CA Unicenter®

Network and Systems Management, r11.1 SP1 CCV

Common Criteria
Security Target
Version 2.7

April 24, 2008
Prepared for:

CA, Inc.

Prepared by:

CYGNACOM SOLUTIONS

An Entrust Company

Suite 5200♦ 7925 Jones Branch Drive ♦ McLean, VA 22102-3305 ♦ 703 848-0883 ♦ Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF FIGURES AND TABLES

TABLE/FIGURE **PAGE**

1 SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET IDENTIFICATION

Target of Evaluation (TOE) Identification: CA Unicenter® Network and Systems Management, r11.1 SP1 CCV

Security Target (ST) Identification: CA Unicenter® Network and Systems Management, r11.1 SP 1 CCV Common Criteria Security Target.

ST Version Number: Version 2.7

ST Author: CygnaCom Solutions, Inc.

Assurance level: EAL2.

Registration: <To be filled in upon registration>

Keywords: Network security, network management, systems management, systems monitoring, network monitoring, performance monitoring.

1.2 SECURITY TARGET OVERVIEW

This ST forms the basis for the evaluation of the CA Unicenter® Network and Systems Management, r11.1 SP1 CCV product, referred to in the ST as 'Unicenter NSM'.

Unicenter NSM is a software tool for the administration of enterprise IT Environments. It provides platform-independent control over the combined IT infrastructure and the applications they support. Its architecture and design provides users a single management approach to monitor resources and invoke policy. The management functions provide information system services to manage traditionally discrete systems resources including, enterprises with heterogeneous networks, systems, applications, databases, and non-IT devices.

CygnaCom Solutions developed this ST under contract with CA, Inc. The ST revision history is provided in the front of this document. This is a software only TOE.

1.3 COMMON CRITERIA CONFORMANCE

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2.

The ST considered the CC International Interpretations as of the evaluation kick-off date and found none that are applicable to this ST. The NIAP interpretations were not considered.

1.4 DOCUMENT ORGANIZATION

Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, states that this ST does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Section 9, References, presents a list of the documents used in the creation of this ST.

1.5 ACRONYMS

Table 1-1 defines acronyms used in this document.

Table 1-1: Acronyms

Acronym	Definition
ACL	Access Control List
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AEC	Advanced Event Correlation
AES	Advanced Encryption Standard
AGD	Guidance Documents
AMS	Alert Management System
ATE	Tests
AVA	Vulnerability Assessment
CAICCI	CA International Common Communications Interface
CAFT	CA File Transport
CAM	CA Messaging
CC	Common Criteria [for IT Security Evaluation]

Acronym	Definition
CCI	CA International Common Communications Interface (CAICCI)
CCISSF	CAICCI Secure Sockets Family
CLI	Command Line Interface
DIA	Distributed Intelligence Architecture
DSM	Distributed State Machine
EAL	Evaluation Assurance Level
EM	Event Manager
FAU	Security Audit
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocols over SSL
ID	Identifier
IP	Internet Protocol
IPX	Internet Packet eXchange
IT	Information Technology
JDBC	Java Database Connectivity
JRE	Java Runtime Environment
MAC	Message Authentication Code
MCC	Management Command Center
MDB	Management Database
NSM	Network and Systems Management
OS	Operating System
PDG	Performance Data Grid
PEO	Proprietary Encryption Option
PM	Performance Monitoring
PP	Protection Profile
RSA	Rivest Shamir Adleman
SAP	Service Advertising Protocol
SF	Security Function
SFP	Security Function Policy
SHA1	Secure Hash Algorithm

Acronym	Definition
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SQL	Structured Query Language
SSL	Secure Socket Layer
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
UBI	Unicenter Browser Interface
UCM	Unicenter Configuration Manager
UMP	Unicenter Management Portal
UNS	Unicenter Notification Services
WRS	Web Reporting Services
WV	WorldView Manager

2 TOE DESCRIPTION

2.1 PRODUCT DESCRIPTION

CA Unicenter® Network and Systems Management, r11.1 SP1 CCV (Unicenter NSM) is a software tool that manages and monitors the health and performance of an IT infrastructure. It provides users with a single management approach to monitor resources and invoke policy. Its management functions provide information system services to manage systems resources including, enterprises with heterogeneous networks, systems, applications, databases, and non-IT devices.

Unicenter NSM's components are modular, thus it can be deployed on shared or distributed platforms. The secure communication services include identification and authentication among the communicating components and integrity and confidentiality for the data they transmit.

Unicenter NSM management capabilities provide the ability to identify resources throughout an enterprise and organize, monitor, and manage them. It monitors and controls: data and information from both CA and non-CA management systems; TCP/IP and IPX network communications; Windows, UNIX, Linux, and proprietary server platforms; hierarchical, relational and object databases; web servers; and diverse network devices.

Unicenter NSM's user interfaces are either role-based or are restricted to users granted permission to use their functionality. Unicenter NSM uses visualization models and a common object repository to turn significant amounts of data into useful and relevant information. Its object management and access control functions allow enforcement of management policies, user interface, and interaction. Users are authenticated and have access to multiple user interfaces to perform their administrative and management functions.

2.2 TOE BOUNDARY

The TOE includes the Unicenter NSM components as depicted in the Figures below. (The figures below show the distributed configuration of Unicenter NSM.)

Legend:

The boxes bordered by heavy lines represent the components of the TOE that are also components of the TSF.

Non-TSF components of the TOE appear within the box bordered by a light line.

Yellow fill indicates a user interface

Solid Black thin lines represent an internal connection between components

Violet lines represent HTTPS protocol connection

Pink lines represent CAM protocol connection

Blue lines represent DIA protocol connection

Orange lines represent CCI protocol connection

Solid Green lines represent SQL or JDBC protocol connection

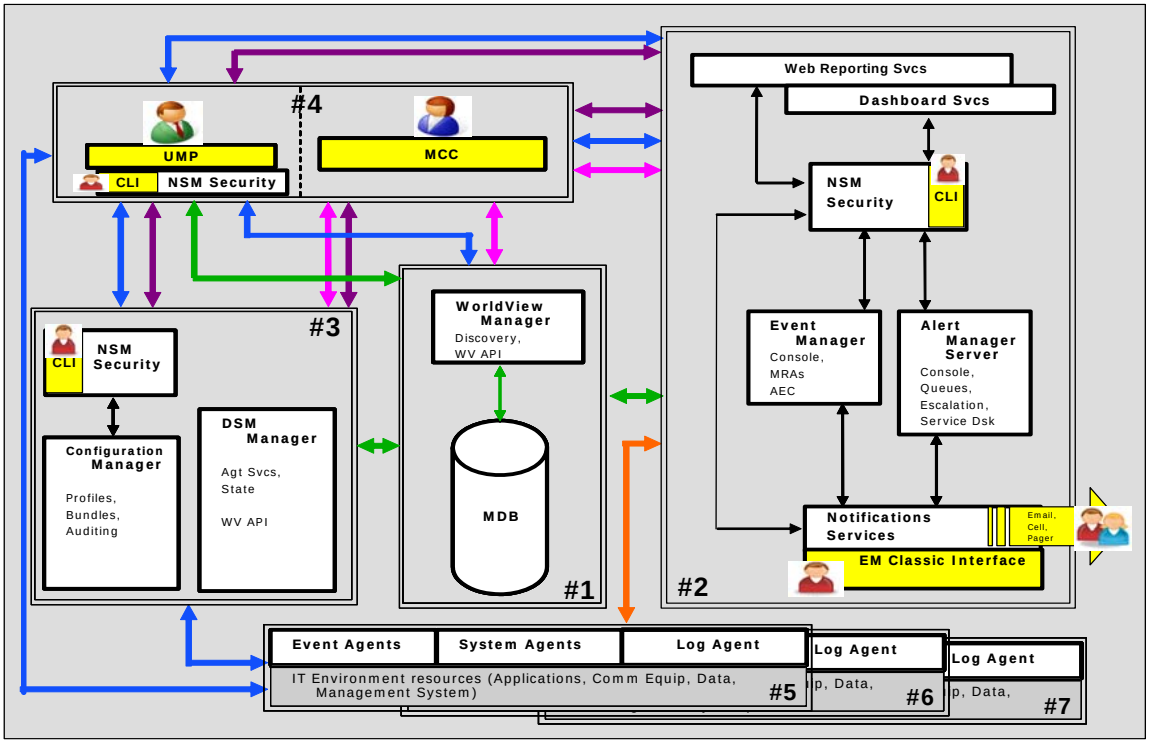

Figure 2-1: Target of Evaluation Physical Boundary (excluding Performance Monitoring Components)

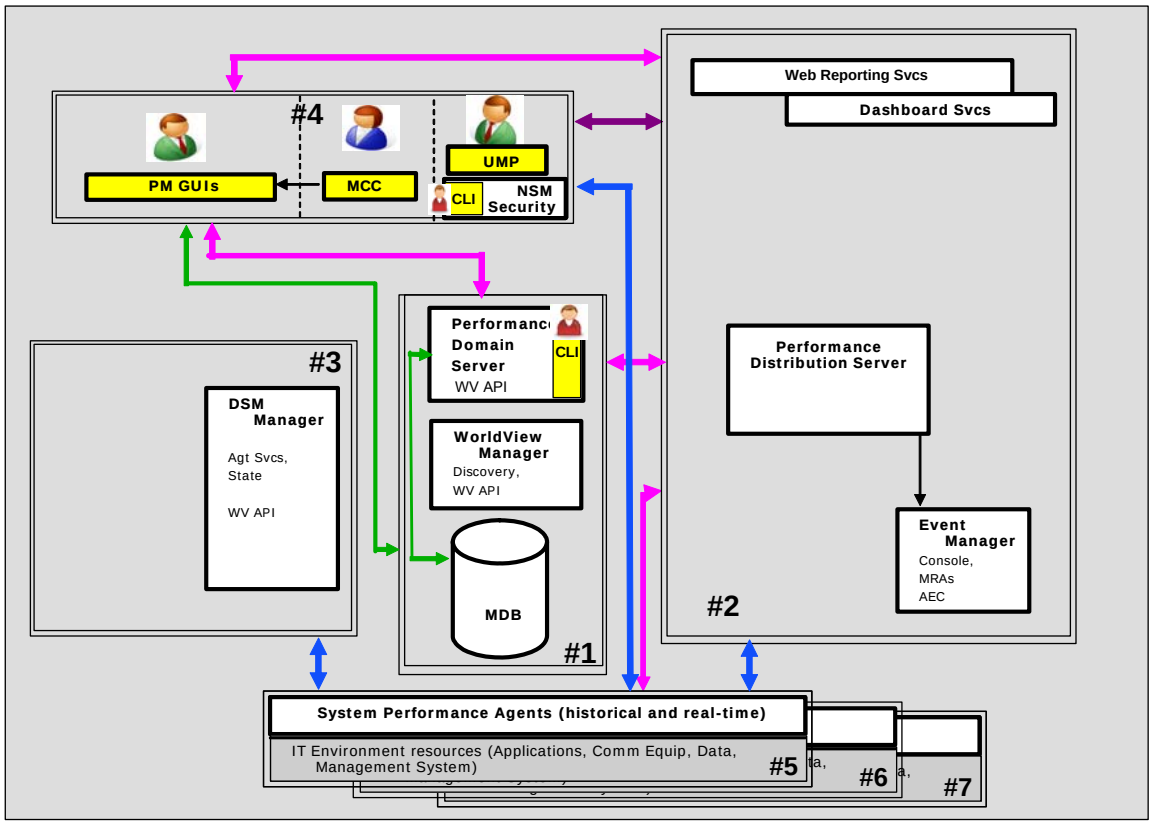

Figure 2-2: Target of Evaluation Physical Boundary (Performance Monitoring Components)

2.2.1 Unicenter NSM TOE Components

The following Unicenter NSM components are part of the TOE and the TSF:

- User Interfaces
    - Management Command Center (MCC) integrates many of the Unicenter NSM components into one command center. MCC is the primary interface for privilege based administration tasks such as audit review and policy configuration. It provides for the collection of I&A information and then passes the information on to the selected manager The managers then pass the collected information onto the NSM Security component for the I&A check and access control decisions. Enforcement of the I&A and access control decision is the responsibility of the individual requesting manager.
    - Unicenter Management Portal (UMP) is a customizable, secure and role-based portal for summary views. The UMP is used mainly by IT management to view the status of the environment at a high level. UMP provides its own identification and password based authentication security function, access control enforcement, and limited management functionality.
    - Classic Interface – WIN32 executables (GUI) and DOS CLIs. The only Classic Interface applications required to support the evaluated configuration (in-scope) are:
        - EM Classic – a WIN32 executable which is only available on the host machine of the UNS component. EM Classic is used to configure the UNS component.
        - secadmin – a command line executable only available on each host machine containing the NSM policy component and which is used to commit (apply) the NSM Security Policy changes made via the MCC interface.

      Users requiring the use of the above functions must be authenticated by the respective UNS or NSM Security component instantiation's host OS prior to being allowed access to these interfaces.

      All other security functionality that could be provided by other WIN32 executables and CLIs, which comprise the Classic Interface, have been incorporated into the MCC User interface. Therefore, all other Win32 executables and CLIs that are part of the Classic Interface are outside the scope of the evaluation and should not be used.
    - Performance Monitoring User Interfaces

      The Performance Monitoring functionality of the TOE provides GUI applications which are used to visualize, analyze, report, and configure performance and resource usage data. These applications are as follows:
        - Performance Scope - provides monitoring of the current performance of an enterprise and real-time analysis of any performance problems or outages that occur. Performance Scope also allows users to assign performance thresholds to resources, causing alarms to be generated and

actions to occur when a threshold breach occurs. Performance Scope runs as either a stand-alone GUI or launched from the MCC interface.

- Performance Trend – allows the user to observe patterns of activity and resource consumption, identify short-term and long-term usage trends, and analyze the impact of moving workload and traffic across different servers and devices. Performance Trend runs as either a stand-alone GUI or launched from the MCC interface.
- Performance Chargeback – identifies and reports on the usage of system resources, so that end-users can be charged for the computing resources and services that they consume. Performance Chargeback runs as a stand alone GUI. *Note: This component of Systems Performance requires Excel from Microsoft Office 97 SR-1, SR-2, Office 2000, or Office 2003.*
- Performance Configuration - used to create and apply configuration policies (called profiles) to Performance Agents. Once a Performance Agent has received a profile, it knows what performance data to collect, when to collect it, and where to send it. Performance Configuration runs as either a stand-alone GUI or launched from the MCC interface.

