CA SPECTRUM® Network Fault Manager r9 SP1 Security Target

Version 1.5
August 14, 2009

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.

ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation. This ST targets Evaluation Assurance Level 2 (EAL2).

1.1.1 ST Identification

ST Title:	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target
ST Version:	1.5
ST Publication Date:	August 14, 2009
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this ST provides identifying information for the CA SPECTRUM® Network Fault Manager r9 SP1. It includes an ST Introduction, ST Reference, ST Identification, TOE Reference, TOE Overview, and TOE Type. Chapter 2 discusses the TOE Description, which consists of 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 the CA SPECTRUM® Network Fault Manager r9 SP1 to satisfy the security functional and assurance requirements. Chapter 10 provides a rationale, or pointers to a rationale, for security objectives, assumptions, threats, requirements, dependencies, and PP claims. Chapter 11 provides the terminology and acronyms used within the ST.

1.1.3 References

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2007-09-004, Version 3.1 Revision 2, September 2007.	[CC]
SPECTRUM OneClick Console User Guide [5130] r9.0	[5130]
SPECTRUM SpectroSERVER Performance Administration Guide [3509] r9.0	[3509]

Reference Title	ID
SPECTRUM OneClick Administration Guide [5166] r9.0	[5166]
SPECTRUM Control Panel User Guide [5029] r9.0	[5029]
SPECTRUM Installation Guide [5136] r9.0	[5136]
SPECTRUM Report Manager Installation and Administration Guide [5169] r9.0	[5169]

Table 1 References

TOE Reference

1.1.4 TOE Identification

CA SPECTRUM® Network Fault Manager r9 SP1

1.1.5 TOE Type

SPECTRUM® Network Fault Manager r9 SP1 provides the following: Network Management

1.1.6 TOE Overview

SPECTRUM® Network Fault Manager r9 SP1, hereupon referred to as SPECTRUM, is a network management system that monitors the state of managed elements, including devices, host systems, and connections. Status information, such as fault and performance data from these elements, is collected and stored. SPECTRUM constantly analyzes this information to track conditions within the network it monitors. If an abnormal condition is detected, the event is analyzed and the appropriate users are alerted. SPECTRUM presents the user with possible causes and solutions to the problem.

The TOE will:

- Provide auditing of user's actions on the TOE
- Provide identification and authentication of its users
- Provide access control based on assigning security communities, privileges, and roles to a specific user, or to a group in which a user belongs
- Provide management of user accounts and their security attributes

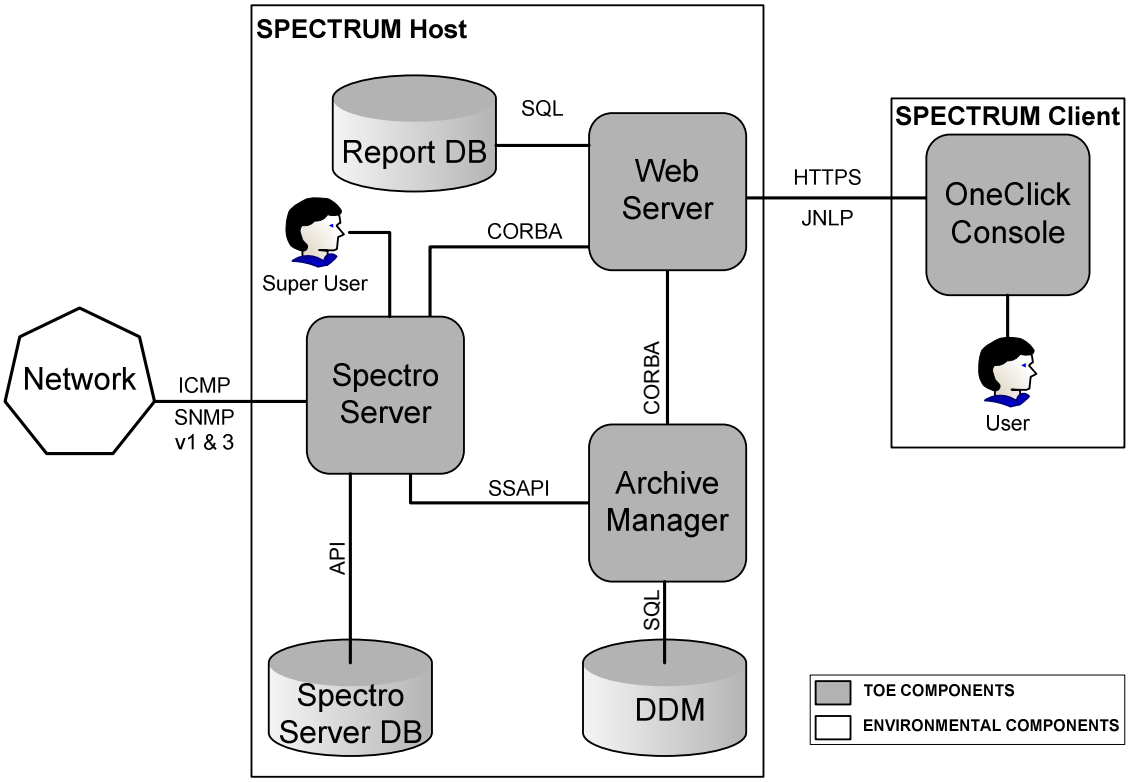

Figure 1 TOE Boundary

There are three default user roles in the evaluated configuration which are maintained by the TOE: Super User, Administrator, and Operator. Access to SPECTRUM by users is performed over three interfaces during the setup and configuration of the TOE, but only two of those interfaces are security relevant while the TOE is in the evaluated configuration. Only the user with the Super User role will have direct access to the host machine with the main components of the TOE; while the client machine will be accessible to all users maintained by the TOE. From the client machine the users have access to two interfaces to SPECTRUM, all of which connect to SPECTRUM via the Web Server located on the host machine. The interface which is not security relevant in the evaluated configuration but are used during the setup and configuration of the TOE are the SPECTRUM Control Panel; which hereupon will be described as a SPECTRUM interface. The two interfaces which are security relevant in the evaluated configuration of the TOE are the OneClick Console, and the OneClick & Report Manager Web Pages; which hereupon will be described as TOE interfaces.

The user with the Super User role will be the only user who has direct access to the host machine and thus access to the SPECTRUM Control Panel. This is because the user with the Super User role will be the user who installs SPECTRUM, and therefore will receive the highest level of privileges for the TOE, including the Service Manager role's privileges. The Services Manager role is an additional role provided by SPECTRUM which can be assigned to any user; however, this role will not be provided to any other user in the evaluated configuration. SPECTRUM relies on the host machine's OS to provide identification, authentication, and authorization support for access to the SPECTRUM Control Panel interface, which is why the TOE will be installed under the administrator or root account for the OS. This interface is used to start and stop the SpectroSERVER and Archive Manager, configure the TOE, and perform other maintenance tasks. The only security relevant features for the SPECTRUM Control Panel are the abilities to create and maintain user accounts. These abilities can also be done via the OneClick Console; therefore, this interface is placed outside the evaluated configuration and will only be used for the initial setup and configuration of the TOE.

The first interface on the client machine is the OneClick & Report Manager Web Pages which can be accessed via the OneClick Console or through the following URLs:
https://host_ip_address:port_number/spectrum/admin/index.jsp
https://host_ip_address:port_number/spectrum/repmgr
When access to the web pages is requested the user must provide their authentication information, username and password, to gain access to SPECTRUM. These web pages provide access to many configuration pages for SPECTRUM, and integration components within SPECTRUM which allow SPECTRUM to interface with additional CA and third party products. These web pages are also used to generate reports on the information the TOE has collected on the monitored network. Note: This interface is encrypted by SPECTRUM; however, the encryption of this interface has not been included as part of the TOE. 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 second interface from the client machine is the OneClick Console. This is a GUI which can be launched from either the OneClick & Report Manager Web Pages or the executable file located on the machine's OS which is downloaded during the installation of the TOE. Once launched the user must provide their authentication information, username and password, to gain access to the TOE. Once access to this interface is granted, a user can access the event records which the TOE creates. The OneClick Console is also used to provide the functionality which makes the TOE a network management system to its users. This functionality includes allowing a user to discover elements, model elements, and manage events or alarms. Note: This interface is encrypted by SPECTRUM; however, the encryption of this interface has not been included as part of the TOE. 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.

Components of the TOE (in evaluation)

CA SPECTRUM® Network Fault Manager r9 SP1 is made of seven components; the SpectroSERVER, the SpectroSERVER Database, the Archive Manager, the Distributed Data Manager (DDM) database, the Web Server, Report Database and the OneClick Console.

