National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

CA eHealth Network Performance Manager 6.1.2

Report Number: CCEVS-VR-VID10367-2010
Version 1.3
May 19, 2010

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

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

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is version 6.1.2 of the CA eHealth Network Performance Manager (eHealth) product. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in April 2010. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 2 (EAL2) augmented with ASE_TSS.2 (TOE Summary Specification). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Booz Allen Hamilton Common Criteria Test Laboratory evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on this, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions are justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

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.

The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The document *CA eHealth Network Performance Manager Security Target version 1.1, dated 7 April 2010* identifies the specific version and product code of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the CA eHealth product by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Table 1 provides the evaluation details:

Table 1 – Evaluation Details

Evaluated Product	CA eHealth Network Performance Manager (eHealth) 6.1.2, product code **EHDVCP990**
Sponsor & Developer	CA, Inc., Framingham, MA
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	April 2010
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL2 augmented with ASE_TSS.2
Description	The TOE is the eHealth 6.1.2 software, which is a network management product developed by CA, Inc.
Disclaimer	The information contained in this Validation Report is not an endorsement of the eHealth product by any agency of the U.S. Government, and no warranty of the eHealth product is either expressed or implied.
PP	None
Evaluation Personnel	Justin Fisher Christopher Gugel Kevin Micciche Jeremy Sestok Amit Sharma
Validation Body	NIAP CCEVS

2.1 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

Table 2 – Threats

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

Users whether they be malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.
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.
A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
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.

3 Identification

The product being evaluated is CA eHealth Network Performance Manager 6.1.2. The product code for acquiring the CC-certified version of the product is **EHDVCP990**.

4 Security Policy

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. 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.

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.

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.

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.

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.

5 Assumptions

5.1 Personnel Assumptions

Table 3 – Personnel Assumptions

One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.
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.
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.
Administrators exercise due diligence to patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.
It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data.

5.2 Physical Assumptions

Table 4 – Physical Assumptions

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

5.3 Connectivity Assumptions

Table 5 – Connectivity Assumptions

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).

6 Clarification of Scope

6.1 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.

6.1.1 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.

6.1.2 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. In addition, the Motif Console, Reports Center, Reports Scheduler, and High Availability capabilities were not tested. The OneClick for eHealth component was tested operationally to access the TOE and the Command Line Interface was tested during initial configuration to enable the trusted path.

- **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.

6.1.3 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.

6.2 System Requirements

6.2.1 Hardware Components

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

Table 6 – eHealth's Hardware Components

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

6.2.2 Software Components

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

Table 7 – eHealth's Software Components

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

7 Architectural Information

7.1 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

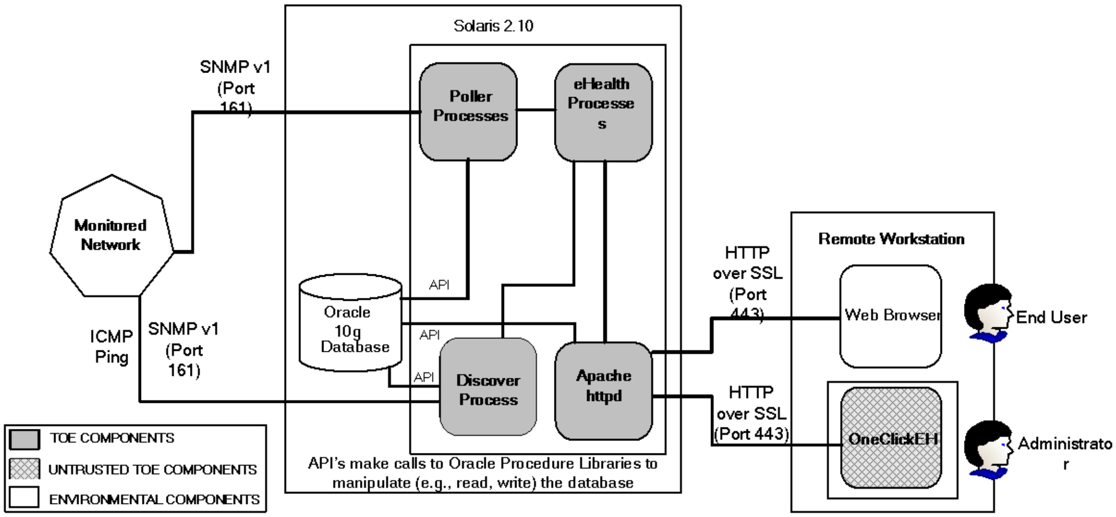

Figure 1 – TOE Boundary

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. 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. The 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.