Performance Monitoring also provides a number of configuration commands (CLI utilities) that complement the GUIs listed above. As with the Classic Interface, the security functionality of these CLIs is either incorporated into the GUIs listed above or is not needed for the standard operation of the TOE. Only the following CLI is included in the scope of the evaluation:

- cfgutil – a command line executable which communicates requests for Performance Monitoring configuration. Sets MDB credentials for publishing of summary performance data.

- MDB – the common object repository. Used for storage and retrieval of System data and Managed Object data. The types of TSF data stored are Managed Objects (representation of managed network resource), System data (configuration data for the TOE), UMP System data (security data controlled by the UMP) and Performance Monitoring summary data. TSF Data is further discussed in Section 2.2.3

  Application Note: MDB in actuality is a database instance inside MS-SQL 2005 (MSSQL). MSSQL, the I&A and access control functionality it provides, and its interfaces, though used by the TOE, are not configured or controlled through a TOE interface. Therefore, the I&A and access control functionality requirements are specified in the IT Environment.

- NSM Security – provides the access control (NSM Security Policy) decision for the Manager components to enforce when a user has requested an action against System data. The NSM Security component can be configured so that there is one instantiation (centralized) per environment or multiple instantiation (decentralized) per environment. The NSM Security component is typically installed on each machine that is hosting a TOE component that requires the use of NSM Security for access control. Each instantiation is separately configured and managed. Each instantiation has its own individual NSM Security Policy stored in the MDB. This allows the NSM Security Policy to be specialized based on what managers it is supporting. Each manager (that requires the use of NSM Security) is configured to use a specific NSM Security component.

NSM Security can also be used to provide the Identification and Authentication decision. When configured to provide this service, NSM Security checks its host OS to determine if the user has an account on that platform (i.e. the requesting user must have a valid OS account on that machine). NSM Security relies on each manager component to supply the user context in which it is making the access or authorization request.

- Managers
  - WorldView Manager (WV or WV Manager) – an abstraction between the MCC and UMP User interfaces and the MDB Managed Object data. It provides a hierarchical view of the MDB data and provides access control (Data Scoping Policy) of the Managed Object data for the MCC Users. WV provides a history log, which is stored in the MDB, and contributes to auditing functionality.
  - Distributed State Machine Manager (DSM or DSM Manager) - serves as the Unicenter NSM Agent Manager. DSM provides state status of the System Agents and provides a view of the environment for TOE users. Customization of the managed network (DSM Scoping Policy) is enforced by the DSM.
  - Event Manager (EM) – used to categorize, log, and process events received from Event Agents throughout the IT Environment. EM receives detailed descriptions of events from Event Agents and processes the events using message record and action profiles.

    Message record and action profiles are policies that define how identified events should be handled. Events can be identified for automatic handling and/or specific processing that Unicenter NSM should perform when encountering them. The profile capabilities can be further enhanced by using Advanced Event Correlation (AEC) to identify a set of events to monitor and correlate, and decide what actions should be performed if correlation exists or does not exist.

    EM generates and maintains its own Event Log. The Event Log is maintained outside of the MDB and contributes to the audit functionality. There may one or more Event Manager in an IT Environment. Each instantiation of EM operates independently and is configured and managed independently. Each Event Agent is configured to use a specific EM instantiation.
  - Alert Manager System (AMS or Alert Manager) - tracks the most important events occurring in an enterprise (or a logical segment of an enterprise). Responsible for elevating alerts based on a customizable policy (AMS Alert notification Policy) and initiating notifications through UNS and providing a visual representation of the alerts to the MCC/UMP interfaces. AMS provides an AMS log, which is stored in the MDB, and contributes to auditing functionality.
  - Configuration Manager (UCM) - used to deliver configuration data to Unicenter NSM Managed Servers (via Unicenter NSM Agents) from a central location and maintains a comprehensive knowledge base of configuration data. UCM provides a UNS log, which is stored in the MDB, and contributes to auditing functionality.

- Services
    - Unicenter Notification Services (UNS) - sends wired and wireless messages (e.g., email, pages, etc.) using various protocols and services to get the attention of operators or administrators who must resolve a situation. UNS implements a customizable notification policy.
    - Dashboard Services – provides the security functionality for Agent configuration to authorized MCC Users. It allows the MCC User to query the Agent's configuration policy and update the configuration policy. UMP provides its own equivalent services to this.
    - Web Reporting Services (WRS) – provides the administrators with the ability to customize reports on different aspects of the enterprise being managed. This component provides the security functionality of audit review. Audit report templates for UCM activity are available to authorized MCC and UMP Users.
- Performance Monitoring Components (PM)

  Performance Monitoring provides the functionality for collecting, analyzing, and reporting performance information collected by the Performance Agents installed on managed IT systems. PM consists of two components which run as persistent services/daemons, so they can react to registration requests from Agents and service instructions from the Performance Configuration GUI application. Performance Agents (running on the managed systems) report to the Performance Distribution Servers, which in turn report to a Performance Domain Server.
    - Performance Domain Server component

      The Performance Domain Server holds all the performance configuration information for an entire domain and manages the Performance Distribution Servers within its domain. The Performance Domain Server automatically publishes the historical performance data that it has obtained from the Performance Distribution Servers to the MDB.
    - Performance Distribution Server component

      The Performance Distribution Server requests configuration data from the Performance Domain Server and delivers it to the Performance Agents. Performance Distribution Servers operate without the need for any local persistent information. The Performance Distribution Server manages performance data for the machines for which it is responsible and maintainsthis data in its local stores. If there is more than one Performance Distribution Server in a Unicenter NSM configuration, the servers are connected with each other in what is called the Performance Data Grid (PDG).
- Agents – provide the collection capabilities for the managed network. An Agent is installed on the IT resource it monitors and transmits (pushes) the information to the Event and DSM Managers for analysis and processing. The Agents have a configuration policy that can be viewed, modify, and installed/updated via the MCC or UMP interfaces. The Agents communicate with the Managers via a trusted channel that requires certificate-based authentication.

The categories of Agents that come with the product are:

- System Agents -responsible for monitoring the system status and statistics such as CPU, memory, and file system usage.
- Log Agents -only report on the log(s) that exist on their host.
- Event Agents -responsible to monitor their host and only report on the user-defined events that happen
- Performance Agents -collect data on a wide range of system and database resources, SAP resources, and SNMP-based resources. There are two types of Performance Agents:
  - Real-Time Performance Agents responsible for the real-time, transient collection of performance data, which it supplies to client applications such as Performance Scope.
  - Historical Performance Agents collect historical data and store it in highly compressed files called Performance Cubes. These cubes are initially stored on the file system of the Agent host machine, and are then automatically transferred to a designated Performance Distribution Server.

Any one or a combination of all types of Agents can be installed on the managed systems.

In addition to the components listed above, Unicenter NSM includes the following communication interfaces which are used for secure transmission of information between product components:

- Unicenter Distributed Intelligence Architecture (DIA) is a proprietary communications Interface and is the primary Unicenter NSM communication method.
- CA International Common Communications Interface (CACCI, also referred to as CCI for short) is a proprietary communication method still used by some parts of the Unicenter NSM product. It is used for remote calls to the NSM Security Module when remotely installed from the calling Manager and between the Event Agents and the Event Manager. The CCI will only be tested for communications between the Event Agent and the Event Manager.
  - CCISSF transmits any data from components or products using CCI over a Secure Sockets Layer (SSL) connection. CCISSF effectively “wraps” all data in an encrypted envelope.
- CA Messaging (CAM) is a proprietary lightweight messaging service used by some parts of the Unicenter NSM product. This service is used by the MCC to communicate to managers that require the MCC collected authentication information to be passed.
  - CAFT is a simple file transfer protocol (similar to FTP) that uses CAM for its data transport. CAM/CAFT is only used to transfer Performance Cube data (See Section 2.2.3) from the Performance Agents to the Performance Distribution Servers.

The evaluation is only testing the services provided by these communication methods. Any claim of conformance to standards and uses of encryption methods is based on Vendor Assertion and was not validated by this evaluation.

2.2.2 Users

Unicenter NSM users are those that communicate with Unicenter NSM via the user interfaces described above. The general Unicenter NSM user (who uses Unicenter NSM to manage the IT Environment) may also be referred to by the interface they use to access Unicenter NSM. They are:

- MCC User - a user that accesses Unicenter NSM from a workstation that has the MCC component installed.
- UMP User- a user that accesses Unicenter NSM from a workstation through a web browser pointing to the server that has the UMP component installed.
- Local User- a user that accesses Unicenter NSM from the workstation where the Unicenter NSM component (UNS or NSM Security) is installed (used for the Classic Interface GUI or CLIs necessary for two of the management requirements).
- Performance User – a user that accesses the Performance Monitoring functionality of Unicenter NSM either through the stand-alone Performance Monitoring GUIs or through the Performance Monitoring CLI.

There are only two defined roles for MCC Users and UMP Users who perform security administration and management functions. They are:

- *Administrators:* An individual(s) that have been granted all privileges.
- *Users*: An individual(s) that have been granted partial administrative privileges.

Unicenter NSM does not maintain roles for *Local Users* or *Performance Users*. However, the identity of the *Local User*, obtained from the UNS or the NSM Security instantiation's host OS, is used for the access control decision when requesting to perform either of the two security administrative functions described earlier using the Classic interface. Similarly, the identity of the *Performance User*, obtained from the host OS on which the Performance Monitoring GUI or CLI is installed, is used for access control to the PM functionality.

2.2.3 Data

All TOE data is trusted data, there is no user data. The following provides terminology the ST uses for the TSF data.

- Managed Objects data – the collection of data that has been stored in the MDB to represent the object(s) that are within the scope of Unicenter NSM control. An object is a unique identifier representing an individual IT Environment resource. Object data is the statistical and informational data associated with a particular object (IT Environment resource) that has been collected and processed by the TOE.
- UMP System data – the TSF data which is stored in the MDB (which includes user I&A information) and the UMP component's host file system and is under the control of the UMP Access Control Policy. UMP System data is also referred to as 'UMP objects'. The UMP objects include configuration parameters and reports generated via the UMP interface.

- Performance Monitoring data - The compressed files called Performance Cubes which store historical performance data as described in Section 2.2.1. A Performance Distribution Server also builds a summary cube for each machine for which it is the primary source of performance data. Each summary cube contains one year's worth of data for a single machine. The Performance Domain Server automatically stores summary historical performance data in the MDB.
- System data – the data used by the TSF to provide the security functionality, this includes configuration data, user attributes, and Unicenter NSM component certificates. Almost all of this data resides in the MDB. Some data resides with its associated Manager component as files on the host OS, e.g. event logs, and configuration files such as the user.dat file which provides the access control information for Performance Monitoring. Access to this type of data is enforced by a combination of the access control policies of the host OS and of the TOE.

2.2.4 Other components

There are CA Unicenter NSM r11.1 SP1 CCV software components that are included on the installation media but are **NOT** included in the scope of the evaluation. These components are being deprecated, have counterparts that are available through the in-scope user interfaces, or are only used during installation. These are not identified in Figure 2-1 or Figure 2-2.

These components are:

- Other User Interfaces:
  - Classic Interface WIN32 GUIs and CLIs not previously listed in Section 5.
  - Performance Monitoring CLIs not previously listed in Section 5.
  - Unicenter Browser Interface (UBI) [deprecating].
- Other tools provided on the installation media which are not part of the TOE:
  - XML GUI Editor for DIA (used during installation and configuration of DIA and is not needed for operational TOE).
  - Continuous Discovery and Classification - Used to continuously scan the network for new resources that have been added into the network via DHCP request monitoring. This feature is planned to be deprecated in r12.0. A manual counterpart to this functionality is available via the MCC and UMP interfaces and was tested.

2.2.5 IT Environment

The TOE is intended to be used in cases where there is a low level of risk. The TOE is intended to protect itself against attackers assumed to be unsophisticated with access to only standard equipment and public information about the product. The EAL2 Assurance Requirements are consistent with such an environment.

Unicenter NSM expects the following support from the customer's IT Environment:

1. Physical protection of TOE component host platforms that are critical to the security policy enforcement. No untrusted users or software are allowed on the host platforms of the NSM components.
2. Windows® Server 2003 OS platforms running on Intel based native hardware and network communication stack (specifically the TCP/IP stack) which provide:

a. Support for secure communications for trusted channels (in conjunction with the TOE) among the TOE (Unicenter NSM) components.

b. Support for certificate-based mechanisms used in establishing the trusted channels.

c. Reliable time stamps from the platform.

d. File protection.

e. User identification and password based authentication configured and required for access to OS and TOE components requiring users to have an OS account on its host platform.

f. A security domain for each platform's own protection and process isolation.

g. Policy enforcement mechanisms that are invoked and must succeed before each request to a resource within the scope of control of the host OS is allowed to proceed

3. Web services provided by Tomcat/Apache (version 4.1.29). Tomcat does not provide any other service for the TOE, such as I&A. This product is provided on the distribution media and does not need to be installed separately.
4. OpenSSL Cryptolibrary (version 0.9.8g) used for establishing secure communications between TOE components. This library is provided on the distribution media and does not need to be installed separately.
5. Dylan Secure Sockets library used for establishing secure communications between TOE components. This library is provided on the distribution media and does not need to be installed separately.
6. JRE - DIA does not require that a JRE be installed or running on the system. DIA lays down a JRE (1.4.2_16), but it is not installed or registered with the system. DIA is fully encapsulated and starts executables and JREs as needed during the course of normal operations.
7. MSSQL 2005 RDBMS - MSSQL is used by the TOE to implement is MDB instantiation for data storage and retrieval. The installation process ensures that only password-based authenticated MDB users can access MDB data based on database roles and privileges. The environment protections ensure the database does not have an external interface. Encrypted communication services must be turned on.
8. Microsoft Excel from Microsoft Office 97 SR-1, SR-2, Office 2000, or Office 2003. Needed for the operation of the Performance Chargeback GUI.
9. Microsoft Internet Explorer version 6.1 or better for using the UMP interface.

The TSF Components and their platforms in the IT Environment are listed in Table 2-1: Evaluated Configuration.