1.1.7 SpectroSERVER

SpectroSERVER is the primary server for the SPECTRUM product; it functions as a database server, modeling engine, and device manager. SpectroSERVER processes events, generates alarms, and tracks statistics concerning managed elements.

1.1.8 SpectroSERVER Database

The SpectroSERVER relies on this object-oriented database which contains model types that define how a managed element is represented, and models that represent specific managed elements.

1.1.9 Archive Manager

The Archive Manager is used to log and retrieve historical event records, which it provides to users via the Web Server when access to the stored information is requested.

1.1.10 Distributed Data Manager

The Distributed Data Manager (DDM) database stores the logged historical event records of the elements which SPECTRUM manages on its monitored network. The DDM database is updated with the information which is sent to it via the Archive Manager.

1.1.11 Web Server

The Tomcat Web Server contains two components: the OneClick Server and the Report Manager. The OneClick Server allows users from a remote machine to connect to the TOE to manage the TOE's users, access control features, and perform the TOE's network management capabilities on the models of elements within the network the TOE manages. Report Manager allows users generate up-to-date reports about the inventory, availability, performance, change and fault history of network assets managed by SPECTRUM.

1.1.12 Report Database

The Report Database stores the information which the Report Manager extracts from the SpectroSERVER Database. This information is kept current by the Report Manager by extracting the information at regular intervals.

1.1.13 OneClick Console

The OneClick Console is a graphical user interface which is designed to deliver SPECTRUM information to remote users. OneClick's architecture uses the Java Network Launch Protocol (JNLP) v1.6.0 and the Java Web Start application to allow remote systems and users to access the Web Server.

1.1.14 Network

The network and its elements which SPECTRUM monitors are not components of the TOE. Depending on how the user with the Super User role configures the TOE to operate, the SpectroSERVER receives information from various different elements on the network. Communications traverse between the network elements and the SpectroSERVER via the IETF Standard SNMP protocol version 1, or 3. SPECTRUM will work with an SNMP manageable device that has defined MIB support which can be certified and supported with SPECTRUM. The SNMP management devices are listed at *http://support.concord.com/devices/html/search_sp.html*.

Excluded From TOE (out of evaluation)

- Local Configuration Files
- Operating Systems
- E-Mail Alerts
- Distributed SpectroSERVER
- Integration with CA eHealth
- Integration with LDAP Directory
- Single Sign-On (Integration with CA EEM or SiteMinder)
- Integration with CA Unicenter NSM
- Model Type Editor
- All Other Third Party Applications (includes the installation and use of the CORBA Toolkit and Extensions Integration Toolkit to integrate the Third Party Applications with the TOE)
- Service Manager and the Service Manager Role

SPECTRUM Concepts

This section details the concepts regarding the SPECTRUM approach to a network management system. SPECTRUM will monitor and manage the performance of networks, and systems which have been discovered by the SpectroSERVER.

1.1.15 Elements

An element is a device, host system, or connection that SPECTRUM discovers and then collects data through the element's MIBs via the Simple Network Management Protocol (SNMP) version 1, or 3. Depending on the TOE's configuration an element can then be polled by the TOE on a regular basis, to update the attributes which make up the TOE's informational representation of that particular element.

1.1.16 Knowledge Base

One of the main parts of SpectroSERVER is the knowledge base, which stores current model types, relations, models, and event information. The knowledge base is comprised of data and the procedural information necessary to manage the monitored network. This includes a modeling catalog which is the knowledge base's meta-data.

1.1.16.1 Model Types

Model types correspond mainly with different families of managed elements and are the templates used to build models. Model types contain the information (attributes) needed to manage a specific type of managed element. In addition, there are also model types for the users and groups which are created.

1.1.16.2 Attributes

Each model type has attributes that defines the characteristics and properties of the managed element that the model type represents. These attributes can be either internal or external. External attributes reflect objects from the MIBs supported by the managed element. Internal attributes reflect information that is specific to SPECTRUM's management of a particular element. All attributes have default values associated with the model type.

1.1.16.3 Relations

Relations define the potential ways that models can be related to each other. There are many relations defined in the SPECTRUM knowledge base. Contains, Manages, and Connects_to are all examples of relations. A meta-rule identifies the model types that the models need to be in order to participate in a relation. Examples of a relation which follows the meta-rule format would be: '*LAN* contains *workstations*' or '*switch* connects_to *workstations, routers, etc*.'

1.1.16.4 Models

In addition to storing model types, the knowledge base stores all of the models that have been instantiated to represent elements of the network it monitors, as well as, the users/groups of the TOE which have been created. A model is created by copying the template of the model type it is, and then inputting values for the attributes to represent the real world element in the monitored network or the user/group that has been created. The knowledge base stores the current value for each attribute of the model.

1.1.16.5 Inference Handlers

Inference handlers define the behavior and intelligence of a model type. Each inference handler can perform a specific task. The task can be as simple as changing the value of an attribute, or it may be as complex as discovering all the managed elements on a segment of a network. An inference handler may perform a generic task like calculating an average, or it may perform a task specific to a model type, such as creating models of ports in LAN switches.

1.1.16.6 Actions

SPECTRUM defines a set of operations that can be performed on a model, such as reading or writing an attribute. To expand on the number of operations that can be performed on a model, SPECTRUM provides a mechanism called an action. Sending an action to a model causes the model type to react in some way; for example, it may return requested data to the action's sender, or it may cause the model type to perform a specific task.

1.1.17 Discovery

Discovery finds devices in the network, collects its MIB objects which the SpectroSERVER will use to then create a model of that device. The Discovery process uses a set of configuration parameters to determine which network entities to discover and model. A user specifies these configuration parameters using Discovery accessed from the OneClick Console. Users have the ability to perform Discovery in an automated method or a manual method.

1.1.18 Polling

SpectroSERVER constantly updates its knowledge of network conditions using SNMP and ICMP polling services. When attributes for a model type are defined, they can either be external (to be obtained from the managed element) or internal (stored either in memory or the database). Some external attributes are defined as polled, meaning that SpectroSERVER polls the managed elements on a regular basis.

1.1.19 Managing of Elements

SPECTRUM is a network management system designed to notify its users if there is a fault with a particular managed element in the computing environment. One way that

SPECTRUM accomplishes this is by receiving alerts (SNMP traps) from problem areas in the managed network, and converting those alerts into events and alarms to be displayed to users on the OneClick Console. SPECTRUM uses a series of support files called event configuration files to indicate how alerts, events, and alarms should be processed.

1.1.19.1 Alerts

An alert is an unsolicited message sent from a managed element to SPECTRUM. The management protocol that SPECTRUM uses to communicate with managed elements is SNMP. An alert sent by an SNMP compliant managed element is called a trap. Managed elements with SNMP traps enabled can be configured to direct their traps to the SpectroSERVER. SpectroSERVER uses the trap's source IP address to identify the model associated with that managed element. Once the model is known, the trap is processed as directed by the AlertMap file that is associated with that model type.

1.1.19.2 Events

An event is an object representing an instantaneous occurrence within SPECTRUM. Events usually indicate that something has occurred in relation to the model or other component. When an event occurs SPECTRUM uses EventDisp files to determine how the event should be processed. There are two types of EventDisp files, global and ones that are specific for a model type. If SPECTRUM finds an EventDisp file for a specific model type it will use that file for processing the event; otherwise, it will use the global EventDisp file.

1.1.19.3 Alarms

An alarm is an object that indicates a user-actionable, abnormal condition exists in the managed environment. Usually an alarm is generated when an event has occurred, and the EventDisp file specifies that an alarm should be generated.

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

Physical Boundary

In the evaluated configuration the TOE is installed on two machines, with the TOE being administered remotely which requires the OneClick Console to be installed on a separate machine from the other components. The TOE runs on two machines (SPECTRUM Host and Client) that meet the physical hardware and software requirements as outlined in Tables 2 and 3 respectively. The physical boundary of the TOE includes the SPECTRUM Network Fault Manager r9 SP1 software as depicted in Figure 1 and is responsible for implementing the TOE's security functional requirement components.

As illustrated in Figure 1, the TOE includes the following CA SPECTRUM r9 SP1 components in the evaluated configuration:

- SpectroSERVER
- SpectroSERVER Database
- Archive Manager
- Distributed Data Manager (DDM)
- Web Server
- OneClick Console
- Report Database

The following table illustrates the minimum requirements needed to install the SPECTRUM core components on the Host machine.