7.2 TOE Components

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.

The table below defines each component of CA eHealth Suite Version 6.1.2.

Table 8 – TOE Components

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 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	Definition
	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.

7.3 OneClick for eHealth

The OneClick for eHealth (OneClickEH) component is a standalone downloaded executable that is required to perform many of the administrative functions of the TOE. This executable utilizes Internet Explorer DLLs in order to establish communications with the eHealth server. While it is essentially a web browser with different graphical capabilities, it cannot be used to manually enter URLs.

Data is received from the eHealth server by Internet Explorer as XML. Based on the hooks between the two programs, OneClickEH then receives this XML and uses it to build the presentation that is ultimately shown to the administrator. Because OneClickEH utilizes the client system's version of Internet Explorer, upgrading to the latest version of Internet Explorer will remove comparable risks from the use of OneClickEH.

8 Documentation

The documents were evaluated to satisfy assurance requirements:

Table 9 – Assurance Documents Evidence

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Description	TOE Design Specification Document for CA eHealth Version r6.1.2, Version 1.0, 23 February 2010, BAH	This document describes the security architecture of the TOE.
ADV_FSP.2 Functional Specification with complete summary	Functional Specification Document for CA eHealth Version r6.1.2, Version 1.0, 23 February 2010, BAH	This document describes the functional specification of the TOE with complete summary.
ADV_TDS.1 Architectural Design	TOE Design Specification Document for CA eHealth Version r6.1.2, Version 1.0, 23 February 2010, BAH	This document describes the architectural design of the TOE.
AGD_OPE.1 Operational User Guidance	• CA eHealth Administration Guide r6.1, 2008, CA • CA eHealth Overview Guide r6.1, 2008, CA • CA eHealth Reports User and Administration Guide r6.1, 2008, CA • Evaluated Configuration for CA eHealth Suite Version 6.1.2, version 1.0, 7 April, 2010, 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, 2008, CA • CA eHealth Command and Environment Variables Reference Guide r6.1, 2008, CA • CA eHealth Release Notes r6.1, 2008, CA • Concord Communications Software Delivery Procedures, 11 January 2005, CA (formerly Concord Communications) • Evaluated Configuration for CA eHealth Suite Version 6.1.2, version 1.0, 7 April, 2010, 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 • Current eHealth CM process, 27 January 2010, CA • New eHealth Checkin Process Rollout, CA • Introduction to eHealth Development, CA • NVM Source Code Best Practices, version 1.0, 29 December 2009, CA • NVM IT Backup Strategy, version 1.2, 18 October 2007 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.

Component	**Document(s)**	**Rationale**
ALC_DEL.1 Delivery Procedures	Concord Communications Software Delivery Procedures, 11 January 2005, 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	CA eHealth Network Performance Manager 6.1.2 Security Target version 1.1, 7 April 2010, BAH	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	CA eHealth Network Performance Manager 6.1.2 Security Target version 1.1, 7 April 2010, BAH	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	CA eHealth Network Performance Manager 6.1.2 Security Target version 1.1, 7 April 2010, BAH	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	CA eHealth Network Performance Manager 6.1.2 Security Target version 1.1, 7 April 2010, BAH	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Security Requirements	CA eHealth Network Performance Manager 6.1.2 Security Target version 1.1, 7 April 2010, BAH	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	CA eHealth Network Performance Manager 6.1.2 Security Target version 1.1, 7 April 2010, BAH	This document describes the security problem definition of the Security Target.
ASE_TSS.2 TOE Summary Specification	CA eHealth Network Performance Manager 6.1.2 Security Target version 1.1, 7 April 2010, BAH	This document describes the TSS section of the Security Target.
ATE_COV.1 Analysis of Coverage	ATE coverage matrix, (Booz_Allen_CA_eHealth_6.1_ATE_2_matrix_20091218.xls), 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, version 1.0, 11 February 2010, CA • Prism results matrix, (PrismResults.xls), CA • Prism_Results, 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, version 1.0, BAH	This document describes the independent testing for the TOE.
AVA_VAN.2 Vulnerability Analysis	Vulnerability Analysis CA eHealth Suite Version 6.1.2, version 1.0, 2 February 2010, BAH	This document describes the vulnerability analysis of the TOE.