Table 2-1: Evaluated Configuration

Component	Platform: Operating System, Software, Hardware	Testing Platform
Management Database (MDB) WorldView Manager (WV) Performance Domain Server	OS: • Windows 2003 Software: • OpenSSL Cryptolibrary • MSSQL 2005 RDBMS Hardware: • Processor: Pentium 2 GHz • Memory: 2 GB • Disk Space: 6 GB	Platform #1
Event Manager (EM) Alert Manager (AMS) Unicenter Notification Services (UNS) Dashboard Services Web Reporting Services (WRS) NSM Security Performance Distribution Server	OS: • Windows 2003 Software: • OpenSSL Cryptolibrary • Tomcat/Apache Web Server Hardware: • Processor: Pentium 2.8 GHz • Memory: 2 GB • Disk Space: 8 GB	Platform #2
Distributed State Machine Manager (DSM) Configuration Manager (UCM) NSM Security	OS: • Windows 2003 Software: • OpenSSL Cryptolibrary • Tomcat/Apache Web Server Hardware: • Processor: Pentium 2 GHz • Memory: 1 GB • Disk Space: 4 GB	Platform #3
MCC	OS: • Windows 2003 Software: • OpenSSL Cryptolibrary Hardware: • Processor: Pentium 1.8 GHz • Memory: 512 MB • Disk Space: 1 GB	Platform #4
UMP NSM Security (used for tests when optional configuration is set to use NSM Security)	OS: • Windows 2003 Software: • OpenSSL Cryptolibrary • Tomcat/Apache Web Server • JRE plugin • IE Browser Hardware: • Processor: Pentium 2 GHz • Memory: 1 GB • Disk Space: 4 GB	Platform #4

Component	Platform: Operating System, Software, Hardware	Testing Platform
Performance Monitoring GUIs	OS: • Windows 2003 Software: • OpenSSL Cryptolibrary • Microsoft Excel Hardware: • Processor: Pentium 2 GHz • Memory: 1 GB • Disk Space: 4 GB	Platform #4
Unicenter NSM Agents: • System Agents • Log Agents • Event Agents • Performance Agents	OS: • Windows 2003 Software: • OpenSSL Cryptolibrary Hardware: • Processor: Pentium 550 MHz • Memory: 512 MB • Disk Space: 500 MB	Platforms #5, #6 and #7

2.2.6 TOE Configuration settings

The following configuration options must be set in the evaluated configuration:

- Disable Password Caching
- Continuous Discovery not installed
- UCM, Dashboard Services, and Web Reporting Services configured to use NSM Security I&A
- WV Data Scoping enforcement turned on as part of the post installation procedures
- Default UMP user “uniuser” password must be changed.

2.3 TSF SECURITY FUNCTIONS

The following security functions are in the scope of the evaluation:

- Audit – The TOE provides a decentralized audit generation capability along with a review process that allows the authorized user to selectively generate reports as well as search, sort, and order the display of audit records. The interface does not allow modifications or deletion of audit information.
- Alerts on event data – The TOE collects events that are used to categorize, log, and process events received from the Event Agents and Performance Agents throughout the IT Environment. Alerts are triggered based on a defined escalation policy.
- User attribute definition – The TSF maintains user attributes. These attributes are maintained by the TOE to grant access and permission for managing TSF data.

- Identification and Authentication – The TSF relies on password-based (provided both the TOE, MSSQL, and by the OS) and certificate-based mechanisms to support user authentication. The certificate-based mechanism is also used for the secure communication between the TOE and the Unicenter NSM Agents.
- Administration and management of security – The TSF user interfaces provide a controlled interface for the management functions. The user interfaces to the management functions are GUI based interfaces, with the exception of the required CLIs listed in Section 2.2.1.The user interfaces provide a hierarchical view of the system for navigation to the requested services, referred to as 'Enterprise Management', providing views and access to the specific data to be managed, only displaying the relevant data for the operation and available to the user based on the user's role and permissions. All access control pertains to security management functions.
- Partial Trusted communication – The TSF includes a trusted communication infrastructure that provides trusted communication channels among its distributed application components such as between the UCM and the Unicenter NSM Agents.
- Partial TSF self-protection – The TSF after being invoked by the OS ensures that TOE security functions are non-bypassable and protected from interference and tampering. Since this is a software-only TOE, it also relies on the underlying OS to provide non-bypassability and domain separation. The TSF ensures that security protection enforcement functions are invoked and succeed before each function within Unicenter NSM's scope of control is allowed to proceed. The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. A user session is allocated after successful authentication and all user operations are conducted in the context of the associated session. The TOE is also responsible to ensure that stored audit records cannot be modified or deleted via the TOE interfaces.

3 TOE SECURITY ENVIRONMENT

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 ASSUMPTIONS

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1: Assumptions

Item	Assumption	Description
1	A.Admin	It is assumed that the administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
2	A.Manage	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
3	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the systems that host the Unicenter NSM components.
4	A.Physical	It is assumed that the TOE, including its components critical to the security policy enforcement, will be protected from unauthorized physical access and from unauthorized physical modification.
5	A.Users	It is assumed that users will protect their authentication data.

3.2 THREATS

The following are threats identified for the TOE to counter. The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to only standard equipment and public information about the product.

Table 3-2: Threats

Item	Threat	Description
1	T.Misuse	A TOE resource may be compromised as a result of an authorized administrator of the TOE not having the ability to notice potential security violations by authorized or unauthorized users. Therefore, limiting their ability to identify and take action against a possible security breach.
2	T.Bypass	An attacker may attempt to bypass TOE security functions to gain unauthorized access to TSF through the local machine or network interfaces.
3	T.Mismanage	Authorized administrators may make errors in the installation and management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.

Item	Threat	Description
4	T.ResourceMisuse	Unauthorized accesses and activity indicative of misuse may occur on IT Environment resources that the TOE monitors and go undetected.
5	T.Privilege	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
6	T.Tamper	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted) on the host machines.
7	T.Transmit	An attacker may attempt to view or intercept and modify TSF data while the data is being transmitted between the applications of distributed TOE components or between the TOE and its users.

3.3 ORGANIZATIONAL SECURITY POLICIES

There are no organizational security policies for this TOE.

4 SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives for the TOE are as follows:

Table 4-1: TOE Security Objectives

Item	TOE Objective	Description
1	O.Access	The TOE must provide its authorized users with the means of managing, controlling, and limiting access to the objects and resources they are responsible for, on the basis of user roles and in accordance with the set of rules defined by the Security Functional Policies.
2	O.Admin	The TOE must include a set of functions that allow effective management of its functions and data.
3	O.Alert	The TOE must collect information about events and send notification upon the detection of a potential security violation based on the rules and parameters specified by the user.
4	O.Attributes	The TOE must be able to maintain user security attributes.
5	O.Audit	The TOE will provide the capability to detect, create, and selectively view records of security relevant events.
6	O.AuditProtect	The TOE must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces.
7	O.Collect_I&A	The TOE must provide the ability to collect the identification and/or authentication information, from users attempting to access restricted TOE components, functions and data through the TOE's own interfaces.
8	O.IDAuth	The TOE must be able to identify and authenticate users attempting to access restricted TOE components and functions.
9	O.PartialNonBypass	The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed.
10	O.PartialSelfProtection	The TSF must maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.
11	O.PartialProtectComm	The TOE, in conjunction with the IT Environment, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents..
12	O.Roles	The TOE must support multiple roles.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT Environment are as follows:

Table 4-2: Security Objectives for the IT Environment

Item	IT Environment Objective	Description
E1	OE.Admin	The IT Environment must include a set of functions that allow effective management of user attributes required to support TOE functionality.
E2	OE.Attributes	The IT Environment must be able to maintain user security attributes.
E3	OE.AuditProtect	The IT Environment must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces.
E4	OE.IDAuth	The IT Environment must provide identification and authentication mechanisms for UMP Users, MCC Users, Local Users, and Performance Users prior to allowing any other TSF-mediated actions on behalf of that user.
E5	OE.PartialProtect	The IT Environment must protect itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control.
E6	OE.PartialProtectComm	The IT Environment, in conjunction with the TOE, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents.
E7	OE.Time	The underlying Operating System (OS) must provide reliable time stamps.

4.2.2 Non-IT Security Objectives

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

Table 4-3: Security Objectives for Non-IT Environment

Item	Non-IT Security Objective	Description
N1	ON.Install	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
N2	ON.NoUntrusted	The administrator must ensure that there are no untrusted users and no untrusted software on the systems that host the Unicenter NSM components.
N3	ON.Operations	The TOE must be managed and operated in a secure manner as outlined in the supplied guidance.
N4	ON.Person	Personnel working as authorized administrators must be carefully selected and trained for proper operation of the system.

Item	Non-IT Security Objective	Description
N5	ON.Physical	Those responsible for the TOE must ensure that the TOE, including those components that are critical to the security policy (e.g., the NSM Security component shown in Figure 2-1), is protected from any physical attack.
N6	ON.ProtectAuth	Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons.

5 IT SECURITY REQUIREMENTS

This section provides the TOE security functional and assurance requirements. In addition, the IT Environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, explicitly stated requirements based on Part 2 of the CC, and assurance components from Part 3 of the CC.

5.1 FORMATTING CONVENTIONS

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 2 and paragraph 2.1.4 as:

assignment: allows the specification of an identified parameter;

refinement: allows the addition of details or the narrowing of requirements;

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

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

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

- *Assignments* and *Selections* specified by the ST author are in ***[italicized bold text].***
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "**-#**". These follow the short family name and allow components to be used more than once with varying operations. "*****" refers to all iterations of a component.
- *Explicitly stated requirements* are named with an "_EXP" extension (additionally with a "_TOE" for TOE SFRs or with an "_ENV" extension for IT Environment SFRs) to denote that the requirement has been explicitly stated. For example: "FAU_STG_EXP_TOE.1"
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The Security Functional Requirements for the TOE consist of the following components derived from Part 2 of the CC and components of explicitly stated requirements, summarized in Table 5-1 below.

Table 5-1: Security Functional Requirement (SFR) Components

Item	SFR Component	SFR Component Name
1	FAU_GEN.1	Audit data generation
2	FAU_SAR.1	Audit review
3	FAU_SAR.2	Restricted audit review
4	FAU_SAR.3	Selectable audit review
5	FAU_STG_EXP_TOE.1	Partial protected audit trail storage: TOE
6	FAU_ARP_EXP.1	Alerts on event data
7	FIA_ATD.1-1	User attribute definition [UMP Users]
8	FIA_ATD.1-2	User attribute definition [MCC Users]
9	FIA_ATD.1-3	User attribute definition [Local Users]
10	FIA_ATD.1-4	User attribute definition [Performance Users]
11	FIA_UID.1	Timing of identification
12	FIA_UAU.1	Timing of authentication
13	FIA_UAU_EXP_TOE.5	Multiple authentication mechanisms: TOE
14	FMT_MTD.1	Management of TSF data
15	FMT_SMF.1-1	Specification of Management Functions
16	FMT_SMR.1	Security roles
17	FPT_RVM_EXP_TOE.1	Partial Non-bypassability of the TSP: TOE
18	FPT_SEP_EXP_TOE.1	Partial TSF domain separation: TOE
19	FTP_ITR_EXP_TOE.1	Partial Intra-TSF trusted channel among distributed TOE components: TOE

5.2.1 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) ***[the auditable events listed in column three of the Table 5-2 below]***.

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, ***[information specified in column three of*** **Table 5-2** ***below]***

Dependencies: FPT_STM.1 Reliable time stamps

Table 5-2: Auditable Events

Audit Type	Where Stored	Information contained in record
EM Log	OS Flat File	• Time stamp • NSM security access violations and authentication failures. • Commit of database changes (i.e. new policy definitions, modifications, deletes) for calendar, security, message records and actions (automation), and advanced event correlation. . • Resource state changes (from DSM)
UCM Audit Reports	MDB	• Time stamp • Name (definition of which depends on report type) • Creation, Updates, or Deletion of : o bundles o models o objects o delivery schedules
AMS Log	MDB	• Time stamp • User ID OR Name of modifying process • Action taken.
WV History Log	MDB	• Time stamp • Any additions, deletions, or updates to Managed Object properties performed by the owner initiating the change.
UNS Log	OS Flat File	• Time stamp • Sender, group, recipient, protocol, provider, alias, ID, step, direction, time sent, and time received
PM Domain Server Log	OS Flat File	• Time stamp • Configuration Profile changes • Performance Agent configuration delivery • Performance Agent configuration status changes

5.2.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide ***[administrators and users with privileges to read audit data]*** with the capability to read ***[audit data of type listed in column one accessed as specified in column three of Table 5-3 below]*** from the audit records.

Table 5-3: Auditable Review

Audit Type	Where Stored	How Accessed	Search/Sort/Order
EM Log	OS Flat File	MCC / UMP	Search on: • Node • Event • Time frame • Process • User Identity • Severity • Success • Failure
UCM Audit reports	MDB	MCC: WRS / UMP Customize support on predefined data,	Search on: • Predefined reports • Time frame • Name (definition depends on report type)
AMS Log	MDB	MCC	Not Selectable Presented in order of occurrence
WV History Log	MDB	MCC	Not Selectable Presented in order of occurrence

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

5.2.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

5.2.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform ***[searches, sorting, and* ordering]** of audit data based on ***[See column 4 in Table 5-3 above].***

Dependencies: FAU_SAR.1 Audit review

5.2.5 FAU_STG_EXP_TOE.1 Partial protected audit trail storage: TOE

FAU_STG_EXP_TOE.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion initiated through its own TSFI.

FAU_STG_EXP_TOE.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail initiated through its own TSFI.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXP_ENV.1 Partial protected audit trail storage: IT Environment

5.2.6 FAU_ARP_EXP.1 Alerts on event data

Hierarchical to: No other components

FAU_ARP_EXP.1.1 The TSF shall collect the event data it receives from the Unicenter NSM Event Agents and Performance Agents.

FAU_ARP_EXP.1.2 The TSF shall apply a set of rules in monitoring the event data and based on these rules send notification to the appropriate personnel (e.g., operators or administrators).

FAU_ARP_EXP.1.3 The notification method and form will be based on user-specified rules and parameters.

Dependencies: No dependencies

5.2.7 FIA_ATD.1-1 User attribute definition [UMP Users]

Hierarchical to: No other components.

FIA_ATD.1-1.1 **Refinement:** The TSF shall maintain the following list of security attributes belonging to individual ***UMP Users: [***

- ***when UMP configured for 'native' authentication: identity, password, group(s)***
- ***when UMP component is configured to use the NSM Security component for authentication: identity, group(s)]***.

Dependencies: No dependencies

5.2.8 FIA_ATD.1-2 User attribute definition [MCC Users]

Hierarchical to: No other components.