Component	Windows 2003 Server SP2	Solaris 10 (Unix)
CPU	Intel x86 1.5 GHz or better (dual processor)	UltraSPARC III (dual processor)
Memory	4096MB	4096MB
Available Disk Space	2 separate	2 separate
Screen Resolution	1024x768 pixels 20-inch monitor or larger	1024x768 pixels 20-inch monitor or larger
PDF Document Viewer	Adobe Reader 5.x or later	Adobe Reader 5.x or later

Table 2 Minimum requirements for installation of SPECTRUM

The following table illustrates the minimum requirements needed to install the SPECTRUM OneClick Console component on the Client machine.

Component	Windows 2003 Server SP2	Solaris 10 (Unix)
JRE	Version 1.6.0	Version 1.6.0

Web Browser	Internet Explorer 6.0 or later	Firefox 1.5 or later

Table 3 Minimum requirements for installation of OneClick Console

Logical Boundary

The logical boundaries of the TOE are described in the terms of the security functionalities that the TOE provides to users who access the TOE to manage its users, the TOE's access control features, and the information stored by the TOE on the elements on the network which the TOE monitors.

The logical boundary of the TOE will be broken down into six security class features. The TOE provides the following security features:

2.1.1 Identification and Authentication

The TOE provides user identification and authentication through the use of user accounts and passwords for users of the TOE. Users have to identify and authenticate themselves before being allowed to access the OneClick Console. This is accomplished by the Web Server requesting and then checking the username and password of the user when they first launch the OneClick Console's GUI or the OneClick & Report Manager Web Pages. Identification and Authentication is explained in more detail in section 9.1.1.

2.1.2 Authorization

The TOE provides authorization checks before granting users the right to view or perform actions on TOE information. The TOE maintains three default user roles: Super User, Administrator, and Operator. The Super User has full privileges of the TOE, and cannot have his privileges changed by any user. The SPECTRUM Administrator and Operator roles have a specific set of privileges assigned to them. A user with the user management privileges (by default users of the Super User and Administrator roles) can provide specific users and groups with additional privileges other than those provided by the default roles. They can also create new roles with a custom set of privileges which can include a combination of privileges normally assigned to both the Administrator and Operator roles.

A user's access to the event records, through the OneClick Console and OneClick & Report Manager Web Pages interfaces, are determined by the privileges assigned to a user's roles (default or custom), any additional privileges assigned to that user, or a group to which they belong; and the security community assigned to that user or to a group in which they belong. Security communities are assigned to usernames and groups, while security strings are assigned to models. For a user to view a model's event records, the user or a group in which the user belongs must have a security community with the same value as that model's security string. Authorization is explained in more detail in section 9.1.2.

2.1.3 Security Management

The OneClick Console provides SPECTRUM users with security management capabilities. OneClick Console allows users with user management privileges to manage users and manage access control with the use of usernames, groups, and security communities. All users in the evaluated configuration will have the ability to change their own password via the OneClick Console and the OneClick & Report Manager Web Pages interfaces, because in the evaluated configuration all users will be assigned the change password privilege. Security Management is explained in more detail in section 9.1.3.

2.1.4 Security Audit

The TOE provides security auditing capabilities. The Web Server records user actions performed via the OneClick Console and the OneClick & Report Manager Web Pages interfaces. These actions are stored in the Tomcat Web Server log file or in the Distributed Data Manager (DDM) database as an event. Security Audit is explained in more detail in section 9.1.4.

TOE Security Environment

It is assumed that there will be no untrusted users or software on the SPECTRUM host and client machines. The TOE relies upon the underlying operating system and platform to provide reliable time stamps and to protect SPECTRUM's components on the host and client machines from interference or tampering. Tables 2 and 3 provide information regarding the supported operating systems for the two machines. The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE security environment requires the following security support:

- **Identification and authentication –** There are three default user roles in the evaluated configuration which are maintained by the TOE: Super User, Administrator, and Operator. Only the user with the Super User role will have direct access to the host machine with the main components of the TOE; while the client machine will be accessible to all users maintained by the TOE. Access to the TOE by users is performed over three interfaces during the setup and configuration of the TOE: SPECTRUM Control Panel (Host machine), OneClick & Report Manager Web Pages (Client machine), and OneClick Console (Client machine). However, only the OneClick Console and OneClick & Report Manager Web Pages will be used while in the evaluated configuration.

The TOE relies on the Operational Environment to provide user identification and authentication for the user with the Super User role on the SPECTRUM Host machine. The root or Windows administrator on the SPECTRUM Host machine is automatically granted full control of the SPECTRUM Control Panel. This account, therefore, has administrative control over the SPECTRUM Host machine and the features available from the SPECTRUM Control Panel. In the evaluated configuration the user with the Super User role must be the root or Windows administrator of the OS on the SPECTRUM Host machine.

On the SPECTRUM Client machine, operating system access is based on the OS user accounts, and will only give access to the OneClick Console executable and a web browser to access the OneClick & Report Manager Web Pages. Access to the TOE via this interface is provided by the TOE's identification and authentication services.

- **Partial protection of TSF** - The TOE relies on the underlying OS to provide security capabilities for the TOE's protection. The TSF relies on the host OS to prevent other applications from:
    - Interfering with an executing TSF
    - Bypassing the TOE security functions at the OS level, and
    - Modifying TSF configuration, audit data, and executable images on disk.

Reliable Time – The TOE relies on the underlying OS for reliable time. TOE functions such as audit logging rely on reliable time stamps.

3 Conformance Claims

CC Version

This ST is CC v3.1.

CC Part 2 conformant

This ST and Target of Evaluation (TOE) is Part 2 Revision 2 conformant for EAL2.

CC Part 3 conformant

This ST and Target of Evaluation (TOE) is Part 3 Revision 2 conformant for EAL2.

PP Claims

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

Package Claims

This ST claims a package for EAL2.

Package Name conformant or Package Name Augmented

This ST and Target of Evaluation (TOE) is conformant to EAL2 package claims.

Conformance Claim Rationale

There is no Conformance Claim rationale for this ST.

4 Security Problem Definition

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

Organizational Security Policies

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

Assumptions

The specific conditions listed in this section are assumed to exist in the environment in which the TOE is deployed. 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.

4.1.1 Personnel Assumptions

A.ADMIN	There will be only one user (Super User) assigned to install, and configure the TOE, while one or more users will manage the TOE and the security information it contains.

A.PATCHES The user with the Super User role will exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g. OS) so they are not susceptible to network attacks.

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

4.1.2 Logical Assumptions

A.LOCATE The network the TOE will monitor is isolated from any other network. The SNMP monitored traffic is limited to the isolated intranet, (i.e., no connections exist to other networks).

4.1.3 Physical Assumptions

A.PROTECT The TOE's software which is critical to security policy enforcement will be protected from unauthorized physical modification.

5 Security Objectives

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 users to access specified TOE information once the user has been authenticated. User authorization is based on access rights configured by the TOE users with user management privileges.

O.AUDIT The TOE will provide measures for recording security relevant events that will assist the users with the appropriate privileges 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 all users and will authenticate the claimed identity prior to granting a user access to the TOE and its information.

O.MANAGE The TOE will provide users with user management privileges with the resources to manage user accounts, information, and security information relative to the TOE.

O.ROBUST_ADMIN_GUIDANCE The TOE will provide the TOE's users with the necessary information for secure delivery, installation, management, and operation of the TOE.

Security Objectives for the operational environment of the TOE

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 user (Super User) will be assigned to install, and configure the TOE, while one or more users will manage the TOE and the security of the information it contains.

OE.FILESYS The security features offered by the underlying Operating System protect the files used by the TOE.

OE.LOCATE The TOE will be located on an isolated network with no connections to other networks.

OE.NOEVIL	Administrators of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.
OE.PROTECT	The parts of the TOE critical to security policy enforcement will be protected from unauthorized physical modification.
OE.SYSTIME	The Operational Environment will provide reliable system time.
OE.AUDIT	The Operational Environment will provide local access control, storage, and the ability to read to the audit logs which are stored on the machine where the TOE is installed.
OE.TRUSTED_CHANNEL	The Operational Environment shall ensure that data sent between the TOE and users is protected from unauthorized disclosure and modification.
OE.TRUSTED_PATH	The Operational Environment shall maintain a trusted path for user identification and authentication.

6 Extended Requirements

Extended Security Functional Requirements

There are no extended Security Functional Requirements in this ST.

Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

7 Security Functional Requirements

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

Security Function	Security Functional Components
Security Audit	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAR.1 Audit review
User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
Identification and Authentication	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_MSA.1 Management of security attributes
	FMT_MSA.2 Secure security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1(1) Management of TSF data
	FMT_MTD.1(2) Management of TSF data
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

Table 4 Functional Components

7.1.1 Class FAU: Security Audit

7.1.1.1 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. [**All auditable events specified in Table 5.**]*

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, 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, ***[the information specified in the third column of Table 5]***.