These documents are provided to customers who have purchased the TOE.

9 TOE Acquisition

The NIAP-certified eHealth product is acquired via normal sales channels and digital delivery of the TOE is coordinated with the end customer by the vendor. The product code for the certified product can be found in section 3 of this document.

10 IT Product Testing

The test team's test approach was to test the security mechanisms of the CA eHealth Version 6.1.2 by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface is to be described in CA eHealth design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Security Architecture (ARC) and the vendor's test plans will be used to demonstrate test coverage of all EAL2 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements will be determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing of the vendors’ tests. Booz Allen also performed a vulnerability assessment and penetration testing consistent with the requirements of EAL2.

Consistent with validator recommendation at the initial VOR, the evaluation team ran a subset of the tests using IE8.

10.1 TEST METHODOLOGY

10.1.1 Vulnerability Testing

The evaluation team executed the following vulnerability tests against CA eHealth 6.1.2:

- **Eavesdropping on Communications**

  In this test, the evaluators will manually inspect network traffic to and from the TOE in order to ensure that no useful information could be obtained by a malicious user on the network.

- **Unauthenticated Access / Directory Traversal / CGI Exploitation**

  This test includes three different methods of URL exploitation

  The first part of this test attempts to access protected TOE resources as an unauthenticated outsider.

  The second part of the test attempts different methods to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).

  The third part of the test attempts to access protected resources on the TOE through any potential CGI vulnerabilities

- **Port Scanning**

  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test will attempt to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- **Direct Database Access**

  The TOE should perform all direct interaction to and from the backend database.

  This test will attempt to access the backend database directly and bypass the normal access procedures.

- **Web Server Vulnerability Scanner**

  This test uses the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interface. This scanner probes a wide range of vulnerabilites that include the following:

  - File Upload
  - Interesting File / Seen in logs
  - Misconfiguration / Default File
  - Information Disclosure
  - Injection (XSS/Script/HTML)
  - Remote File Retrieval
  - Denial of Service
  - Remote File Retrieval
  - Command Execution / Remote Shell.
  - SQL Injection.
  - Authentication Bypass
  - Software Identification
  - Remote source inclusion

- **Generic Vulnerability Scanner**

This test uses the Nessus Vulnerability scanner to further test not only the web interface of the TOE, but also any other interface that is present. This scanner probes a wide range of vulnerabilities that include the following:

- Backdoors
- CGI abuses
- Denial of Service
- Finger abuses
- Firewalls
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- Miscellaneous
- Netware
- NIS
- Port scanners
- Remote file access
- RPC
- Settings
- SMTP Problems
- SNMP
- Untested
- Useless services

- **Buffer Overflow / Cross Site Scripting / SQL Injection**

  This will perform automated buffer overflow, cross site scripting, and SQL injection attacks against the TOE as both an authenticated and an unauthenticated user.

- **Hijack SNMP Session**

  This test will attempt to corrupt the state of the TOE by effectively taking over a session between the eHealth server and a polled device. If successful, the TOE will be given false information about the device and potentially report it as true.

- **Certificate Integrity**

  This test will demonstrate the claimed functionality of the TOE to overwrite and change encryption keys.

- **ICMP Blind Connection Reset**

  This test will attempt to exploit a known vulnerability using ICMP connection reset packets. If effective, this test would prevent the normal functionality of the TOE and invoke a denial of service against it.

10.1.2 Vulnerability Results

The following lists any issues that were discovered as a result of the vulnerability testing process. These issues along with the related guidance for mitigation have been included in the document *Evaluated Configuration for CA eHealth 6.1.2, version 1.0, 7 April 2010.*

- **HTTP TRACE methods allowed by the web server**

  The web server running eHealth needs to be configured to disable the execution of HTTP TRACE methods. The potential exists for these methods to contain malicious requests, and since they are not used by the TOE, they can safely be disabled.