FIA_ATD.1-2.1 **Refinement:** The TSF shall maintain the following list of security attributes belonging to individual ***MCC Users: [identity, privilege(s)]***.

Dependencies: No dependencies

5.2.9 FIA_ATD.1-3 User attribute definition [Local Users]

Hierarchical to: No other components.

FIA_ATD.1-3.1 **Refinement:** The TSF shall maintain the following security attribute belonging to individual ***Local Users: [identity]***

Dependencies: No dependencies

5.2.10 FIA_ATD.1-4 User attribute definition [Performance Users]

Hierarchical to: No other components.

FIA_ATD.1-3.1 **Refinement:** The TSF shall maintain the following security attribute belonging to individual ***Performance Users: [identity, domain or hostname]***

Dependencies: No dependencies

Application note: The four iterations of FIA_ATD.1-1 through FIA_ATD.1-4 cover the security attributes that the TOE maintains for all types of users. Security attributes are also maintained by the IT Environment.

5.2.11 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow ***[see Table 5-4 below*]** on behalf of the user to be performed before the user is identified.

Table 5-4: Capabilities prior to Identification

Data Access by Component via:	MCC User	UMP User	Local User	Performance User
DSM	DSM Views	None	N/A	N/A
AMS	None	None	N/A	N/A
EM	Displays collapsed view of available EM servers	None	N/A	N/A
UCM	None	None	N/A	N/A
WV	Displays collapsed view of available servers	None	N/A	N/A
NSM Security	N/A	N/A	None	N/A
UNS	N/A	N/A	None	N/A

Data Access by Component via:	MCC User	UMP User	Local User	Performance User
PM	None	N/A	N/A	Access to Performance Cube Data via the Performance Trend GUI only if the GUI is installed on the same machine on which the cube data is stored

FIA_UID.1.2 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

5.2.12 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow ***[see Table 5-5 below]*** on behalf of the user to be performed before the user is authenticated.

Table 5-5: Capabilities prior to Authentication

Data Access by Component via:	MCC User	UMP User	Local User	Performance User
DSM	DSM Views	None	N/A	N/A
AMS	Displays view of available AMS servers and allows interaction.	None	N/A	N/A
EM	Displays collapsed view of available EM servers	None	N/A	N/A
UCM	None	None	N/A	N/A
WV	Displays collapsed view of available servers	None	N/A	N/A
NSM Security	N/A	N/A	Perform Commit action	N/A
UNS	N/A	N/A	View/Modify UNS configuration policy	N/A

Data Access by Component via:	MCC User	UMP User	Local User	Performance User
PM	Displays view of Performance servers and allows interaction. Allows viewing of Performance Data via Performance Monitoring GUIs	N/A	N/A	Displays view of Performance servers and allows interaction. Allows viewing of Performance Data via Performance Monitoring GUIs

FIA_UAU.1.2 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

5.2.13 FIA_UAU_EXP_TOE.5 Multiple authentication mechanisms: TOE

Hierarchical to: No other components.

FIA_UAU_EXP_TOE.5.1 The TSF shall require each user to be successfully authenticated by invoking authentication mechanisms in the TOE before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU_EXP_TOE.5.2 The TSF shall ensure that each user's claimed identity is authenticated according to the following multiple authentication mechanism rules:

- all UMP Users are authenticated by the TOE using a password-based authentication mechanism, when the UMP component is configured to use 'native' authentication
- all UMP Users are authenticated by the NSM Security component using the NSM Security's host OS's stored user attributes, when the UMP component is configured to use the NSM Security component for authentication.
- all MCC Users are authenticated by the IT Environment using the authentication information collected by the TOE (via MCC component), prior to accessing the following TOE components:
    - WorldView Manager (topology),
    - DSM tools to configure DSM Scoping,
    - Event Manager,
    - Configuration Manager, and
    - Dashboard and Web Reporting Services.

Dependencies: FIA_UAU_EXP_ENV.5 Multiple authentication mechanisms: IT Environment

Application note: Accessing the AMS and PM does not require authentication only identification.

5.2.14 FMT_MTD.1 Management of TSF data: TOE

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to ***[operations as specified in Table 5-6]*** the ***[TSF Data as specified in Table 5-6]*** to ***[the role as specified in Table 5-6].***

Dependencies:

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Table 5-6: Management of TSF Data

Operation	TSF Data	Role
Read, update, create, or delete	MDB Data (Managed Object information)	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke access to	MDB Data (Managed Object information)	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Read, update, create, or delete	UMP User I&A Information	• UMP: Administrator • UMP: Users who are granted privileges by an Administrator
Read, update, create, or delete	UMP User Groups	• UMP: Administrator • UMP: Users who are granted privileges by an Administrator
Read, update, create, or delete	UMP Access Control Policy*	• UMP: Administrator • UMP: Users who are granted privileges by an Administrator
Read, update, create, or delete	MCC User I&A Information	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke	MCC User Privileges (Read, Update, Write, Execute, Delete, Create, Search, Control)	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Read, update, or commit	Agent Configurations differenciate between agents (PM vs event, system, …)	• Administrators* • Users who are granted privileges by an Administrator* *Applies to accessing the functionality either by the UMP or MCC User interface.

Operation	TSF Data	Role
Read or update	NSM Security Policy Assets (AMS, EM, UCM, UNS)	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke user permission to	NSM Security Policy Assets (AMS, EM, UCM, UNS)	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Commit (Apply changes to NSM Security Policy)	NSM Security Policy	• Local User that has been granted privileges by an Administrator (Must be executed from the local host machine of each instance of NSM Security that requires the updates.)
Read or update	WV Security Policy Assets (Managed Objects)	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke user permission to	WV Security Policy Assets (Managed Objects)	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Read or update	DSM Scoping Policy	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke user permission to	DSM Scoping Policy	• Local User that has been granted privileges by an Administrator
Read or update	AMS Alert Notification Configuration Policy*	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke user permission to	AMS Alert Notification Configuration Policy*	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Respond to	Alerts and Events	• Administrators* • Users who are granted privileges by an Administrator* **Applies to accessing the functionality either by the UMP or MCC User interface.*
Read or update	EM Event Elevation Message and Alert Profiles	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator

Operation	TSF Data	Role
Grant or revoke user permission to	EM Event Elevation Message and Alert Profiles	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Read or update	EM AEC Message Policy	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke user permission to	EM AEC Message Policy	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Read or update	Notification Services Configuration	• Local User that has been granted privileges by an Administrator
Grant or revoke user permission to	Notification Services Configuration	• Local User that has been granted privileges by an Administrator
Read, update, create, or delete	Configuration Manager Profiles	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Grant or revoke user permission to	Configuration Manager Profiles	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Create	Unicenter NSM Reports	• Administrators* • Users who are granted privileges by an Administrator* **Applies to accessing the functionality either by the UMP or MCC User interface.*
View	Performance Monitoring Data • Scope • Trends	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator • Performance User that has been granted privileges by an Administrator
View	Performance Monitoring Data • Chargeback	• Performance User that has been granted privileges by an Administrator
Read, update, create	Performance Agent Profiles	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Read, update, create, delete	Performance Agent Profiles	• Performance User that has been granted privileges by an Administrator

Operation	TSF Data	Role
Read, update, or respond to	Performance Monitoring Alerts	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator
Read	Performance Monitoring Alerts	• Performance User that has been granted privileges by an Administrator
Grant or revoke user permission to	Performance Monitoring Configuration and Data	• MCC: Administrators, and • MCC: Users who are granted privileges by an Administrator • Performance User that has been granted privileges by an Administrator
Read, update, create, or delete	Performance Domain Server Configuration	• MCC: Administrators, and o MCC: Users who are granted privileges by an Administrator • Performance User that has been granted privileges by an Administrator

* *The term "policy" is used here to refer to the set of all parameters that may be modified by the user to configure the actions of the TOE component.*

5.2.15 FMT_SMF.1-1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1-1.1The TSF shall be capable of performing the following security management functions: ***[***

- ***Secure audit review;***
- ***as specified in FMT_MTD.1]****.*

Dependencies: No Dependencies

Application note: Managing the attributes to support user password-based authentication (OS and MSSQL) and MSSQL access control are specified in the IT Environment.

5.2.16 FMT_SMR.1 Security roles

Hierarchical to: No other components.

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

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

Dependencies: FIA_UID.1 Timing of identification

Application note: Both roles apply to UMP and MCC Users.

5.2.17 FPT_RVM_EXP_TOE.1 Partial Non-bypassability of the TSP: TOE

Hierarchical to: No other components.

FPT_RVM_EXP_TOE.1.1 The TSF, when invoked by the underlying OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: FPT_RVM_EXP_ENV.1 Partial non-bypassability of the TSP: IT Environment.

5.2.18 FPT_SEP_EXP_TOE.1 Partial TSF domain separation: TOE

Hierarchical to: No other components.

FPT_SEP_EXP_TOE.1.1-1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the TSFI (where an untrusted subject is a user that either does not have authorization to access Unicenter NSM or is a legitimate user performing unauthorized actions).

FPT_SEP_EXP_TOE.1.2-1 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: FPT_SEP_EXP_ENV.1 Partial TSF domain separation: IT Environment.

5.2.19 FTP_ITR_EXP_TOE.1 Partial Intra-TSF trusted channel among distributed TOE components: TOE

Hierarchical to: No other components.

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

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

Dependencies: FTP_ITR_EXP_ENV.1 Intra-TSF trusted channel among distributed TOE components: IT Environment

5.3 STRENGTH OF FUNCTION

The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

Strength of function applies only to non-cryptographic, probabilistic or permutational mechanisms. The TOE contains one probabilistic or permutation mechanism.

This mechanism is defined in FIA_UAU_EXP_TOE.5. The UMP Users are authenticated by the TOE using a *password-based authentication mechanism*, when the UMP component is configured to use 'native' authentication.

This mechanism has a claim of SOF-Basic.

5.4 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

The following Security Functional Requirements are required by the IT Environment to support the TOE security functions.

Table 5-7: SFR Components for the IT Environment

No.	SFR Component	SFR Component Name
20	FAU_STG_EXP_ENV.1	Partial protected audit trail storage: IT Environment
21	FIA_ATD.1-5	User attribute definition [UMP Users]
22	FIA_ATD.1-6	User attribute definition [MCC Users]
23	FIA_ATD.1-7	User attribute definition [Local Users]
24	FIA_ATD.1-8	User attribute definition [Performance Users]
25	FIA_UID.2	User identification before any action
26	FIA_UAU.2	User authentication before any action
27	FIA_UAU_EXP_ENV.5	Multiple authentication mechanisms: IT Environment
28	FMT_SMF.1-2	Specification of Management Functions
29	FPT_RVM_EXP_ENV.1	Partial Non-bypassability of the TSP: IT Environment
30	FPT_SEP_EXP_ENV.1	Partial TSF domain separation: IT Environment
31	FPT_STM.1	Reliable time stamps
32	FTP_ITR_EXP_ENV.1	Partial Intra-TSF trusted channel among distributed TOE components: IT Environment

5.4.1 FAU_STG_EXP_ENV.1 Partial protected audit trail storage: IT Environment

FAU_STG_EXP_ENV.1.1 The IT Environment shall protect the stored audit records in the TSF audit trail from unauthorized deletion initiated through the IT Environment's Interfaces.

FAU_STG_EXP_ENV.1.2 The IT Environment shall be able to prevent unauthorized modifications to the audit records in the TSF audit trail initiated through the IT Environment's Interfaces.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXP_TOE.1 Partial protected audit trail storage: TOE

5.4.2 FIA_ATD.1-5 User attribute definition [UMP Users]

Hierarchical to: No other components.

FIA_ATD.1-5.1 **Refinement:** The ***IT Environment*** shall maintain the following security attribute belonging to individual ***UMP Users***: ***[when UMP component is configured to use the NSM Security component for authentication: OS identity, OS password]***

Dependencies: No dependencies

5.4.3 FIA_ATD.1-6 User attribute definition [MCC Users]

Hierarchical to: No other components.

FIA_ATD.1-6.1 **Refinement:** The ***IT Environment*** shall maintain the security attribute belonging to individual ***MCC Users***: **[*OS identity, OS password, MSSQL identity, MSSQL password, MSSQL privilege(s)]***

Dependencies: No dependencies

Application note: MCC has two sets of IT Environment user attribute definitions. When accessing a component that requires OS credentials, the attributes are identity and password. When accessing WV which requires MSSQL credentials, the attributes are identity, password, and privileges (for database operations only).

5.4.4 FIA_ATD.1-7 User attribute definition [Local Users]

Hierarchical to: No other components.

FIA_ATD.1-7.1 **Refinement:** The ***IT Environment*** shall maintain the security attribute belonging to individual ***Local Users***: ***[OS identity, OS password]***

Dependencies: No dependencies

5.4.5 FIA_ATD.1-8 User attribute definition [Performance Users]

Hierarchical to: No other components.

FIA_ATD.1-8.1 **Refinement:** The ***IT Environment*** shall maintain the security attribute belonging to individual ***Performance Users: [OS identity, OS password]***

Dependencies: No dependencies

Application Note: The four iterations of FIA_ATD.1-5, through FIA_ATD.1-8 cover the security attributes that the IT Environment maintains for all types of users. Security attributes are also maintained by the TOE.

5.4.6 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 **Refinement:** The ***IT Environment*** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application note: This applies to potential MCC, UMP, Local Users or Performance Users that are requiring access to the MCC, UMP, Classic Interfaces or Performance Monitoring GUIs or CLI.

5.4.7 FIA_UAU.2 User authentication before any action

Hierarchical to: No other components.

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

Dependencies: FIA_UID.2 Timing of identification

Application note: This applies to potential MCC, UMP, Local Users, or Performance Users that are requiring access to the MCC, UMP, Classic Interfaces or Performance Monitoring GUIs and CLI.

5.4.8 FIA_UAU_EXP_ENV.5 Multiple authentication mechanisms: IT Environment

Hierarchical to: No other components.