Dependencies: *FPT_STM.1 Reliable time stamps*

Application Note: *The TOE meets the requirements of bullet 'a' by recording the following: the date and time at which the page of GUI was accessed (date and time of the event), the name of the operation that was performed (type of event), the user account name (subject identity), and the return code (outcome (success or failure) of the event).*

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	
FAU_GEN.2	None	
FAU_SAR.1	None	
FDP_ACC.1	Decision to permit/deny access to an operation on an object	The identity of the individual user which tried to perform the operation on the object. The Hostname and/or IP address of the Remote Workstation from which the action was performed.
FDP_ACF.1	Decision to permit/deny access to an operation on an object	The identity of the individual user which tried to perform the operation on the object. The Hostname and/or IP address of the Remote Workstation from which the operation was performed.
FIA_ATD.1	None	
FIA_UAU.2	None	Claimed identity of the user using the identification mechanism. The Hostname and/or IP address of the Remote Workstation from which the operation was performed.
FIA_UID.2	All use of the user identification mechanism used for authorized users (that is, those that authenticate to the	Claimed identity of the user using the identification mechanism. The Hostname and/or IP address of the

Requirement	Auditable Events	Additional Audit Record Contents
	TOE)	Remote Workstation from which the operation was performed.
FMT_MSA.1	All manipulation of the security attributes	The identity of the Super User or Administrator performing the function. The Hostname and/or IP address of the Remote Workstation from which the operation was performed.
FMT_MSA.2	None	
FMT_MSA.3	None	
FMT_MTD.1(1)	All manipulation of the security attributes	The identity of the Super User or Administrator performing the function. The Hostname and/or IP address of the Remote Workstation from which the operation was performed
FMT_MTD.1(2)	All manipulation of a user's password	The identity of that specific user, the Super User or Administrator performing the function. The Hostname and/or IP address of the Remote Workstation from which the operation was performed.
FMT_SMF.1	All manipulation of users and their attributes All manipulation of groups All manipulation of objects and object attributes (security communities)	The identity of the Super User or Administrator performing the function. The Hostname and/or IP address of the Remote Workstation from which the operation was performed.
FMT_SMR.1	None	

Table 5 Auditable Events

7.1.1.2 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*

7.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: *No other components.*

FAU_SAR.1.1 The TSF shall provide *[a **user with the appropriate privileges assigned**]* with the capability to read *[**Hostname and/or IP address of the Remote Workstation from which the action was completed, the user's account name responsible for the record's creation, date and time at which the action was performed, name of the operation that was performed, and the success or failure of the operation**]* 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*

7.1.2 Class FDP: User Data Protection

7.1.2.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the ***[SPECTRUM Discretionary Access Control (DAC) Policy]*** on ***[subjects: processes acting on the behalf of users, objects: event records and all operations among subjects and objects covered by the SPECTRUM DAC Policy]***

Dependencies: *FDP_ACF.1 Security attribute based access control*

Application Note: *The SPECTRUM DAC Policy is based upon assigning privileges for an operation and/or a role of bundled privileges to a specific username, or to a group in which the user belongs; and the assignment of security communities to a specific username, or to a group in which the user belongs. In addition to the privileges assigned to a specific user, the user also gains the privileges of their assigned roles, and any groups in which they belong. The privileges associated to a user from these three sources define how the SPECTRUM DAC Policy affects their operations on the event records. Security strings are assigned to models and are associated to the event records (objects) for those models. For a user to access an event record for a particular model, their username or a group in which they belong must be assigned a security community with the same value as the model's security string. See Section 9.1.2.1 for more information.*

Application Note: *The SPECTRUM DAC Policy does not require a user to be assigned to one of the default roles. These roles represent a default set of privileges which have been bundled together for the default operation of the TOE. The roles are merely a method to allow for easier user management capabilities through the ability to assign roles to users instead of individual privileges. Therefore, roles are not a security attribute for users in determining access control. See Section 9.1.2.2 for more information.*

7.1.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: *No other components.*

FDP_ACF.1.1 The TSF shall enforce the ***[SPECTRUM Discretionary Access Control (DAC) Policy]*** to objects based on the following: ***[Username, Group, Security Communities]***.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[A process acting on behalf of a user is granted access to perform an operation on an object, by association of the operation to their username or a group in which they belong; and by comparing the security string assigned to the object and the security community assigned to their username or a group in which they belong.]***.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***[The Super User has full control with no exceptions]***

FDP_ACF.1.4 TSF shall explicitly deny access of subjects to objects based on the ***[none]***.

Dependencies: *FDP_ACC.1 Subset access control and FMT_MSA.3 Static attribute initialization.*

Application Note: *The SPECTRUM DAC Policy is based upon assigning privileges for an operation and/or a role of bundled privileges to a specific username, or to a group in which the user belongs; and the assignment of security communities to a specific username, or to a group in which the user belongs. In addition to the privileges assigned to a specific user, the user also gains the privileges of their assigned roles, and any groups in which they belong. The privileges associated to a user from these three sources define how the SPECTRUM DAC Policy affects their operations on the event records. Security strings are assigned to models and are associated to the event records (objects) for those models. For a user to access an event record for a particular model, their username or a group in which they belong must be assigned a security community with the same value as that model's security string. See Section 9.1.2.1 for more information.*

Application Note: *The SPECTRUM DAC Policy does not require a user to be assigned to one of the default roles. These roles represent a default set of privileges which have been bundled together for the default operation of the TOE. The roles are merely a method to allow for easier user management capabilities through the ability to assign roles to users instead of individual privileges. Therefore, roles are not a security attribute for users in determining access control. See Section 9.1.2.2 for more information.*

7.1.3 Class FIA: Identification and Authentication

7.1.3.1 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, security communities, group]***

Dependencies: *No dependencies*

Application Note: *Roles and individual privileges have not been listed as security attributes for individual users. This is because these access control attributes are associated with usernames and groupnames and do not have to be assigned to an individual user. When the TOE performs access control, it is their username or groupname which is checked to determine if they are granted or denied access to an object.*

7.1.3.2 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*

7.1.3.3 FIA_UID.2 User identification before any action

Hierarchical to: *FIA_UID.1 Timing of identification*

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*

7.1.4 Class FMT: Security Management

7.1.4.1 FMT_MSA.1 Management of security attributes

Hierarchical to: *No other components.*

FMT_MSA.1.1 The TSF shall enforce the ***[SPECTRUM Discretionary Access Control (DAC) Policy]*** to restrict the ability to [***modify***] the security attributes ***[used for access control]*** to ***[users with the Super User or Administrator role assigned to their username or to a group in which they belong]***

.

Dependencies: *[FDP_ACC.1 Subset access control]*
FMT_SMR.1 Security roles,
FMT_SMF.1 Specification of Management Functions

Application note: *This SFR only lists the Super User and Administrator roles because this is the TOE's default means to control access to this ability. In addition, the TOE also allows administrators to create custom roles which can have user management privileges. These custom roles and the individual user management privileges can be assigned to usernames or to groups. A user with a username or a group in which they belong that has been assigned the user management privileges directly or through a role, can also manage user security attributes.*

7.1.4.2 FMT_MSA.2 Secure security attributes

Hierarchical to: *No other components.*

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [***username, security communities, group, security strings***].

Dependencies: *[FDP_ACC.1 Subset access control]*
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

7.1.4.3 FMT_MSA.3 Static attribute initialization

Hierarchical to: *No other components.*

FMT_MSA.3.1 The TSF shall enforce the ***[SPECTRUM Discretionary Access Control (DAC) 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 ***[users with the Super User or Administrator role assigned to their username or a group in which they belong]*** 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*

Application note: *This SFR is included to capture the management of security attributes which relate to access control.*

Application note: *This SFR only lists the Super User and Administrator roles because this is the TOE's default means to control access to this ability. In addition, the TOE also allows administrators to create custom roles which can have user management privileges. These custom roles and the individual user management privileges can be assigned to usernames or to groups. A user with a username or a group in which they belong that has been assigned the user management privileges directly or through a role, can also manage user security attributes.*

7.1.4.4 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 ***[view, create,*** *modify, delete]* the ***[security attributes]*** to ***[users with the Super User or Administrator role assigned to their username or a group in which they belong]***.

Dependencies: *FMT_SMR.1 Security roles*
FMT_SMF.1 Specification of Management Functions

Application note: *This SFR only lists the Super User and Administrator roles because this is the TOE's default means to control access to this ability. In addition, the TOE also allows administrators to create custom roles which can have user management privileges. These custom roles and the individual user management privileges can be assigned to usernames or to groups. A user with a username or a group in which they belong that has been assigned the user management privileges directly or through a role, can also manage user security attributes.*

Application note: *Security attributes include user security attributes listed under FIA_ATD.1.1, as well as, object attributes such as security strings.*

7.1.4.5 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 *[**change**]* the *[**password of a specific user**]* to *[**that specific user, users with the Super User or Administrator role assigned to their username or a group in which they belong**]*.