- **mod_ssl certificate buffer overflow**

  The version of mod_ssl used by the TOE is potentially exploitable by overflowing the buffer with an arbitrarily long malformed certificate. This vulnerability can be mitigated by using shmcb for the shared session cache. shmcb is a cyclic buffer so any overflow will only overwrite itself as opposed to a hashtable buffer. This can be mitigated by updating ssl.conf.

- **Apache benchmark denial of service**

  The potential exists for opening a large number of connections to the TOE’s web server to deny legitimate traffic. This is considered an acceptable residual vulnerability due to the ubiquity of DoS attacks and the lack of a claim of protection against T.DOS in the ST.

- **SSL cipher suite downgrade**

  The evaluators discovered that the default configuration for the SSL module in eHealth allowed a client to use cryptographic ciphers that were below the strength level described in the ST. The web server should be configured to only allow clients that support high strength cipher suites.

- **SQL injection vulnerability**

  The ‘run’ function on the web interface had improperly bound form variables ‘subject’ and ‘subjectSelected’ that can be replaced with arbitrary SQL code in the URL to disrupt or obfuscate data in the database. This is a severe issue that cannot be mitigated through configuration.

  This has been disclosed to the vendor and a hotfix has been developed. The hotfix has been tested and incorporated into the delivery and preparatory guidance so that it no longer applies to the TOE.

  The testing confirmed that the functionality of report generation was not impacted by the fix to the parameter binding

- **Oracle listener active**

The evaluators discovered that the Oracle listener, TCP port 1521, is open on the eHealth server. The vendor has confirmed that it is required to be listening in order for the TOE to function properly. The evaluators have observed that the following mitigation strategies can be applied in order to ensure the TOE is protected from attacks on this interface:

- Enable logging for the listener
- Set a default password for the listener
- Disable runtime modifications in listener.ora
- Remove unused external procedures
- Block incoming SQL*Net requests to the server

The whitepaper for securing the Oracle listener can be found at http://www.integrigy.com/security-resources/whitepapers/Integrigy_Oracle_Listener_TNS_Security.pdf

Fixes that were not mentioned are already applied by default

11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the CA eHealth 6.1.2 TOE meets the security requirements contained in the Security Target.

The criteria against which the CA eHealth 6.1.2 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September, 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2, September, 2007. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the CA eHealth 6.1.2 TOE is EAL2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in April 2010.

12 Validator Comments/Recommendations

The "Evaluated Configuration for CA eHealth 6.1.2" document (version 1.0, April 7, 2010) defines the recommendations and secure usage directions for the TOE as derived from testing.

The following Validator Comments are issued in concurrence with the completion of this evaluation:

1. The OneClickEH executable component of the TOE must reside on a client machine and as such is not considered to be a trusted application. To provide a greater assurance of its integrity, it is recommended that the OneClickEH executable be re-downloaded periodically from the eHealth server.

2. The TOE does not have a mechanism to enforce password composition rules. DOD IAIA control/NIST SP 800-53 IA-5(1) controls are met only through procedural guidance.
3. Discrepancies between the evaluated configuration of the TOE and the STIGs for the operating system, web server, and database used by the TSF have not been analyzed.
4. The TOE does not have built-in audit export capabilities. Audit files are written to the **/log** directory underneath the directory in which eHealth is installed. It is the responsibility of administrators to periodically export these files.
5. When Oracle updates are released, they should not be installed immediately. CA will conduct internal testing on the patched version of Oracle and will provide upgrade instructions to the customer once the testing has completed.
6. When backing up the Oracle database, the instructions specified on pages 122-123 of the *CA eHealth Administration Guide r6.1* should be adhered to.
7. Network administrators should be vigilant of the potential for denial of service attacks against their network assets and ensure their external firewalls are configured properly and their internal network is monitored appropriately.

13 Security Target

The security target for this product’s evaluation is *CA eHealth Network Performance Manager 6.1.2 Security Target, version 1.1, dated 7 April 2010.*

14 List of Acronyms

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

15 Terminology

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.

16 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 2.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 2.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 2.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2.
5. CA eHealth Network Performance Manager 6.1.2 Security Target, version 1.1, dated 7 April 2010.
6. Evaluation Technical Report for a Target of Evaluation CA eHealth Network Performance Manager 6.1.2 Security Target v1.1 Evaluation Technical Report v1.0 dated 7 April 2010.