FIA_UAU_EXP_ENV.5.1 The IT Environment shall require each user to be successfully authenticated by invoking authentication mechanisms in the IT Environment before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU_EXP_ENV.5.2 The IT Environment shall ensure that each user's claimed identity is authenticated according to the following multiple authentication mechanism rules:

- all UMP Users are authenticated by the NSM Security component using the NSM Security's host OS stored user attributes, when the UMP component is configured to use the NSM Security component for authentication.user attributes
- all MCC Users are authenticated using MCC's host OS provided password-based authentication mechanism.
- all MCC Users, when requesting access to the following TOE components, are authenticated using the TOE collected information as follows:
    - WorldView Manager: user authenticated using MSSQL provided password-based authentication,
    - DSM Tools: user authenticated using MSSQL provided password-based authentication,
    - Event Manager: user authenticated using NSM Security's host OS password-based authentication,
    - Configuration Manager: user authenticated using NSM Security's host OS password-based authentication,
    - Dashboard and Web Reporting Services: user authenticated using NSM Security's host OS password-based authentication,
- all Local Users are authenticated using the UNS or NSM Security instantiation's host OS provided password-based authentication.

- all Performance Users are authenticated using the PM user interface (GUI or CLI) instantiation's host OS provided password-based authentication.

Dependencies: FIA_UAU_EXP_TOE.5 Multiple authentication mechanisms: TOE

5.4.9 FMT_SMF.1-2 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1-2.1 **Refinement:** The ***IT Environment*** shall be capable of performing the following security management functions: **[*as specified in Table 5-8*]**

Dependencies: No Dependencies

Table 5-8: Management of required IT Environment Data

Operation	Supporting Data	User Type
Read, update, create, or delete	MCC Users: OS I&A information	• OS Administrator • Owner (password only)
Read, update, create, or delete	MCC Users: MSSQL I&A information and database privileges	• MSSQL Administrator
Read, update, create, or delete	Local Users: OS I&A information	• OS Administrator • Owner (password only)
Read, update, create, or delete	Performance Users: OS I&A information	• OS Administrator • Owner (password only)
Publish performance data to a relational database	Performance Users: MSSQL I&A information and database privileges	• MSSQL Administrator

5.4.10 FPT_RVM_EXP_ENV.1 Partial non-bypassability of the TSP: IT Environment

Hierarchical to: No other components.

FPT_RVM_EXP_ENV.1.1 The IT Environment shall ensure that the OS Security Policy enforcement functions are invoked and succeed before each function within the OS's Scope of Control is allowed to proceed.

Dependencies: FPT_RVM_EXP_TOE.1 Partial Non-bypassability of the TSP: TOE.

5.4.11 FPT_SEP_EXP_ENV.1 Partial TSF domain separation: IT Environment

Hierarchical to: No other components.

FPT_SEP_EXP_ENV1.1 The IT Environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the IT Environment's Interface.

FPT_SEP_EXP_ENV.1.2 The IT Environment shall enforce separation between the security domains of subjects in the IT Environment's Scope of Control.

Dependencies: FPT_SEP_EXP_TOE.1 Partial TSF domain separation: TOE.

5.4.12 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT Environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.4.13 FTP_ITR_EXP_ENV.1 Partial Intra-TSF trusted channel among distributed TOE components: IT Environment

Hierarchical to: No other components.

FTP_ITR_EXP_ENV.1.1 The IT Environment shall provide a communication channel among its distributed component applications that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure using the encryption and certificate services from the IT Environment.

FTP_ITR_EXP_ENV.1.2 The IT Environment shall use this trusted channel for all communication among its distributed application components.

Dependencies: FTP_ITR_EXP_TOE.1 Intra-TSF trusted channel among distributed TOE components: TOE

5.5 TOE SECURITY ASSURANCE REQUIREMENTS

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in the following table.

Table 5-9: EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration

Item	Component	Component Title
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

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

6 TOE SUMMARY SPECIFICATION

Table 6-1 summarizes the functions and maps them to functional requirements for the TOE.

Table 6-1: IT Security Functions Functional Requirements mapping

Item	SFR	Security Class	Security Function ID	Security Functions
1	FAU_GEN.1	Security audit	AUDIT	Audit Generation and Review
2	FAU_SAR.1	Security audit	AUDIT	Audit Generation and Review
3	FAU_SAR.2	Security audit	AUDIT MANAGEMENT	Audit Generation and Review Administration and management of security
4	FAU_SAR.3	Security audit	AUDIT	Audit Generation and Review
5	FAU_STG_EXP_TOE.1	Security audit	PROT	Partial TSF self protection
6	FAU_ARP_EXP.1	Security audit	ALERTS	Alerts on event data
7	FIA_ATD.1-1	Identification and authentication	ATTRIBUTE	User attribute definition
8	FIA_ATD.1-2	Identification and authentication	ATTRIBUTE	User attribute definition
9	FIA_ATD.1-3	Identification and authentication	ATTRIBUTE	User attribute definition
10	FIA_ATD.1-4	Identification and authentication	ATTRIBUTE	User attribute definition
11	FIA_UID.1	Identification and authentication	I&A	Identification and authentication
12	FIA_UAU.1	Identification and authentication	I&A	Identification and authentication
13	FIA_UAU_EXP_TOE.5	Identification and authentication	I&A	Identification and authentication
14	FMT_MTD.1	Security management	MANAGEMENT (AC) MANAGEMENT	Access control for security management Administration and management of security
15	FMT_SMF.1-1	Security management	MANAGEMENT	Administration and management of security
16	FMT_SMR.1	Security management	MANAGEMENT	Administration and management of security
17	FPT_RVM_EXP_TOE.1	Protection of the TSF	PROT	Partial TSF self protection

Item	SFR	Security Class	Security Function ID	Security Functions
18	FPT_SEP_EXP_TOE.1	Protection of the TSF	PROT	Partial TSF self protection
19	FTP_ITR_EXP_TOE.1	Trusted path/channels	TC	Partial Trusted communications

6.1 AUDIT – AUDIT GENERATION AND REVIEW

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

Unicenter NSM provides a decentralized auditing capability. The WV, EM, AMS, UCM, UNS, and PM components maintain logs or tables that provide an administrator with an audit capability. Although the audit functionality is not centralized and there is not a standardized format across the audit records, there are multiple places within NSM which provide auditing / logging capabilities.

1. WorldView Manager (WV) maintains a status history table within the MDB. This table maintains time stamped records of any additions, deletions, or updates to Managed Object properties performed by the ID of the database connection owner initiating the change. An administrator or user with privilege can view this audit trail through the MCC interface known as the Historian (displays time stamp and state information only). This interface provides the ability to search on an object or objects as well as search by a time frame. The remainder of items maintained within the status history table (additions, deletions, updates; and the severity and status number that was changed for an object) can be viewed by looking at the table through native SQL (access is via theSQL Query Analyzer).
2. The Alert Management System (AMS) stores in the MDB each automated, or user initiated, action that is performed on every alert from the time an alert is created in the MDB. An administrator or user with privilege can view this audit trail through the MCC interface. MCC presents audit trail records in order of occurrence.
3. Unicenter Notification Services (UNS) requests and replies are logged to a file in the Unicenter NSM directory tree. Another detailed log is created under the same directory in a CSV or XML format and contains information about completed notifications. This includes date, time, sender, group, recipient, protocol, provider, alias, ID, step, direction, user data, time sent, and time received. These are readable files that are stored on the UNS Server and can be displayed by a text editor like ‘notepad’. An administrator or user with privilege, authenticated by the UNS host OS, can locally view this audit trail.
4. The Configuration Manager (UCM) provides information, stored in the MDB, for audit reports that are available to an administrator or user with privilege from the UMP or MCC: Web Reporting Services interface. The auditing reports can also be filtered or searched by timeframe or a name field, the definition of which depends on the report type. Available reports include:
    - *Configuration Bundle Audit Report*: Report of the configuration bundles that were created, updated, or deleted during a specified time range. There is the capability to filter the report by Resource Type and delivery Schedule Name.

- *Configuration Model Audit Report*: The configuration model audit report displays configuration models (groups) created, deleted, or updated during a specific date range. There is the capability to filter the report by the resource model Group Name.
- *Configuration Object Audit Report:* Report of the configuration objects (file packages, base profiles, and differential profiles), that were created, updated, or deleted during a specified time range. There is the capability to filter the report by the Configuration Object Name.
- D*elivery Schedule Audit Report*: Report of the delivery schedules, that were created, updated, or deleted during a specified time range. There is a capability to filter the report by delivery Schedule Name.

5. *Adaptive Configuration Objects Audit Report:* The Adaptive Configuration Objects Audit Report Pane lets the user view a report of Base Profiles and Differential Profiles that were inserted, updated, activated or deleted during the time range selected on a remote Server that has adaptive configuration activated. This report provides information on configurations that are active for monitored resources that have adaptive configuration running. There is the capability to filter the report by Configuration Object Name.The Event Manager is considered the keeper of the audit log for NSM. Once this information is entered into the event log, it cannot be modified. Information maintained in this log includes the following:
   - NSM security access violations and authentication failures.
   - (Optionally) NSM security access and authentication attempts (success or failure)
   - Commit of database changes (i.e. new policy definitions, modifications, deletes) for calendar, security, message records and actions (automation), and advanced event correlation.
   - Resource state changes (from DSM)

   An administrator or user with privilege can view this audit trail through the UMP or MCC interface. The interface provides the ability to search on timeframe, node, event, process, user ID, severity, success, or failure.
6. Performance Monitoring (PM) audit data is recorded in a flat file, the PM Domain Server log, stored on the Performance Domain Server.. No specific functionality is provided by the TOE to view these logs. Instead, the end user would log onto the Domain Server system, navigate to the appropriate directory and view the files using a text editor such as notepad. The audit trail records are presented in order of occurrence. Information contained log in this includes:
   - Configuration Profile changes
   - Performance Agent configuration delivery
   - Performance Agent configuration status changes
   - Client application connections

Informational: In addition to the audit logs listed above, the Agent components produce trace log files which contain debug information. These trace logs may be used by CA Customer Support to resolve problems with the Agents.

IT Environment support: FPT_STM.1

6.2 MANAGEMENT - ADMINISTRATION AND MANAGEMENT OF SECURITY

(FAU_SAR.2, FMT_SMF.1-1, FMT_SMR.1, FMT_MTD.1)

The TSF user interfaces, MCC, UMP, The Classic GUI, PM GUIs, and the CLI utilities provide a controlled interface for the management functions defined in Table 5-6 and for the audit review functionality. The access control mechanisms are specified in Section 6.2.1 MANAGEMENT (AC) - Access Control for security management. The following is a description of the interfaces that provide users with these management capabilities.

These interfaces provide a hierarchical view of the system for navigation to the requested services, referred to as 'Enterprise Management', providing views and access to the specific data to be managed, only displaying the relevant data for the operation, and available to the user based on their role and permissions.

There are TSF management capabilities that can only be accomplished using the Classic Interface. The customization of the UNS notification policy (defines how to get hold of whom) and enabling NSM Security Policy changes for any instantiation of the NSM Security component [called a 'commit']. The TOE relies on the host OS for the UNS and NSM Security components to enforce identification and authentication prior to allowing access to these executables.

Management capabilities for Performance Monitoring can be accomplished either through the MCC interface or through the stand-alone PM GUIs. Management of the PM components also requires the use of a DOS CLI utility to communicate requests for Performance Monitoring configuration and set MDB credentials for the publishing of summary performance data. The TOE relies on the host OS for the PM Security components to enforce identification and authentication prior to allowing access to these stand-alone GUIs and the CLI.

The TSF specifies two types of roles: Administrator and Users.

- Administrator: The Administrators have full privileges and have access to all data and management functions. The Administrator is created during installation.
- Users: Users are granted privileges by Administrators. These privileges scope the user's management capabilities against TSF data. Default settings for 'users' is that there is no access or capabilities until assigned.

The TOE does not maintain a role for *Local Users* or *Performance Users*. However, the identity of the Local User, obtained from the UNS or the NSM Security instantiation's host OS, is used for the access control decision when requesting to perform the security administrative functions described earlier using the Classic Interface. Similarly, the identity of the Performance User, is obtained from the host OS on which the Performance Monitoring GUI or CLI is installed and is used for the access control decision when requesting to perform the security administrative functions for Performance Monitoring. (See Section 2.2.1)

The TOE relies on the IT Environment, as specified in FMT_SMF.1-2 to manage and enforce policy for the user identity and password.

IT Environment support: FMT_SMF.1-2

6.2.1 MANAGEMENT (AC) - Access Control for security management

(FMT_MTD.1)

Four access control policies define the control over access to the TSF data: the Data Scoping Policy, the UMP Access Control Policy, the PM Access Control Policy and the NSM Security Policy.

Administrators (or users with granted privilege) can specify rules and access control lists (ACL), to grant or deny permission to a user(s) to execute an action against an object(s) The ACLs can be defined for a specific asset (object) or a group of assets (class) or a group of classes (superclass). The rules that make up the ACL are based on user ID and user privileges. The group of rules and ACLs that grant or deny permissions for Managed Object data comprise the Data Scoping Policy. The rules that grant or deny permissions for UMP System data comprise the UMP Access Control Policy. The group of rules and ACLs that grant or deny permissions for Performance Monitoring data comprise the PM Access Control Policy. The group of rules and ACLs that grant or deny permissions for System data residing in the MDB comprise the NSM Security Policy.

In the most simplistic explanation, the access control check looks at the requesting user's ID and privileges and the requested action on an object and compares it to the information contained in the rule or ACL for the object/class/superclass to grant or deny the user's request.

Access to System data that resides with its associated Manager component as files on the host OS is enforced by a combination of the access control policies of the host OS and of the TOE user interfaces which allow or deny access to this data.

Informational: The IT environment also is relied upon to provide protection of the Classic Interface GUI, PM GUIs and the CLI commands used for management functions as defined by FMT_SMF.1-2.

6.2.1.1 Data Scoping

The enforcement of the access control policy for users requesting access to Managed Object data is referred to as 'Data Scoping'. The Data Scoping Policy enforcement provides further protection and filtering of specific data fields of Managed Object data from unauthorized access by controlling access between specific user ID's and the MDB objects, classes, superclasses, and groups of data based on data-type. As stated above, it is rule-based and uses Access Control Lists (ACLs) for granting or denying permission for the user's request to the Managed Object. The privileges that a user can be granted include: Select, Update, Insert, or Delete. By default, users connected to the repository (via MCC passed credentials to the WorldView component [See Section 6.5 for complete details]) have full access to the Managed Object data until Data Scoping Policy rules are generated to deny access to particular objects.

This Data Scoping Policy is implemented and enforced by the WorldView Manager component. The WV component is the access point for any user trying to access Managed Object data (also referred to as a WorldView object or WorldView data).