Dependencies: *FMT_SMR.1 Security roles*
FMT_SMF.1 Specification of Management Functions

Application note: *This SFR only lists the Super User and Administrator roles because this is the TOE's default means to control access to this ability. In addition, the TOE also allows administrators to create custom roles which can have user management privileges. These custom roles and the individual user management privileges can be assigned to usernames or to groups. A user with a username or a group in which they belong that has been assigned the user management privileges directly or through a role, can also manage user security attributes.*

7.1.4.6 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 management functions: *[*

1. ***View, Create, Modify, and Delete Users and User Attributes (including passwords)***
2. ***View, Create, Modify, and Delete Groups and Group Attributes***
3. ***View, and Modify Objects and Object Attributes (Security Strings)]***

Dependencies: *No dependencies*

Application note: *The reference to objects in this SFR refers the TOE data which represents the network elements which the TOE monitors.*

7.1.4.7 FMT_SMR.1 Security roles

Hierarchical to: *No other components.*

FMT_SMR.1.1 The TSF shall maintain the roles ***[Super User, Administrator, Operator]***.

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

Dependencies: *FIA_UID.1 Timing of identification*

Application note: *The TOE maintains three default roles: Super User, Administrator, and Operator. It is also possible for additional roles to be created and managed by users with user management privileges; the TSF will also maintain these custom roles.*

Application Note: *The SPECTRUM DAC Policy does not require a user to be assigned to one of the default roles. These roles represent a default set of privileges which have been bundled together for the default operation of the TOE. The roles are merely a method to allow for easier user management capabilities through the ability to assign roles to users instead of individual privileges. Therefore, roles are not a security attribute for users in determining access control. See Section 9.1.2.2 for more information.*

Proper dependencies

All dependencies for the security functional requirements were pulled from CC Part 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. Font style and clarifying information conventions were developed to aid the reader.

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

7.1.5 Assignments made

Assignments allow the specification of parameters and are specified by the ST author in ***[italicized bold text].***

7.1.6 Iterations made

Iterations allow a component to be used more than once with varying operations and are specified by the ST author by placing the iteration number in round brackets “(1)”. These follow the short family name and allow components to be used more than once with varying operations. An asterisk “*” refers to all iterations of a component.

7.1.7 Selections made

Selections allow the specification of one or more items from a list and are specified by the ST author in ***[italicized text].***

7.1.8 Refinements made

Refinements allow the addition of details and are specified by the ST author with "Refinement:" right after the short name. Additions to the CC text are specified in **italicized bold and underlined text.**

8 Security Assurance Requirements

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

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 untrusted 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 initialisation 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 Security-Enforcing Functional Specification (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 each SFR-enforcing TSFI, 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 Basic 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 behaviour of each SFR non-interfering subsystem of the TSF in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4C	The design shall summarise the SFR-enforcing behaviour 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 behaviour 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.

Guidance Documents

8.1.4 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.

8.1.5 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.

Life Cycle Support

8.1.6 Use of a CM System (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 labelled 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.

8.1.7 Parts of the TOE CM Coverage (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.

8.1.8 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.

Security Target Evaluation

8.1.9 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.

8.1.10 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.

8.1.11 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.

8.1.12 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.

8.1.13 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.2.9C 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.

8.1.14 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.

8.1.15 TOE Summary Specification (ASE_TSS.1)

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

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

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

Tests

8.1.16 Evidence 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.

8.1.17 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.

8.1.18 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.

Vulnerability Assessment

8.1.19 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, 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

TOE Security Functions

This section describes the security functions provided by the TOE.

Note: The remote user interfaces described in Section 9.1 are encrypted by SPECTRUM; however, the encryption of these interfaces have not been included as part of the TOE. 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.

9.1.1 Identification and Authentication

The TOE provides user identification and authentication through the use of user accounts and passwords for users of the TOE. In the evaluated configuration, all users will access the TOE via the OneClick Console or the OneClick & Report Manager Web Pages on the SPECTRUM Client machine. After launching the OneClick Console or accessing the OneClick & Report Manager Web Pages, the TOE requires the user to submit their username and password. The user's username and password will then be used to identify and authenticate the user against the stored authentication information located in the SpectroSERVER Database. The verification of the user's authentication information is accomplished by the Web Server component and is required before a user is allowed to perform any other actions on the TOE.

9.1.2 Authorization

The SPECTRUM Discretionary Access Control (DAC) Policy is what determines access control for the TOE over the OneClick Console and the OneClick & Report Manager Web Pages interfaces. This policy relies on the TOE's ability to maintain a set of three security attributes, and to allow for users with user management privileges to manage the security attributes for users. The security attributes used by the policy are username, groups, and security communities. For more information regarding these attributes refer to Section 9.1.3.1 Management of Security Attributes.

9.1.2.1 SPECTRUM DAC Policy

The SPECTRUM DAC Policy provides access control of users over the OneClick Console and the OneClick & Report Manager Web Pages interfaces. Starting immediately after the identification and authentication process, the Web Server performs authorization processes to determine what information will be provided to that individual user. In addition, the OneClick Console GUI will appear differently to users with different privileges based on the SPECTRUM DAC Policy which determines the information they are authorized to view and manage.

The Web Server will use the user supplied username during authentication to determine access control. The username is used by the Web Server to determine the roles and individual privileges which have been assigned to that individual user. The username is also used to find the group in which the user belongs. Once the Web Server has the group-names for the groups the user belongs to, it then finds the roles and individual privileges which have been assigned to those group-names. The Web Server then uses all the roles and individual privileges, which were assigned to the user's username and their groups' group-names, to determine what operations the user is allowed to perform. This decision is used by the Web Server to determine how the OneClick Console GUI will appear to an individual user; only the tabs, frames, fields and buttons that control the operation processes which the user can perform are presented to the user.

Access to the information within the tabs and frames is controlled by both the Web Server and the OneClick Console. In the evaluated configuration, the objects that the TOE controls access to are the models and their event records. Event records are stored in the Distributed Data Manager (DDM) database, and are records of events that occurred on the elements in SPECTRUM's monitored network. When a user requests access to a particular model or its event records, the Web Server makes a decision on if that user has access to that particular model and its event records. This is accomplished through the assignment of security communities to users and groups, while assigning security strings to models. For a user to be granted access to a particular model and its event records the security string assigned to the model must match a security community assigned to that user's username or to the group-name of a group to which the user belongs. By default ADMIN is the security community assigned to all users and groups, and the security string assigned to models. The ADMIN security community allows users to have access to all models regardless of a model's security string. To limit user access, a user with user management privileges must change the ADMIN security community for the individual users and their groups. Then the user with user management privileges must assign a security string to the models associated with the event records to which they are granting those users and groups access. However, if a user with user management privileges does not set a security string for a model, then the TOE will grant access to the model's event records without performing this authorization check.

9.1.2.2 Roles and Individual Privileges

The TOE maintains three default user roles for the SPECTRUM DAC Policy: Super User, Administrator, and Operator. The SPECTRUM DAC Policy utilizes roles as a bundled set of privileges which can be assigned to a user or to a group. The Super User has full privileges of the TOE, and cannot have his privileges changed by any user. The Administrator and Operator roles have a specific set of privileges assigned to them. Also, both the Administrator and Operator roles have read only and read/write privileges. In the evaluated configuration, the main difference between these two roles is that the Administrator role has user management privileges.

The SPECTRUM DAC Policy does not require a user to be assigned to one of the default roles, since a user can be assigned privileges individually, or belong to a group which has been assigned a role or privileges individually. These roles represent a default set of privileges which have been bundled together for the default operation of the TOE. The roles are merely a method to allow for easier user management capabilities through the ability to assign roles to users instead of individual privileges. Therefore, roles are not a security attribute for users in determining access control.

In the evaluated configuration all new users will be assigned both the Administrator and Operator roles during their creation and the user's assignment to these roles can be modified after initial creation on a user by user basis. The ability to modify a user's role and assign individual privileges to a user can be done by any user with user management privileges. In addition to being assigned individual privileges and default roles, a user or group can also be assigned a custom role. Custom roles are also created by users with user management privileges, and can include privileges which would normally be found in both the Administrator and Operator roles. It is also possible for a user or group to be assigned multiple roles and/or individual privileges at the same time.

