA.3's dependency on FMT_MSA.1 is to enforce the management of the security attributes by specifying which users (Administrators) are authorized to modify the attribute values. The intended functionality of FMT_MSA.1 has been captured in FMT_MTD.1 (3) requirement, which states that only Administrators have the ability to modify the User Policy. Therefore, since the functionality of FMT_MSA.1 has already been captured by another requirement (FMT_MTD.1 (3)) claimed in the evaluation, the intent of the dependency has been met.

10.5 Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the Security Functional Requirement components that address the stated TOE and Operational Environment objectives.

Objective	Security Functional Components	Rationale
O.ACCESS The TOE will provide measures to authorize End Users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the eHealth Administrator of the TOE.	FDP_ACC.1 Subset access control	FDP_ACC.1 requires the TOE to prevent unauthorized access to TOE resources by enforcing the eHealth User Policy.
	FIA_ATD.1 User Attribute Definition	FIA_ATD.1 ensures that End Users have a defined set of tasks that they can perform based on their access permissions defined by the User Policy set by the eHealth Administrator.
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 requires the TOE to enforce the User Policy on the protected TOE resources and requires the eHealth Administrators to configure End User access rights accordingly.
O.AUDIT The TOE will provide measures for recording security relevant events that will assist the eHealth Administrators in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and	FAU_GEN.1 Audit data generation	FAU_GEN.1 defines the security relevant events that will be recorded by the TOE along with the details of the event that will be recorded.

Objective	Security Functional Components	Rationale
violate the security objectives of the TOE.	FAU_GEN.2 User identity association	FAU_GEN.2 requires the TOE to associate each auditable event with the identity of the End User or eHealth Administrator that caused the event.
	FAU_SAR.1 Audit Review	FAU_SAR.1 requires that the TOE provide audit records in a manner that is suitable for an administrator to interpret.
	FAU_SAR.2 Restricted audit review	FAU_SAR.2 ensures that the TOE provides mechanisms to protect the audit records from unauthorized access.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 provides the ability for an administrator to sort the audit data to readily locate security relevant events of interest.
O.MONITOR The TOE will collect and analyze critical data for network devices, systems, and applications and report on the performance, capacity, availability, and response of these resources.	FAU_GEN_EXT.1(1) Discover log generation	FAU_GEN_EXT.1(1) requires generation discover log based on additional logical or physical elements and the ability to record information for each server object audit job.
	FAU_GEN_EXT.1(2) Poller audit log generation	FAU_GEN_EXT.1 (2) requires generation of poller audit logs based on MIBs and recording information within each entry of the web log.
	FAU_GEN_EXT.1(3) Message log generation	FAU_GEN_EXT.1 (3) requires generation of message logs and recording information within each entry of the poller audit log.
	FAU_GEN_EXT.1(4) Report generation	FAU_GEN_EXT.1 (4) requires the TOE to be able to generate reports based on data stored in the Oracle database populated by the TOE.

Objective	Security Functional Components	Rationale
	FAU_SAR_EXT.1 Audit review	FAU_SAR_EXT.1 requires the TOE to read information collected in FAU_GEN_EXT.1(1), FAU_GEN_EXT.1(2), FAU_GEN_EXT.1(3) FAU_GEN_EXT.1 (4) from the discover logs, poller audit logs, message logs, and Health reports in a manner that is suitable for an administrator to interpret.
O.IDEN The TOE will provide measures to uniquely identify End Users and will authenticate the claimed identity prior to granting a user access to the TOE.	FIA_ATD.1 User attribute definition	FIA_ATD.1 ensures that End Users have a defined set of tasks that they can perform based on their access permissions defined by the User Policy set by the eHealth Administrator. The TOE maintains user ID and password for users and groups and grouplists for elements.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires a user be authenticated before any access to the TOE and resources protected by the TOE is allowed.
	FIA_UID.2 User identification before any action	FIA_UID.2 requires a user be identified before any access to the TOE and resources protected by the TOE is allowed.
O.MANAGE The TOE will provide eHealth Administrators with the resources to manage and monitor user accounts, resources and security information relative to the TOE.	FMT_MSA.3Static Attribute Initialization	FMT_MSA.3 states the TSF shall enforce the User Policy to provide restrictive default values for security attributes that are used to enforce the SFP. It allows the Administrators to override the default values set for security attributes when creating data for use by the TOE such as user accounts.
	FMT_MOF.1(1) Management of security functions behavior	FMT_MOF.1 (1) ensures that modification of any setting on the eHealth Server is handled by an eHealth Administrator. End Users are permitted to modify their own password once authenticated through the web browser.