When receiving an incoming request the TSF determines the requesting user ID and loads all the Data Scoping Policy rules that correspond to the user and any applicable calendar time and date. The TSF uses a cache to help with performance. It synchronizes the cache with Data Scoping Policy rule updates and verifies it on a request-by-request basis. When multiple rules apply to a requesting user ID, order of precedence rules are applied as follows:

- Object-level rules take precedence over class-level rules. If object-level rules conflict, the Allow rule takes precedence.
- If class-level rules conflict, the Allow rule always takes precedence. This means that the rule is tied to the current class and has precedence over all other class generation level rules. A class generation level 1 rule is a rule that is tied to a class that is a direct superclass (parent) of the current class. (Class generation level 2 is the next level up in the hierarchy, and so on.) Rules for a class always take precedence over superclass rules.
- An Allow object-level rule takes precedence over any other object-level rule. An Allow class-level rule takes precedence over any other class-level rule. An Allow class-level rule never takes precedence over any object-level rule.
- If there is no specific class-level rule or object-level for a class or any of its superclasses, the inclusion hierarchy is used for Data Scoping evaluation. That is, the topology of the network is used for evaluation. Rules are evaluated for the parent of an object. If the rule applies to the parent, it applies to all children. If the parent has no rule that applies, its grandparent is searched, then its great grandparent, and so forth.
- For objects that are in multiple locations in the topology of the network, where one location has a Deny rule, and the other an Allow rule, the Allow rule takes precedence.
- Rules for an individual user take precedence over a group rule.

The Data Scoping Policy rules are stored in the MDB and are protected as WorldView objects and through MS SQL from modification and deletion.

6.2.1.2 UMP Access Control Policy

The enforcement of the access control policy for users requesting access to UMP System data (stored in the MDB and the UMP component's host file system) is referred to as 'UMP Access Control'. UMP System data is also referred to as 'UMP objects'. The UMP Access Control Policy enforcement provides protection for UMP objects from unauthorized access by controlling access between specific users (or user groups) and the UMP objects generated via the UMP interface (such as configuration parameters and reports). The privileges that a user or user group can be granted for a UMP object include: View & Modify.

This UMP Access Control Policy is implemented and enforced by the UMP component. The UMP Access Control Policy enforcement operates independently of the WorldView Manager component and the Data Scoping Policy and the NSM Security component and the NSM Security Policy.

UMP Access Control Policy rules are stored in the MDB as a table and are protected via the UMP Access Control Policy from modification and deletion. Only an authorized UMP User with proper privileges may modify the policy rules.

6.2.1.3 Performance Monitoring Access Control Policy

The enforcement of the access control policy for users requesting access to Performance Monitoring data is referred to as 'Performance Monitoring Access Control'.

Access permissions for this data are controllable through the file 'users.dat' which is stored on the Performance Domain Server. The users.dat file is used to control what operations users can perform against the Performance Data Grid (the interconnected Performance Domain Server and Performance Distribution Servers). When an attempt is made to connect to the Performance Data Grid, the Identity (user ID) and Domain Name / Machine Name of the user initiating the connection is checked sequentially against the entries in users.dat. When a match is found, this is used to determine which operations are allowed.

The configurable operations are:

- **read** - The user can view the profiles within this domain.
- **write** - The user can update the profiles within this domain.
- **deliver** - The user can deliver profiles to Agents and devices in this domain.
- **monitor** - The user can view the delivery status of profiles within this domain; for example, to see if an Agent is configured.
- **setstatus** - The Performance Distribution Server uses this status to report status back to the Domain Server. Set this permission for the machine where the Distribution Server is located.
- **admin** - Allows administrative operations against the Performance Data Grid.

6.2.1.4 NSM Security

The enforcement of the access control policy for users requesting access to System data stored in the MDB (MDB System data) is referred to as 'NSM Security'. NSM Security Policy enforcement provides protection for specific MDB System data from unauthorized access by controlling access between specific user IDs and MDB assets (specific System data). The NSM Security Policy component operates independently of WV and the Data Scoping Policy and has its own set of rules and ACLs. The privileges that a user can be granted in the NSM Security ACLs include: Read, Update, Write, Execute, Delete, Create, Search, and Control.

This NSM Security Policy is implemented and enforced by the NSM Security component. The NSM Security component is the access point for any user trying to access MDB System data (also referred to as an NSM asset).

Unlike the WorldView Manager component which has one instantiation operating in an environment, the NSM Security component can have multiple instances operating in an environment. The NSM Security component typically resides on all the platforms that have TOE component(s) that require the NSM Security services. Therefore, each instantiation has a uniquely identified and customized NSM Security Policy for that host.

Components that have an NSM instantiation installed on the same machine use a shared memory call (internal to the platform) instead of the external CCI communication which is used if the NSM Security component is located on a separate machine.

The NSM Security component can be centralized (one instance). This would require all distributed TOE components to use CCI communication to access the NSM Security component. This is not the typical scenario for Unicenter NSM installations.

NSM Security Policy rules are stored in the MDB and are protected via the NSM Security Policy from modification and deletion. Changes to the NSM Security Policy have to be manually activated (committed) on each NSM Security host platform. This requires an authorized TOE user to be authenticated at the OS level and execute a command line interface command (as described in Section 2.2.1) on each instantiation of the NSM Security component.

6.3 ALERTS - ALERTS ON EVENT DATA

(FAU_ARP_EXP.1)

As described in Section 2, the Event Manager receives details of events from the Event Agents. The EM processes these events and determines which of these events needs to be elevated to the Alert Manager (AMS).

Alert classes are groups of alert attributes and profiles including queue, escalation policy, and display attributes. Alert classes organize alerts and supply most of their initial properties. These classes help the user to define alerts because properties are automatically inherited by the alerts in each class.

Based on alert classes, AMS determines the alert properties and creates an alert based on user-defined policy profiles compared against the properties. Alert options can be set through the AMS interfaces for visualization and notification through the UNS component.

The UNS implements notifications in a number of ways. User actions can be defined so that notifications can be sent manually (by right-clicking with the mouse on the alert description displayed within the queue listing and selecting the action within the context menu that says "page" or "e-mail"). Additionally, notifications can be generated based on the alert's initial creation, its transfer between queues, and its closure. Notifications can also be sent based on a defined escalation policy. For example, if an alert has had no action taken on it for set amount of time, a notification can be immediately sent. Another example is if the priority of an alert reaches a specified value, a notification can be forced to occur (page, email, etc).

The Performance Agents also can be defined to send Alerts called “Alarms” in CA terminology. Alarms are triggered when a user defined threshold reaches a defined critical value.

The Threshold and Alarms area of the Performance Configuration Profile Editor allows the authorized user to view and define thresholds: the points at which selected resources that the Performance Agent is monitoring reach warning or critical states. So far as Performance Monitoring is concerned, a threshold breach only occurs if the average value of a resource exceeds the defined threshold throughout the entire time band.

The Performance Scope GUI allows the authorized user to assign performance thresholds to resources, causing alarms to be generated and actions to occur when a

threshold breach occurs. When a threshold breach occurs, assigned actions may include: display a message box, sound an alarm, log an error message in the Errors and Notifications window, or run an external application and pass parameters to it.

These threshold breaches are also visible in MCC.

The thresholding provided by the Performance Agents differs from that provided by the System Agents by the time over which the resources are monitored.

System Agents typically monitor their resources every minute or so, and a health alarm is triggered if a resource is detected to be operating outside the threshold limits.

Performance Agents sample the resources at user defined intervals; for example: every 20 minute or hourly. The metrics gathered by the Performance Agents are true averages of how the resources performed over this extended period, and the threshold calculations are determined from this. Only when this averaged value falls outside the threshold limits, is a Performance alarm triggered.

6.4 ATTRIBUTE - USER ATTRIBUTE DEFINITION

(FIA_ATD.1-1, FIA_ATD.1-2, FIA_ATD.1-3, FIA_ATD.1-4)

The attributes used to determine what a user is capable of accomplishing are broken down into several groups. They are based on which interface the user is attempting to access the data from and how the manager or component is configured for I&A access (See Table 6-2 below).

The attributes (user identity and groups/privileges) determine who can perform what security administration and management functions.

The TOE relies on the IT Environment (OS) to maintain some of the identification and password attributes for users (mainly for MCC Users accessing managers).

The TOE relies on the IT Environment (MSSQL) to maintain username, password, and database privileges for users requiring WV access.

The following table breaks down the attributes and how they are stored and used (I&A or access control). Components with alternative I&A configurations are also noted and are identified with a (alt) next to the X or Y.

IT Environment support: FIA_ATD.1-5, FIA_ATD.1-6, FIA_ATD.1-7, FIA_ATD.1-8

Table 6-2: Attributes maintained by the TSF that are used for I&A

User	TOE Sec Attributes	For UMP I&A functionality		For MCC I&A functionality		For EM I&A functionality		For WV I&A functionality	For UCM I&A functionality	For AMS I&A functionality		For DSM I&A functionality	For Dashboard Services I&A functionality
		stored in MDB	stored in NSM Host OS	stored in MDB	stored in MCC Host OS	stored in EM Host OS	stored in NSM Host OS	stored in SQL	stored in NSM Host OS	stored in MCC Host OS	stored in MDB	stored in SQL	stored in NSM Host OS
UMP	identity	X	Y (alt)										
	password	X	Y (alt)										
MCC	identity				Y	Y(alt)	Y	Y	Y	Y	X	Y	Y
	password				Y	Y(alt)	Y	Y	Y	Y		Y	Y

User	TOE Sec Attributes	For UNS I&A functionality		For NSM Security Component I&A functionality		User	TOE Sec Attributes	For PM I&A functionality	
		stored in NSM Host OS	stored in MDB	stored in NSM Host OS	stored in MDB			stored in PM Host OS	stored in MDB
Local	identity	Y	X	Y	X	Performance	identity	Y	X
	password	Y		Y			password	Y	

X – Totally maintained by the TSF

Y – Totally maintained by the IT Environment in support of the TSF

Table 6-3: Attributes maintained by the TSF that are used for access control

User	TOE Sec Attributes	For UMP Access Control functionality	For MCC Access Control functionality	For EM Access Control functionality	For WV Access Control functionality	For UCM Access Control functionality	For AMS Access Control functionality	For DSM Access Control functionality	For Dashboard Access Control functionality	For UNS Access Control functionality	For NSM Security component instantiation Access Control functionality	For PM Access Control functionality
		stored in MDB	stored in MDB	stored in MDB	stored in MDB	stored in MDB	stored in MDB	stored in MDB	stored in MDB			
UMP	identity	X										
	password											
	group	X										
MCC	identity		X	X	X	X	X	X	X			
	password											
	privileges		X	X	X	X	X	X	X			
Local	identity											X
Perfor mance	identity									X	X	

X – Totally maintained by the TSF

Y – Totally maintained by the IT Environment in support of the TSF

6.5 I&A - IDENTIFICATION AND AUTHENTICATION

(FIA_UID.1, FIA_UAU.1, FIA_UAU_EXP_TOE.5)

The TSF provides a minimal capability for the user prior to being identified or authenticated by the TOE. Table 5-4 gives details to what the user is capable of doing or seeing prior to identification. Table 5-5 gives details to what the user is capable of doing or seeing prior to authentication.

The only pre-authenticated capabilities for the user are via the MCC interface and the use of the Classic Interface.

UMP Users are identified and authenticated prior to being allowed any further functionality. The UMP User is authenticated using a password based mechanism provided by the TOE. The password policy implemented is:

- Maximum username and password length of 97 characters
- Minimum password length of 8 characters
- No restriction on characters (e.g. abc!@#$%^&*()_+-={}[]|\:";'<>?,./`~defÇüéâ are all permissible)
- Unlimited login failures
- No software enforcement of password expiration

The MCC component relies on the host OS to enforce the identification and authentication of the user prior to executing the MCC interface. In most cases, the MCC interface forces the collection of identification and authentication information from the user (via a pop-up window) when directed to do so by the manager component (i.e. EM) the user selected to access information from. The manager will then receive this information (MCC passed credentials) and the NSM Security component will verify these user credentials with the host OS. Since the NSM Security component will be loaded on the same machine as the manager that is configured to use it, the MCC User must have a valid user account on the manager's host OS machine.

There are two exceptions to the scenario above. The first is when the MCC User has requested access to an AMS server. In this case, the MCC does not collect the identification and authentication information via a pop-up window. Instead, it automatically retrieves the logged in user's OS *user ID* which is forwarded to the AMS and the NSM Security component will verify only access control based on the identity (and privileges assigned to that user).

The second exception is when the MCC User has requested access to WorldView Manager data (e.g. topology view). The I&A information is collected via a pop-up window and is sent to the WorldView Manager. However, the credentials are verified against the MSSQL identification and authentication mechanism. Therefore, the MCC User must have a valid MSSQL user account.

Informational: MS-SQL is installed for UMP and Unicenter NSM to use in mixed mode authentication. When enabled, mixed mode authentication allows users to log into MS-SQL server using either a Windows username and password or a MS-SQL database username and password. When logged in using Windows username and password, the user will have access to all the databases on the server. The TOE will be tested using the OS credentials only.

Informational: Agents use a certificate-based mechanism for the secure communication between them and the other TOE components. This mechanism is described in Section 6.6 TC – Partial Trusted Communication, below.

The Classic Interface (Win32 GUI and CLI) and Performance Monitoring interfaces (stand-alone GUIs and CLI) require that the user be authenticated at the OS level (local machine). These functions behave in a similar manner as the MCC to AMS identification described above. The Classic Interface software collects the requesting user's *user ID* and passes this information along with the requested action to the NSM Security for the access control check. The Performance Monitoring interfaces collects the requesting user's user ID and passes this information along with the requested action to the Performance Domain Server where it is checked against the entries in the users.dat file for the access control decision.

IT Environment support: FIA_UID.2, FIA_UAU.2, FIA_UAU_EXP_ENV.5)

6.6 TC – PARTIAL TRUSTED COMMUNICATION

(FTP_ITR_EXP_TOE.1)

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

DIA is a proprietary communications Interface and is the primary Unicenter NSM communication method. DIA uses JRE libraries that come with the Unicenter NSM product.

CAM is a proprietary lightweight messaging service used by some parts of the Unicenter NSM product. This communication is used by the MCC to communicate to managers that require the MCC collected authentication information to be passed. CAM can be configured for either UDP or TCP communications.

CAFT is a simple file transfer protocol (similar to FTP) that uses CAM for its data transport. CAM/CAFT is only used to transfer Performance Cube data from the Performance Agents to the Performance Distribution Server.