9.1.3 Security Management

9.1.3.1 Management of Security Attributes

The TOE's access control functions rely on the ability of the TOE and its users, with user management privileges, to be able to manage the security attributes assigned to its users. The TOE's default roles which have been assigned user management privileges are the Super User and Administrator roles; however, these privileges can be assigned individually or new custom roles can be created as well. Therefore, any user with a username or a group in which they belong that has been assigned the user management privileges, through any of the above means, can manage the security attributes of the TOE's users. Through the SPECTRUM DAC Policy, the TOE ensures that default values are assigned to the security attributes during user creation, and ensures that only secure values are assigned while the security attributes are being maintained by a user with user management privileges. Table 6 below lists the three security attributes for users which are maintained by the TOE, includes a brief description of each attribute, and their default value.

Security Attribute	Description	Default Value
Username	A uniquely named character string assigned to an individual user upon creation of their account.	Assigned. Users must be assigned a unique username during creation.
Groups	A list of unique group-names that represent the groups to which the individual user belongs.	None. Users will not be assigned groups upon creation.
Security Community	A character string which is assigned to each individual user. It is checked against a model's security string in the event	ADMIN

	records, if they match then the user gains access. When assigned to a username or group the ADMIN security community allows unrestricted access. A user and group can be assigned multiple security communities.	

Table 6 Security Attributes

9.1.3.2 Management of TSF Data

The OneClick Console provides its users an interface into the TOE to perform functions on the TOE and its information. The OneClick Console is made up one main frame which includes standard toolbars and contains three sub-frames: Navigation, Contents, and Component Detail. Within these sub-frames the OneClick Console lists the information that the user requests. This information can be requested through the use of the tabs, fields, and button located within each frame.

9.1.3.2.1 User Creation and Management

The TOE's OneClick Console component allows a user with user management privileges, such as a user with the Super User or Administrator roles, to manage users and their attributes including their three security attributes and passwords. When a user with user management privileges wants to view, create, modify, or delete a user and their attributes, they must select the Users tab of the Navigation frame. This will populate the Navigation and Content frames with a list of current TOE users and populates the Component Detail frame with the user's attributes.

A new user can be created by clicking the Create a New User button, once clicked there is a popup window where the new user's username must be assigned a new unique value and must be assigned a password to be create. At this point the user can also be assigned a different security community other than the default ADMIN and be assigned to the Administrator and/or Operator roles, which can be changed at a later time. In the evaluated configuration all new users will be assigned both roles at this time, and their assignment to these roles can be modified after initial creation on a user by user basis. After a user is created the user can be viewed, deleted, or have any of their attributes (including security attributes and password) modified other than their username through the use of the three frames of OneClick Console. In the evaluated configuration, the TOE's ability to restrict access to the management of users and their attributes will be limited to a user's security attributes and password.

All users have the ability to change their own passwords in the evaluated configuration, since all users, other than the user in the Super User role, will be assigned the change password privilege. This can be given through the assignment of the Operator role, the change password privilege, or a custom role with the change password privilege to the user's username or a group in which the user belongs. A user can perform a self password change by logging into the OneClick Console, and clicking the change password link in the bottom toolbar of the main frame. Once clicked there is a popup window which requests the old password, the new password, and a confirmation of the new password. A user can also change their password from the OneClick & Report Manager Web Pages in the same manner as described via the OneClick Console; the only difference is that the action is performed via a popup window in the user's web browser. Once the user submits the password change request, and the old password is verified and the new password is confirmed by the TOE, the user's password is updated.

9.1.3.2.2 Group Creation and Management

The TOE's OneClick Console component allows a user with user management privileges, such as a user with the Super User or Administrator roles, to manage groups and their attributes. When a user with user management privileges wants to view, create, modify, or delete a group and their attributes, they must select the Users tab of the Navigation frame. This will populate the Navigation frame with a list of current TOE groups. When one of the current TOE groups is selected in the Navigation frame, the Contents frame will provide a list of users in the group, and the Component Detail frame will provide the group's attributes.

A new group can be created by clicking the Create a New Group button, once clicked there is a popup window where the new group's group-name must be assigned a new unique value. At this point the group can also be assigned a different security community other than the default ADMIN and be assigned to the Administrator and/or Operator roles, which can be changed at a later time. In the evaluated configuration all new groups will be assigned both roles at this time, and their assignment to these roles can be modified after initial creation on a group by group basis. After a group is created the group can be viewed, deleted, or have any of their attributes modified other than their group-name through the use of the three frames of OneClick Console. In the evaluated configuration, the TOE's ability to restrict access to the management of groups and their attributes will not be evaluated.

9.1.3.2.3 Modify Model Security Strings

The TOE's OneClick Console component allows a user with model management privileges, such as a user with the Super User or Administrator roles, to view and modify models and their attributes (security string). When a user with model management privileges wants to view, or modify a model and their attributes, they can navigate to the model in many ways. One method would be through the Explorer tab on the Navigation frame. This will populate the Navigation frame with a list of TOE configuration items, including the Universe which contains models. When one of the models is selected in the Navigation frame, the Contents frame and Component Detail frames will provide several tabs of information. Now to change an attribute, such as a model's security string, in the Component Detail frame the information tab can be selected and under SPECTRUM Modeling Information the model's attributes can be modified. In the evaluated configuration, the TOE's ability to restrict access to the management of model's and their attributes (security string) will not be evaluated.

9.1.4 Security Audit

The TOE provides security auditing capabilities via the Web Server and the SpectroSERVER components. The auditing of authentication and the initial authorization of users is performed by the Web Server, as well as, the auditing of start-up and shutdown of the audit functions. The auditing of any actions which occur after the initial authorization, are recorded by the SpectroSERVER as an event because the action results in a change of the affected model's information. Auditing allows a user with the appropriate privileges the ability to track user activity over the OneClick Console and the OneClick & Report Manager Web Pages interfaces. At a minimum, the audit record for a process acting on behalf of a user's action on the TOE will store: the date and time the record was created, the remote workstation's hostname and/or IP address from which the action was completed, the user's account name responsible for the record's creation, the operation that was performed, and the success or failure of the operation. Based on the content of these logs, the TOE is able to associate the event with the user that caused the event.

The audit records for authentication and initial authorization of users are stored in the Web Server's Tomcat audit logs which are located in the Operational Environment. These logs are viewed by a user via the OneClick & Report Manager Web Pages interface; which requires that the user to have the appropriate privileges assigned to their username or to a group in which they belong to view these logs. The audit records for the start-up and shutdown of the TOE's audit functions are stored in the respective OS's syslog file. The TOE relies on the Operational Environment to protect these audit records from unauthorized access, modification and/or deletion to the records in the audit logs. For the Super User to view the syslog logs, they must authenticate to the SPECTRUM Host machine's OS which the Web Server component is installed on and access the audit log files with an equal or higher level of permissions than those used when the Super User installed SPECTRUM. Finally, the audit records for all other authorizations of users are stored in the DDM as events, and are accessed by the Archive Manager. These files are viewed as events by users via the OneClick Console; which requires that the user to have the appropriate privileges assigned to their username or to a group in which they belong. The appropriate privileges include having either the ADMIN security community or the security community which matches the security string of the event's model.

For all audit logs, TOE's auditing capabilities also rely on the SPECTRUM Host machine's underlying operating system to provide reliable time stamps.

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_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAR.1 Audit review
User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
Identification and Authentication	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_MSA.1 Management of security attributes
	FMT_MSA.2 Secure security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1(1) Management of TSF data
	FMT_MTD.1(2) Management of TSF data

Security Function	Security Functional Components
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

Table 7 Security Functional Components

Note: The remote user interfaces described in Section 9.2 are encrypted by SPECTRUM; however, the encryption of these interfaces have not been included as part of the TOE. 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.

9.1.5 Security Audit

The security audit function of the TOE enforces the FAU_GEN.1, FAU_GEN.2, and FAU_SAR.1 requirements.

In the evaluated configuration for Windows, and Solaris (UNIX), each operating system's respective syslog file stores the record of the startup and shutdown of the TOE's audit functions. The TOE also provides user auditing capabilities through its use of the Tomcat web server, which is part of the SPECTRUM Web Server component, and the SpectroSERVER's creation of events on models. The audit logs include the records of processes acting on behalf of a user's activity over the OneClick Console and the OneClick & Report Manager Web Pages interfaces. The minimum contents of each record in the audit log include the following: Date and time of the record's creation, the hostname and/or IP address of the remote workstation from which the action was completed, the user's account name responsible for the record's creation, name of the operation performed, and the success or failure of the operation. The audit logs on user authentication and initial authorization located in the Tomcat's log file are viewed via the OneClick & Report Manager Web Pages interface. The audit logs on all other user authorizations are viewed as events via the OneClick Console. Whereas, the syslog files are viewed by the Super User in the form of the OS's predefined syslog file.