Objective	Security Functional Components	Rationale
	FMT_MOF.1(2) Management of security functions behavior	FMT_MOF.1 (2) ensures that only Administrators and authorized end users can generate views of the Elements stored in the Oracle 10g database.
	FMT_MTD.1 (1) Management of TSF data.	FMT_MTD.1 (1) allows only authenticated users to query the eHealth reports.
	FMT_MTD.1 (2) Management of TSF data.	FMT_MTD.1 (2) allows only the specific end user and eHealth System Administration the ability to modify the user's password.
	FMT_MTD.1 (3) Management of TSF data.	FMT_MTD.1 (3) allows only the eHealth Administrator the ability to modify the end user profiles and access permissions.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 requires that the TOE provide the ability to manage its security functions including the management of user accounts and user access rights, TOE resources and security information recorded in the audit logs.
	FMT_SMR.1 Security roles	FMT_SMR.1 requires the TOE to provide the ability to set roles for security relevant authority as well as to restrict the ability to define and assign roles to eHealth Administrators.
O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.	ALC_DEL.1 Delivery Procedures	ALC_DEL.1 describes product delivery and a description of all procedures used to ensure objectives are not compromised in the delivery process.
	AGD_PRE.1 Preparative Procedures	AGD_PRE.1 documents the procedures necessary and describes the steps required for the secure installation, generation, and start-up of the TOE.
	AGD_OPE.1 Operational user guidance	AGD_OPE.1 describes the proper use of the TOE from a user standpoint.
O.CRYPTOGRAPHIC_FUNCTIONS The TOE shall provide	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 states that the TOE generates cryptographic keys for SSL

Objective	Security Functional Components	Rationale
cryptographic functions for its own use, including encryption/decryption and secure hash.		v3.0 using RSA with 1024 bit keys.
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 states that the TOE destroys cryptographic keys using the overwrite method.
	FCS_COP.1 Cryptographic operation	FCS_COP.1 states that the TOE uses 3DES-EDE-CBC with 168 bit keys for encryption and decryption and 64 bit keys for secure hash.
	FTP_TRP.1 Trusted Path	FTP_TRP.1 ensures that the TOE provides a logically distinct communication path between itself and remote users and for initial user authentication.

Table 10-4: Security Functional Requirements Rationale

10.6 Extended Requirements Rationale

This TOE contains the following extended security functions:
FAU_GEN_EXT.1(1)
FAU_GEN_EXT.1(2)
FAU_GEN_EXT.1(3)
FAU_GEN_EXT.1(4)
FAU_SAR_EXT.1(1)

10.6.1 FAU_GEN

FAU_GEN_EXT.1 (1), FAU_GEN_EXT.1 (2), FAU_GEN_EXT.1 (3), FAU_GEN_EXT.1 (4) were created to capture the basic functionality provide by the TOE. FAU_GEN_EXT.1 (1) allows for TOE to perform discovery of the monitored network and generate a discover log to identify the logical or physical elements that were discovered. FAU_GEN_EXT.1(2) was created for the TOE to continue polling those elements discovered during the discovery process and generating a poller audit log to record captured information within each entry of the remote MIBs. FAU_GEN_EXT.1 (3) was created to allow the TOE to record audit data in a message log to capture statistics polling window messages. FAU_GEN_EXT.1(4) was created to allow end-users and administrators of the TOE to query the data collected by the other logs and run graphical reports on the data and track trends and perform analysis that can be used to improve the “health” of the network monitored by the polling process.

10.6.2 FAU_SAR

FAU_SAR.EXT.1 (1) was created to provide additional capabilities of the TOE to read information collected in FAU_GEN_EXT.1 (1), FAU_GEN_EXT.1 (2), FAU_GEN_EXT.1 (3), and FAU_GEN_EXT.1 (4).

This Security Target does not include any explicitly stated Security Assurance Requirements.

10.7 PP Claims Rationale

This Security Target does not claim Protection Profile conformance.