CCI is a proprietary communication method used by some parts of the Unicenter NSM product. It is used for remote calls to the NSM Security component when remotely installed from the calling manager and also for communications between the Event Agents and the Event Manager. The testing configuration will only be testing the service between the Event Agent and the Event Manager.

CCI relies on the CCI Secure Sockets Facility (**CCISSF**) to provide the security services which is part of the IT Environment. CCISSF transmits and receives all Unicenter NSM component data over a Secure Sockets Layer (SSL) connection over TCP/IP. CCISSF works at the application level using cryptographic services from its environment to implement cryptographic-based security mechanisms. The CCISSF uses the SSL protocol for encryption capabilities. The SSL protocol uses the OpenSSL Cryptolibrary.

CCI can be configured to use **PEO** (Proprietary Encryption Option) as an alternative to SSL. By default, PEO is not enabled and PEO will not be used in the evaluated configuration.

The TOE requires mutual authentication between the endpoints of the connection using x.509v3 certificate-based RSA asymmetric digital signature and verification before exchanging data.

The TSF interface to the cryptographic support provided by the IT Environment is a set of API calls from CCI to encrypt, decrypt and manage the flow of the data.

The evaluation is only testing the services provided by these communication methods. Any claim of conformance to standards and uses of the above encryption methods is based on Vendor Assertion and is not validated by this evaluation.

Using these mechanisms a trusted path between the user and the interface is provided in conjunction with the underlying OS.

IT Environment support: FTP_ITR_EXP_ENV.1

6.7 PROT – PARTIAL TSF SELF PROTECTION

(FPT_RVM_EXP_TOE.1, FPT_SEP_EXP_TOE.1, FAU_STG_EXP_TOE.1)

The TSF, after being invoked by the OS, ensures that TOE security functions are non-bypassable. Since this is a software-only TOE, it also relies on the underlying OS to provide non-bypassability. The TSF ensures that security protection enforcement functions are invoked and succeed before each function within Unicenter NSM's scope of control is allowed to proceed. All user operations are conducted in the context of an associated session. This session is allocated only after successful authentication. User operations are checked for conformance to the granted level of access, and rejected if not conformant. The management session is destroyed when the corresponding user logs out of that session.

The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. Its protected domain includes all the TOE components.

The TSF has well defined external interfaces with its users and its interface to the IT Environment on which it depends.

Since the TOE is software-only, it relies on the OS file system to protect TSF data along with reliable time stamps, trusted channel services, and user verification. The underlying assumption regarding the operation of TOE is that the non-GUI TOE components are installed in an operational environment that is physically protected and that only administrators can gain access to these facilities while the TOE GUIs (MCC, UMP, Classic Interface and PM GUIs) can be run from any computer located within a trusted environment.

The TOE also prevents any user from modifying or deleting the audit records through the TSF interfaces. This works in conjunction with the IT Environment (OS and MSSQL) in order to provide full protection of the files, database structure, and records within the MDB. The following table summarizes what audit trails have TOE TSF interfaces that would contribute to the protection of the audit.

Table 6-4: Audit Protection TSF sumary

Audit Type	Where Stored	How Accessed
EM Log	OS Flat File	MCC / UMP
UCM Audit reports	MDB	MCC: WRS / UMP Customize support on predefined data,
AMS Log	MDB	MCC
WV History Log	MDB	MCC

IT Environment support: FPT_RVM_EXP_ENV.1, FPT_SEP_EXP_ENV.1, FAU_STG_EXP_ENV.1

6.8 SOF CLAIMS

The TOE contains one probabilistic or permutation mechanism. The UMP Users are authenticated by the TOE using a password-based authentication mechanism, when the UMP component is configured to use 'native' authentication as defined in SFR FIA_UAU_EXP_TOE.5 and described in Section 6.5 I&A - Identification and Authentication. This mechanism has a claim of SOF-Basic.

6.9 ASSURANCE MEASURES

The TOE satisfies CC EAL2 assurance requirements. The following lists identify the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures supplied by CA to satisfy the CC EAL2 assurance requirements.

ASE

a. CA Unicenter Network and Systems Management, r11.1 SP1 CCV Security Target, V2.6, Mar 20th, 2008

NOTE: CA Unicenter Network and Systems Management, r11.1 SP1 CCV will be shortened to Unicenter NSM r11.1 SP1 CCV for the rest of the documents.

ACM_CAP.2

a. Unicenter NSM r11.1 SP1 CCV Configuration Management Procedures, V1.0, Mar 10th, 2008
b. CSCR905-LATEST.xls
c. CSCR906-LATEST Sept 20 2007.XLS
d. Unicenter NSM r11.1 SP1 CCV Document Listing, V1.0 Mar 20th, 2008.

ADO_DEL.1

a. Unicenter NSM r11.1 SP1 CCV Delivery Procedures, Version 1, Mar 10th , 2008

ADO_IGS.1

a. Implementation Guide, 05/30/2006
b. Unicenter NSM r11.1 SP1 CCV Common Criteria Supplement to the Administrative Guidance, V1.0, Mar 20th, 2008
c. Common Criteria Installation Manual for Unicenter NSM r11.1 SP1 CCV, V1.0, Mar 20th 2008

ADV_FSP.1

a. Unicenter NSM r11.1 SP1 CCV Proprietary Development Specification, V 1.7, March 13th, 2008
b. All Unicenter NSM Bookshelf Manuals

ADV_HLD.1

a. Unicenter NSM r11.1 SP1 CCV Proprietary Development Specification, V 1.7, March 13th, 2008

ADV_RCR.1

a. Unicenter NSM r11.1 SP1 CCV Proprietary Development Specification, V 1.7, March 13th, 2008

AGD_ADM.1

a. Unicenter NSM r11.1 SP1 CCV Common Criteria Supplement to the Administrative Guidance, V1.0, Mar 20th, 2008
b. Common Criteria Installation Manual for Unicenter NSM r11.1 SP1 CCV, V1.0, Mar 20th 2008

Unicenter NSM BookShelf:

c. MDB Overview, 05/08/2006
d. Administrator Guide, 12/12/2006
e. Agent Technology Support for SNMPv3, 05/30/2006
f. CA SDK Developer Guide, 05/30/2006
g. Getting Started, 05/09/2006
h. Implementation Guide, 05/30/2006
i. Inside Event Management and Alert Management, 12/12/2006
j. Inside the Performance Agent, 05/30/2006
k. Inside Systems Management, 05/30/2006
l. Inside Systems Monitoring, 05/30/2006
m. Inside Systems Performance, 05/30/2006
n. MIB Reference Guide, 05/30/2006
o. Unicenter Management Portal Getting Started Guide, 12/12/2006

AGD_USR.1

a. N/A All users are considered administrators

ATE_COV.1

a. NSM-TCM_(2-4-2008) (version 1).xls

ATE_FUN.1

a. NSM Common Criteria Lab.htm
b. QA Test Plan for ESM-Common Criteria for Unicenter NSM 11.1 (each a separate htm document).
   - AMS, Nov 29th, 2007
   - CAM, Nov 20th, 2007
   - CCI, Nov 19th, 2007
   - DIA, Nov 29th, 2007
   - EM, Oct 29th, 2007
   - MCC, Nov 29th, 2007
   - PM, Nov 28th, 2007
   - UCM, Jan 17th, 2007
   - UMP, Nov 29th, 2007
   - UNS, Oct 29th, 2007
   - WRS, Nov 21th, 2007
   - WV, Oct 29th, 2007
c. Directory of test results

ATE_IND.1

a. Test Facility
b. TOE – Unicenter NSM r11.1 SP1 CCV software

AVA_SOF.1

a. Unicenter NSM r11.1 SP1 CCV Strength of Function Analysis, V1.0, Mar 10th, 2008

AVA_VLA.1

b. Unicenter NSM r11.1 SP1 CCV Vulnerability Analysis, V1.0, Mar 10th, 2008

7 PROTECTION PROFILE (PP) CLAIMS

The Security Target was not written to address any existing Protection Profile.

8 RATIONALE

8.1 SECURITY OBJECTIVES RATIONALE

8.1.1 Threats to Security

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE. Rationale is provided for each threat following the table

Table 8-1: All Threats to Security Countered

Item	Threat Name	Threat Description	Security Objective
1.	T.Misuse	A TOE resource may be compromised as a result of an authorized administrator of the TOE not having the ability to notice potential security violations by authorized or unauthorized users. Therefore, limiting their ability to identify and take action against a possible security breach.	5-O.Audit E7-OE.Time
2.	T.Bypass	An attacker may attempt to bypass TOE security functions to gain unauthorized access to TSF through the local machine or network interfaces.	6-O.AuditProtect 9-O.PartialNonBypass 10-O.PartialSelfProtection 11-O.PartialProtectComm E3-OE.AuditProtect E5-OE.PartialProtect E6-OE.PartialProtectComm N2-ON.NoUntrusted N5-ON.Physical
3.	T.Mismanage	Authorized administrators may make errors in the installation and management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	2-O.Admin 12-O.Roles E1-OE.Admin N1-ON.Install N3-ON.Operations N4-ON.Person
4.	T.ResourceMisuse	Unauthorized accesses and activity indicative of misuse may occur on IT Environment resources that the TOE monitors and go undetected.	3-O.Alert

Item	Threat Name	Threat Description	Security Objective
5.	T.Privilege	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	1-O.Access 4-O.Attributes 7-O.Collect_I&A 8-O.IDAuth E2-OE.Attributes E4-OE.IDAuth N2-ON.NoUntrusted N5-ON.Physical N6-ON.ProtectAuth
6.	T.Tamper	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted) on the host machines.	6-O.AuditProtect 9-O.PartialNonBypass 10-O.PartialSelfProtection 11-O.PartialProtectComm E3-OE.AuditProtect E5-OE.PartialProtect E6-OE.PartialProtectComm N2-ON.NoUntrusted N5-ON.Physical
7.	T.Transmit	An attacker may attempt to view or intercept and modify TSF data while the data is being transmitted between the applications of distributed TOE components or between the TOE and its users.	11-O.PartialProtectComm E6-OE.PartialProtectComm

1. T.Misuse: A TOE resource may be compromised as a result of an authorized administrator of the TOE not having the ability to notice potential security violations by authorized or unauthorized users. Therefore, limiting their ability to identify and take action against a possible security breach. T.Misuse is countered by:

- O.Audit: The TOE will provide the capability to detect, create, and selectively view records of security relevant events. *This objective counters this threat by providing the capability to detect, create, and selectively view records of security relevant events*.
- OE.Time: The underlying Operating System (OS) must provide reliable time stamps. *This objective counters this threat by providing the capability to place audit trails into chronological order to help the administrator determine a sequence of events.*

2. T.Bypass: An attacker may attempt to bypass TOE security functions to gain unauthorized access to TSF through the local machine or network interfaces. T.Bypass is countered by:

- O.AuditProtect: The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed. *This*

objective counters this threat by ensuring that the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.

- O.PartialNonBypass: The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed. *This objective addresses this threat by ensuring that the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed.*
- O.PartialSelfProtection: The TSF must maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. *This objective addresses this threat by ensuring that the TSF maintains a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.*
- O.PartialProtectComm: The TOE, in conjunction with the IT Environment, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents. *This objective addresses this threat by ensuring that the TOE, in conjunction with the IT Environment, provides a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.*
- OE.PartialProtectComm: The IT Environment, in conjunction with the TOE, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components. *This objective addresses this threat by ensuring that the IT Environment, in conjunction with the TOE, provides a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.*
- OE.AuditProtect: The IT Environment must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces. *This objective addresses this threat by ensuring that the IT Environment must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces.*
- OE.PartialProtect: The IT Environment must protect itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control. *This objective addresses this threat by ensuring that the IT Environment protects itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control.*
- ON.NoUntrusted: The administrator must ensure that there is no untrusted software on the systems that host the Unicenter NSM components. *This objective addresses this threat by ensuring that the administrator ensures that there is no untrusted software on the systems that host the Unicenter NSM components.*
- ON.Physical: Those responsible for the TOE must ensure that the TOE, including those components that are critical to the security policy (e.g., the NSM Security

component shown in Figure 2-1), is protected from any physical attack. *This objective provides for the protection of the TOE against physical attacks.*

3. T.Mismanage: Authorized administrators may make errors in the installation and management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. T.Mismanage is countered by:

- O.Admin: The TOE must include a set of functions that allow effective management of its functions and data. *This objective addresses this threat by ensuring that TSF is performing the security management functions.*
- O.Roles: The TOE must support multiple roles. *This objective addresses this threat by ensuring that the TSF maintains roles and associates users with the roles.*
- OE.Admin: The IT Environment must include a set of functions that allow effective management of user attributes required to support TOE functionality. *This objective addresses this threat by ensuring that the IT Environment includes a set of functions that manage the user attributes required to support TOE functionality.*
- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. *This objective provides for secure installation and configuration of the TOE*.
- ON.Operations: The TOE must be managed and operated in a secure manner as outlined in the supplied guidance. *This objective provides for guidance documentation that explains how to securely manage the TOE*.
- ON.Person: Personnel working as authorized administrators must be carefully selected and trained for proper operation of the system. *This objective provides for qualified and trained authorized administrators to manage the TOE*.

4. T.ResourceMisuse: Unauthorized accesses and activity indicative of misuse may occur on IT Environment resources that the TOE monitors and go undetected. T.ResourceMisuse is countered by:

- O.Alert: The TOE must collect information about events and send notification upon the detection of a potential security violation based on the rules and parameters specified by the user. *This objective addresses this threat by generating alerts and notifying the user to the alerts based on the options set by the user*.

5. T.Privilege: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. T.Privilege is countered by:

- O.Access: The TOE must provide its authorized users with the means of managing, controlling and limiting access to the objects and resources they are responsible for, on the basis of user roles and in accordance with the set of rules defined by the Security Functional Policies. *This objective counters this threat by providing access controls that limit the actions an individual is authorized to perform*.
- O.Attributes: The TOE must be able to maintain user security attributes. *This objective counters this threat by requiring the TOE to maintain user security*

attributes that are used to determine whether users have appropriate access privileges.