9.1.6 User Data Protection

The User Data Protection function of the TOE enforces the FDP_ACC.1, and FDP_ACF.1 requirements.

When a user attempts to access the TOE's information via the OneClick Console or OneClick & Report Manager Web Pages, the user's access is determined by the user's security attributes. The SPECTRUM DAC Policy uses individual privileges and roles assigned to a user's username and their groups to determine what operations can be perform on objects via the OneClick Console and the OneClick & Report Manager Web Pages interfaces. This policy also uses security communities to determine which event records a user can access. This is accomplished by checking the security communities associated with the user and the groups in which they belong against the security string of the event record's model; if they match then access is granted. The SPECTRUM DAC policy grants access to an operation on an object if their security attributes meet the requirements for that operation and that object, and the policy does not explicitly deny access to users. Also, only the Super User has unrestricted access to the TOE's functions over these interfaces.

9.1.7 Identification and Authentication

The identification and authentication function of the TOE enforces the FIA_ATD.1, FIA_UAU.2, and FIA_UID.2 requirements.

The TOE provides user identification, and authentication through the use of checking the usernames and passwords of users. Users have to identify and authenticate themselves before being allowed access to any other actions on the TOE via the OneClick Console and the OneClick & Report Manager Web Pages interfaces. During authentication, the Web Server requests the user for their username and password, which it checks against the authentication information stored in the SpectroSERVER Database. If the username and password submitted during authentication matches the username and password in the database, the user is granted access to the TOE; otherwise, access is denied.

9.1.8 Security Management

The security management function of the TOE enforces the FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_SMF.1, and FMT_SMR.1 requirements.

The TOE provides management capabilities through the OneClick Console and the OneClick & Report Manager Web Pages (only self password changes) interfaces. The TSF shall provide the ability to manage users, groups, models and their attributes. In the evaluated configuration, the TOE's ability to restrict access to these management abilities will only be to the management of a user's security attributes and their password. The SPECTRUM DAC Policy ensures that only users with user management privileges, such as a user with the Super User or Administrator roles, have the ability to change a user's security attributes' restrictive default values provided by the TOE, and that all attribute values accepted through the management of the user are secure. The SPECTRUM DAC Policy also ensures that all users can manage their own passwords, and users with user management privileges have the ability to manage other user's passwords.

The TOE maintains three default roles: Super User, Administrator, and Operator. These roles represent a default set of privileges which have been bundled together for the default operation of the TOE. The default roles are merely a method to allow for easier user management capabilities through the ability to assign roles to users instead of individual privileges. It is also possible for additional roles to be created and managed by users with user management privileges; the TSF will also maintain these custom roles. The SPECTRUM DAC Policy does not require a user to be assigned to one of the default roles or a custom role. Therefore, roles are not a security attribute for users in determining access control.

10 Rationale

Security Objectives Rationale

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

Assumption	Objective	Rationale
A. ADMIN There will be only one user (Super User) assigned to install, and configure the TOE, while one or more users will manage the TOE and the security information it contains.	OE.ADMIN One user (Super User) will be assigned to install, and configure the TOE, while one or more users will manage the TOE and the security of the information it contains.	OE.ADMIN maps to A. ADMIN in order to ensure that only the user with the Super User role will install, and configure the TOE to bring it into the evaluated configuration. During operation the user with the Super User role, and any other user with the necessary security attributes assigned to them will be able to manage the TOE in a manner that maintains its security objectives.
A.PATCHES The user with the Super User role will exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g. OS) so they are not susceptible to network attacks.	OE.ADMIN One user (Super User) will be assigned to install, and configure the TOE, while one or more users will manage the TOE and the security of the information it contains.	OE.ADMIN maps to A. PATCHES in order to ensure that the user with the Super User role properly patches the TOE and the Operational Environment in a manner that maintains their security objectives.
A.NOEVIL Administrators 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 Administrators 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 administrators 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 will monitor is isolated from any other network. The SNMP monitored traffic is limited to the isolated intranet, (i.e.,	OE.LOCATE The TOE will be located on an isolated network with no connections to other networks.	OE.LOCATE directly maps to A.LOCATE to ensure that the monitored network is isolated and safe from interference by other networks.

no connections exist to other networks).		
A.PROTECT The TOE's software which is 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.

Table 8 Assumption to Objective Mapping

Threat	Objective	Rationale
T.ACCESS A legitimate user of the TOE could gain unauthorized access to information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	O.ACCESS The TOE will provide measures to authorize users to access specified TOE information once the user has been authenticated. User authorization is based on access rights configured by the TOE users with user management privileges.	O.ACCESS (FDP_ACC.1, FDP_ACF.1) addresses T.ACCESS by providing the users with user management privileges with the capability to specify access restrictions on the protected TOE information to users which meet the access control restrictions for the operation and object.
	OE.TRUSTED_CHANNEL The Operational Environment shall ensure that data sent between the TOE and users is protected from unauthorized disclosure and modification.	OE.TRUSTED_CHANNEL addresses T.MASK by providing a trusted channel between users and the TOE to protect the data sent between the two entities from being read during transit.
	OE.FILESYS The security features offered by the underlying Operating System protect the files used by the TOE.	OE.FILESYS addresses T.ACCESS by ensuring that the underlying Operating System provides the capability to store and protect the files

Threat	Objective	Rationale
		used by the TOE.
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 the TOE's users with the necessary information for secure delivery, installation, management, and operation of 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 The TOE will provide users with user management privileges with the resources to manage user accounts, information, and security information relative to the TOE.	O.MANAGE (FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1) addresses T.ADMIN_ERROR by ensuring only users with user management privileges can use the provided resources to manage user accounts, information, and 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	O.AUDIT The TOE will provide measures for recording security relevant events that will assist the users with the appropriate privileges in detecting	O.AUDIT (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1) addresses T.MASK by providing the users with the appropriate privileges with the tools

Threat	Objective	Rationale
authentication countermeasures.	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.	necessary to monitor user activity to ensure that misuse of the TOE does not occur.
	OE.SYSTIME The Operational Environment will provide reliable system time.	OE.SYSTIME addresses this threat by providing an audit mechanism in the underlying Operating System includes the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.
	OE.AUDIT The Operational Environment will provide local access control, storage, and the ability to read to the audit logs which are stored on the machine where the TOE is installed.	OE.AUDIT addresses this threat by providing the TOE with OS's ability to store and protection the audit log files from local access, and providing the Super User with the ability to read the audit logs through the OS's auditing services.
	O.IDEN The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE and its information.	O.IDEN addresses T.MASK by providing measures to uniquely identify and authenticate users through successful login to the Web Server component.
	OE.TRUSTED_PATH The Operational Environment shall maintain a trusted path for user identification and authentication.	OE.TRUSTED_PATH addresses T.MASK by providing a trusted path between users and the TOE to protect their identification and authentication information from being read during transit.
T.MODIFY Users, whether they be	O.MANAGE The TOE will provide users with user	O.MANAGE addresses T.MODIFY by ensuring

Threat	Objective	Rationale
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.	management privileges with the resources to manage user accounts, information, and security information relative to the TOE.	that only users with user management privileges can use the provided resources for managing and monitoring user accounts, TOE information and security information relative to the TOE.

Table 9 Threat to Objective Mapping

Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the security functional requirement components that address the stated TOE objectives.

Objective	Security Functional Components	Rationale
O.ACCESS The TOE will provide measures to authorize users to access specified TOE information once the user has been authenticated. User authorization is based on access rights configured by the TOE users with user management privileges.	FDP_ACC.1 Subset access control	FDP_ACC.1 states the TSF shall enforce the SPECTRUM DAC Policy when authorizing user access to TOE information (models and event records).
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 states the TSF shall enforce the SPECTRUM DAC Policy to TOE information based on username, groups, and security communities, and requires users with user management privileges to configure user access rights.
O.AUDIT The TOE will provide measures for recording security relevant events that will assist the users with appropriate privileges in detecting misuse of the TOE and/or its security features that would	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.
	FAU_GEN.2 User identity association	FAU_GEN.2 states the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Objective	Security Functional Components	Rationale
compromise the integrity of the TOE and violate the security objectives of the TOE.	FAU_SAR.1 Audit Review	FAU_SAR.1 requires that the TOE provide audit records in a manner that is suitable for interpretation by users with the appropriate privileges assigned.
O.IDEN The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE and its information.	FIA_ATD.1 User attribute definition	FIA_ATD.1 ensures that users have a defined set of tasks that they can perform based on their access permissions defined by users with user management privileges.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires a user be authenticated before any access to the TOE and information 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 its information is allowed.
O.MANAGE The TOE will provide users with user management privileges with the resources to manage user accounts, information, and security information relative to the TOE.	FMT_MSA.1 Management of security attributes	FMT_MSA.1 states the TSF shall enforce the SPECTRUM DAC Policy to restrict the ability to modify security attributes used for access control to users with user management privileges assigned to their username or to a group in which they belong.
	FMT_MSA.2 Secure security attributes	FMT_MSA.2 states the TSF shall ensure that only secure values are accepted.

Objective	Security Functional Components	Rationale
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 states the TSF shall enforce the SPECTRUM DAC Policy to provide restrictive default values for security attributes that are used to enforce the SFP. It allows the users with user management privileges to override the default values set for security attributes when creating user accounts.
	FMT_MTD.1(1) Management of TSF data	FMT_MTD.1(1) states the TSF shall restrict the ability to view or change user security attributes to users which have been assigned the appropriate roles or user management privileges.
	FMT_MTD.1(2) Management of TSF data	FMT_MTD.1(2) states the TSF shall restrict the ability to change a user's password to that user or other users which have been assigned the appropriate roles or user management privileges.
	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, groups, objects, and each security function's attributes.
	FMT_SMR.1 Security Roles	FMT_SMR.1 requires the TOE to provide the ability to maintain the roles Super User, Administrator, and Operator. Users with the Super User and Administrator roles are by default granted the user management privileges.
O.ROBUST_ADMIN_GUIDANCE The TOE will provide the TOE's users with the	ALC_DEL.1 Delivery Procedures	ALC_DEL.1 describes product delivery and a description of all procedures used to ensure objectives are not

Objective	Security Functional Components	Rationale
necessary information for secure delivery, installation, management, and operation of the TOE.		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 for the TOE's management and operation.

Table 10 Security Functional Requirements Rationale

Extended Requirements Rationale

There are no extended Security Functional Requirements, nor extended Security Assurance Requirements in this ST.

Requirement Dependency Rationale

All Security Functional Requirement component dependencies have been met by the TOE with the exception of FPT_STM.1 and FMT_SMR.1.

FPT_STM.1, Reliable Time Stamps is a dependency of FAU_GEN.1. This dependency 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_SMR.1, Security Roles is a dependency of FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1(1), and FMT_MTD.1(2). The FMT_SMR.1 requirement has been included in the ST; however, the intention of these dependencies is based on the use of roles for access control, which has not been met. This is because the TOE's access control policy is based on discretionary access control and not role based access control. Since the TOE still maintains roles this SFR has been included, but the use of roles is merely a method to allow for easier user management capabilities, through the ability to assign roles to users instead of individual privileges. Therefore, roles are not a security attribute for users in determining access control.

Assurance Measures

This section identifies the assurance measures provided by the developer in order to meet the security assurance requirement components for EAL2. A description of each of the TOE assurance measures follows in Table 11.

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Description	TOE Design Specification Document for CA SPECTRUM® Network Fault Manager r9 SP1 version 0.4	This document describes the security architecture of the TOE.
ADV_FSP.2 Security-Enforcing Functional Specification	Functional Specification Document for CA SPECTRUM® Network Fault Manager r9 SP1 version 0.3	This document describes the functional specification of the TOE with complete summary.
ADV_TDS.2 Basic Design	TOE Design Specification Document for CA SPECTRUM® Network Fault Manager r9 SP1 version 0.4	This document describes the architectural design of the TOE.
AGD_OPE.1 Operational User Guidance	SPECTRUM OneClick Console User Guide [5130] r9.0 SPECTRUM OneClick Administration Guide [5166] r9.0	This document describes the operational user guidance for CA SPECTRUM r9 SP1.
AGD_PRE.1 Preparative Procedures	SPECTRUM SpectroSERVER Performance Administration Guide [3509] r9.0 SPECTRUM Control Panel User Guide [5029] r9.0 SPECTRUM Installation Guide [5136] r9.0 SPECTRUM Report Manager Installation and Administration Guide [5169] r9.0 Evaluated Configuration for CA Spectrum Network Fault Manager R9 SP1	This document describes the preparative procedures that need to be done prior to installing CA SPECTRUM r9 SP1.
ALC_CMC.2 Use of a CM System	CM Plan and CI List for Spectrum.zip CA SPECTRUM® Network Fault Manager r9 SP1 (installable media)	These documents describe the use of the CM system in terms of the TOE.
ALC_CMS.2 Parts of the TOE CM Coverage	CM Plan and CI List for Spectrum.zip CA SPECTRUM® Network Fault Manager r9 SP1 (installable media)	These documents describe the CM scope of the TOE.

Component	Document(s)	Rationale
ALC_DEL.1 Delivery Procedures	CA_Spectrum_Delivery Plan (physical).docx ESD Delivery Plan (SPECTRUM document) CA SPECTRUM® Network Fault Manager r9 SP1 (installable media)	This document describes product delivery for CA SPECTRUM r9 SP1 and a description of all procedures used to ensure objectives are not compromised in the delivery process.
ASE_CCL.1 Conformance Claims	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Security Requirements	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5	This document describes the security problem definition of the Security Target.
ASE_TSS.1 TOE Summary Specification	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5	This document describes the TSS section of the Security Target.
ATE_COV.1 Evidence of Coverage	Booz Allen_CA_SPEC9+1_SFR to TSFI Mapping_2_20090619.xls Spectrum Security Test Plan.doc CA SPECTRUM® Network Fault Manager r9 SP1 (installable media)	This document provides an analysis of coverage for the TOE.
ATE_FUN.1 Functional Tests	Booz Allen_CA_SPEC9+1_SFR to TSFI Mapping_2_20090619.xls Spectrum Security Test Plan.doc CA SPECTRUM® Network Fault Manager r9 SP1 (installable media)	This document describes the functional tests for the TOE.

Component	Document(s)	Rationale
ATE_IND.2 Independent Testing	Booz Allen_CA_SPEC9+1_SFR to TSFI Mapping_2_20090619.xls Spectrum Security Test Plan.doc CA SPECTRUM® Network Fault Manager r9 SP1 (installable media)	This document describes the independent testing for the TOE.
AVA_VAN.2 Vulnerability Analysis	CA SPECTRUM® Network Fault Manager r9 SP1 Security Target version 1.5 CA SPECTRUM® Network Fault Manager r9 SP1 (installable media)	This document describes the the TOE and its requirements which will reviewed during the vulnerability analysis.

Table 11 Assurance Requirements Evidence

EAL2 Justification

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

PP Claims Rationale

This Security Target does not claim Protection Profile conformance.

11 Terminology and Acronyms

Terminology

Term	Definition
Administrator	A default role in SPECTRUM with set privileges. In the evaluated configuration the main difference between this role and the Operator role is that this role has user management privileges.
Authorized User	A user that has been identified and authenticated by the TOE.
Client machine	A machine that contains the OneClick Console, and is where all users interface with the TOE.
Discretionary Access Control (DAC) Policy	A means of restricting access to objects based on the identity of users and/or groups in which they belong.
Element	A device, host system, or connection on the network which SPECTRUM is monitoring. SPECTRUM collects information on an element to create a model of that element in its knowledge base.
Event record	A record of events that occurred on its associated element in SPECTRUM's monitored network. In the evaluated configuration, these are the objects the TOE protects.
Group	A named categorization used to manage the privileges of multiple users within the group.
Host machine	A machine that contains the main components of the TOE, including: SpectroSERVER, SpectroSERVER DB, Archive Manager, DDM DB, Web Server, and Report DB.
Model	An instantiation of an element on the network SPECTRUM is monitoring. A model contains information regarding the element and is used to create event record on that element.
Object	A model's event record.
Operation	Any action on an object.
Operator	A default role in SPECTRUM with set privileges. In the evaluated configuration the main difference between this role and the Administrator role is that this role does not have user management privileges.
Security Community	A character string which is assigned to each user and group. They are used to control access to the TOE's objects.
Security String	A character string which is assigned to each model. They are used to control access to the TOE's objects.
Super User	A default role in SPECTRUM with full privileges. In the evaluated configuration only one user can have the Super User role, that user will install and configure SPECTRUM.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any user of the TOE.

Table 12 Customer Specific Terminology

Acronyms

Acronym	Definition
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
ASE	Security Target Evaluation
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
DAC	Discretionary Access Control
DDM	Distributed Data Manager
EAL	Evaluation Assurance Level
FAU	Security Audit
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
ID	Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
JNLP	Java Network Launch Protocol
MIB	Management Information Base
SF	Security Function
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

Table 13 Acronyms