- O.Collect_I&A: The TOE must provide the ability to collect the identification and/or authentication information, from users attempting to access restricted TOE components, functions and data through the TOE's own interfaces. *This objective counters this threat by providing the ability to collect the identification and authentication information, from users attempting to access restricted TOE components and functions through the MCC GUI with support from the IT Environment for the I&A decision and access control decisions enforced by the NSM Security based on the identity information.*
- O.IDAuth: The TOE must be able to identify and authenticate users attempting to access restricted TOE components and functions. *This objective provides for identification and authentication of users when attempting access to restricted TOE components and functions*.
- OE.Attributes: The IT Environment must be able to maintain user security attributes. *This objective addresses this threat by maintaining user security attributes with IT Environment services such as RDBMS and OS components.*
- OE.IDAuth: The IT Environment must provide identification and authentication mechanisms for UMP Users, MCC Users, Local Users and Performance Users prior to allowing any other TSF-mediated actions on behalf of that user. *This objective addresses this threat by providing identification and authentication mechanisms prior to allowing any other TSF-mediated actions on behalf of that user*.
- ON.NoUntrusted: The administrator must ensure that there are no untrusted users on the systems that host the Unicenter NSM components. *This objective provides for the protection of the TOE from untrusted users.*
- ON.Physical: Those responsible for the TOE must ensure that the TOE, including those components that are critical to the security policy (e.g., the NSM Security component shown in Figure 2-1) is protected from any physical attack. *This objective provides for the protection of the TOE against physical attacks.*
- ON.ProtectAuth: Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons. *This objective provides for authorized users not sharing their passwords with others.*

6. T.Tamper: A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted) on the host machines. T.Tamper is countered by:

- O.AuditProtect: The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed. *This objective counters this threat by ensuring that the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.*
- O.PartialNonBypass: The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed. *This objective addresses this threat by ensuring that the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed.*

- O.PartialSelfProtection: The TSF must maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. *This objective addresses this threat by ensuring that the TSF maintains a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.*

- O.PartialProtectComm: The TOE, in conjunction with the IT Environment, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents. *This objective addresses this threat by ensuring that the TOE, in conjunction with the IT Environment, provides a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.*

- OE.PartialProtectComm: The IT Environment, in conjunction with the TOE, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents. *This objective addresses this threat by ensuring that the IT Environment, in conjunction with the TOE, provides a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.*

- OE.PartialProtect: The IT Environment must protect itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control. *This objective addresses this threat by ensuring that the IT Environment protects itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control.*

- OE.AuditProtect: The IT Environment must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces. *This objective addresses this threat by ensuring that the IT Environment provides the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces.*

- ON.NoUntrusted: The administrator must ensure that there is no untrusted software on the systems that host the Unicenter NSM components. *This objective addresses this threat by ensuring that the administrator ensures that there is no untrusted software on the systems that host the Unicenter NSM components.*

- ON.Physical: Those responsible for the TOE must ensure that the TOE, including those components that are critical to the security policy (e.g., the NSM Security component shown in Figure 2-1), is protected from any physical attack. *This objective provides for the protection of the TOE against physical attacks.*

7. T.Transmit: An attacker may attempt to view or intercept and modify TSF data while the data is being transmitted between the applications of distributed TOE components or between the TOE and its users.T.Transmit is countered by:

- O.PartialProtectComm: The TOE, in conjunction with the IT Environment, must provide a trusted communications path which provides for the protection of the

data from modification or disclosure while being exchanged between TOE components and agents. *This objective addresses this threat by ensuring that the TOE, in conjunction with the IT Environment, provides a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.*

- OE.PartialProtectComm: The IT Environment, in conjunction with the TOE, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents. *This objective addresses this threat by ensuring that the IT Environment, in conjunction with the TOE, provides a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.*

Note: The table below is provided to show completeness by demonstrating all security objectives for the TOE map to at least one threat.

Table 8-2: Reverse Mapping of TOE Security Objectives to Threats

Item	Objective	Threat
1.	O.Access	5-T.Privilege
2.	O.Admin	3-T.Mismanage
3.	O.Alert	4-T.ResourceMisuse
4.	O.Attributes	5-T.Privilege
5.	O.Audit	1-T.Misuse
6.	O.AuditProtect	2-T.Bypass 6-T.Tamper
7.	O.Collect_I&A	5-T.Privilege
8.	O.IDAuth	5-T.Privilege
9.	O.PartialNonBypass	2-T.Bypass 6-T.Tamper
10.	O.PartialSelfProtection	2-T.Bypass 6-T.Tamper
11.	O.PartialProtectComm	2-T.Bypass 6-T.Tamper 7-T.Transmit
12.	O.Roles	3-T.Mismanage

8.1.2 Assumptions

Table 8-3: shows that all of the secure usage assumptions are addressed by either security objectives for the IT Environment or Non-IT security objectives. Rationale for each assumption is provided below the table.

Table 8-3: All Assumptions Addressed

Item	Name	Assumption	Objective
1	A.Admin	It is assumed that the administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.	N1-ON.Install N3-ON.Operations
2	A.Manage	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.	N4-ON.Person
3	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the systems that host the Unicenter NSM components.	N2-ON.NoUntrusted
4	A.Physical	It is assumed that the TOE, including its components critical to the security policy enforcement, will be protected from unauthorized physical access and from unauthorized physical modification.	N5-ON.Physical
5	A.Users	It is assumed that users will protect their authentication data.	N6-ON.ProtectAuth

1. A.Admin: It is assumed that the administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation. A.Admin is covered by:

- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. *This objective provides for secure installation and configuration of the TOE.*
- ON.Operations: The TOE must be managed and operated in a secure manner as outlined in the supplied guidance. The procedures provide guidance to the administrator on how to securely operate the TOE. *This objective provides for operational procedures to be in place.*

2. A.Manage: It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security. A.Manage is covered by:

- ON.Person: Personnel working as authorized administrators must be carefully selected and trained for proper operation of the system. *This objective provides for competent personnel to administer the TOE*.

3. A.NoUntrusted: It is assumed that there will be no untrusted users and no untrusted software on the systems that host Unicenter NSM components. A.NoUntrusted is covered by:

- ON.NoUntrusted: The administrator must ensure that there are no untrusted users and no untrusted software on the systems that host the Unicenter NSM components. *This objective provides for the protection of the TOE from untrusted software and users.*

4. A.Physical: It is assumed that the TOE, including its components critical to the security policy enforcement, will be protected from unauthorized physical access and from unauthorized physical modification. A.Physical is covered by:

- ON.Physical: Those responsible for the TOE must ensure that the TOE, including those components that are critical to the security policy (e.g., the NSM Security component shown in Figure 2-1), is protected from any physical attack. *This objective provides for the physical protection of the TOE*.

5. A.Users: It is assumed that users will protect their authentication data. A.Users is covered by:

- ON.ProtectAuth: Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons. *This objective provides for users protecting their authentication data.*

Note: The table below is provided to show completeness by demonstrating all security objectives for the environment map to at least one assumption or threat.

Table 8-4: Reverse Mapping of Security Objectives for the Environment to Assumptions/Threats

Item	Security Objective for Environment	Assumption/Threat
E1	OE.Admin	3-T.Mismanage
E2	OE.Attributes	5-T.Privilege
E3	OE.AuditProtect	2-T.Bypass 6-T.Tamper
E4	OE.IDAuth	T.Privilege
E5	OE.PartialProtect	2-T.Bypass 6-T.Tamper
E6	OE.PartialProtectComm	2-T.Bypass 6-T.Tamper 7-T.Transmit
E7	OE.Time	1-T.Misuse
N1	ON.Install	3-T.Mismanage
N2	ON.NoUntrusted	2-T.Bypass 5-T.Privilege 6-T.Tamper
N3	ON.Operations	3-T.Mismanage
N4	ON.Person	3-T.Mismanage

Item	Security Objective for Environment	Assumption/Threat
N5	ON.Physical	2-T.Bypass 5-T.Privilege 6-T.Tamper
N6	ON.ProtectAuth	5-T.Privilege

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 Functional Requirements

Table 8-5 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included below the table.

Table 8-5: All Objectives Met by Functional Components

Item	Objective	Objective Description	Security Functional Requirement
1.	O.Access	The TOE must provide its authorized users with the means of managing, controlling, and limiting access to the objects and resources they are responsible for, on the basis of user roles and in accordance with the set of rules defined by the Security Functional Policies.	14-FMT_MTD.1 Management of TSF data 15-FMT_SMF.1-1 Specification of Management Functions 3-FAU_SAR.2 Restricted audit review
2.	O.Admin	The TOE must include a set of functions that allow effective management of its functions and data.	15-FMT_SMF.1-1 Specification of Management Functions
3.	O.Alert	The TOE must collect information about events and send notification upon the detection of a potential security violation based on the rules and parameters specified by the user.	6-FAU_ARP_EXP_TOE.1 Alerts on event data
4.	O.Attributes	The TOE must be able to maintain user security attributes.	7-FIA_ATD.1-1 User attribute definition [UMP Users] 8-FIA_ATD.1-2 User attribute definition [MCC Users] 9-FIA_ATD.1-3 User attribute definition [Local Users] 10-FIA_ATD.1-4 User attribute definition [Performance Users]
5.	O.Audit	The TOE will provide the capability to detect, create, and selectively view records of security relevant events.	1-FAU_GEN.1 Audit data generation 2-FAU_SAR.1 Audit review 4-FAU_SAR.3 Selectable audit review

Item	Objective	Objective Description	Security Functional Requirement
6.	O.AuditProtect	The TOE must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces.	5-FAU_STG_EXP_TOE.1 Partial protected audit trail storage: TOE 3-FAU_SAR.2 Restricted audit review
7.	O.Collect_I&A	The TOE must provide the ability to collect the identification and/or authentication information, from users attempting to access restricted TOE components, functions and data through the TOE's own interfaces.	13-FIA_UAU_EXP_TOE.5 Multiple authentication mechanisms: TOE
8.	O.IDAuth	The TOE must be able to identify and authenticate users attempting to access restricted TOE components and functions.	11-FIA_UID.1 Timing of identification 12-FIA_UAU.1 Timing of authentication
9.	O.PartialNonBypass	The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed.	17-FPT_RVM_EXP_TOE.1 Partial Non-bypassability of the TSP: TOE
10.	O.PartialSelfProtection	The TSF must maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.	18-FPT_SEP_EXP_TOE.1 Partial TSF domain separation: TOE
11.	O.PartialProtectComm	The TOE, in conjunction with the IT Environment, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents.	20-FTP_ITR_EXP_TOE.1 Partial Intra-TSF trusted channel among distributed TOE components: TOE
12.	O.Roles	The TOE must support multiple roles.	16-FMT_SMR.1 Security roles

1. O.Access: The TOE must provide its authorized users with the means of managing, controlling, and limiting access to the objects and resources they are responsible for, on the basis of user roles and in accordance with the set of rules defined by the Security Functional Policies. O.Access is addressed by:

- FMT_MTD.1 Management of TSF data: TOE, which specifies the management of TSF data according to assigned roles. This includes requirements implemented by access control policies for the TSF data (refer to Table 5-6).
- FMT_SMF.1-1 Specification of Management Functions, which specifies the security management functions that include the operations listed in Table 5-6 and secure audit review.
- FAU_SAR.2 Restricted audit review, which requires that the TSF prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

2. O.Admin: The TOE must include a set of functions that allow effective management of its functions and data. O.Admin is addressed by:

- FMT_SMF.1-1 Specification of Management Functions, which specifies the security management functions that include the operations listed in Table 5-6 and secure audit review.

3. O.Alert: The TOE must collect information about events and send notification upon the detection of a potential security violation based on the rules and parameters specified by the user. O.Alert is addressed by:

- FAU_ARP_EXP.1 Alerts on event data, which requires the TSF to collect event data, to apply a set of rules in monitoring the event data and based on the rules send notification in a method and form specified by the user.

4. O.Attributes: The TOE must be able to maintain user security attributes. O.Attributes is addressed by:

- FIA_ATD.1-1 User attribute definition [UMP Users], which requires that the TSF maintain security attributes for UMP Users.
- FIA_ATD.1-2 User attribute definition [MCC Users], which requires that the TSF maintain security attributes for MCC Users.
- FIA_ATD.1-3 User attribute definition [Local Users], which requires that the TSF maintain security attributes for Local Users.
- FIA_ATD.1-4 User attribute definition [Performance Users], which requires that the TSF maintain security attributes for Performance Users.

5. O.Audit: The TOE will provide the capability to detect, create, and selectively view records of security relevant events:

- FAU_GEN.1 Audit data generation, which require that the TSF be able to generate an audit record of the following auditable events:
    - Start-up and shutdown of the audit functions
    - Events listed in Table 5-2: Auditable Events

  Where the audit record is made up of the following information:
    - Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.
    - Information based on event typed as listed in Table 5-2: Auditable Events
- FAU_SAR.1 Audit review, which requires that the TSF provide administrators and users with privileges to read audit with the capability to read from the audit records.
- FAU_SAR.3 Selectable audit review, which requires that the TSF provide the ability to perform searches, sorting, and ordering of audit data based on fields shown in column 4 of Table 5-3: Auditable Review.

6. O.AuditProtect: The TOE must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces. O.AuditProtect is addressed by:

- FAU_STG_EXP_TOE.1 Partial protected audit trail storage: TOE, which requires that the TSF protect the stored audit records in the audit trail from unauthorized deletion and prevent unauthorized modifications to the records in the audit trail initiated through its own TSFI.
- FAU_SAR.2 Restricted audit review, which requires that the TSF prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

7. O.Collect_I&A: The TOE must provide the ability to collect the identification and/or authentication information, from users attempting to access restricted TOE components, functions and data through the TOE's own interfaces. O.Collect_I&A is addressed by:

- FIA_UAU_EXP_TOE.5 Multiple authentication mechanisms: TOE, where the TSF requires each user to be successfully authenticated by invoking authentication mechanisms in the IT Environment before allowing any other TSF-mediated actions on behalf of that user. Each user's claimed identity and authentication information is collected and is then authenticated in multiple authentication mechanisms as listed in Section 5.2 under the heading FIA_UAU_EXP_TOE.5.

8. O.IDAuth: The TOE must be able to identify and authenticate users attempting to access restricted TOE components and functions. O.IDAuth is addressed by:

- FIA_UID.1 Timing of identification, which require that the TSF allow capabilities found in Table 5-4 on behalf of the user to be performed before the user is identified.
- FIA_UAU.1 Timing of authentication, which requires that the TSF shall allow capabilities found in Table 5-5 on behalf of the user to be performed before the user is authenticated.

9. O.PartialNonBypass: The TOE must ensure the TOE's security functional policy is invoked and succeeds before allowing another TOE function to proceed. O.PartialNonBypass is addressed by:

- FPT_RVM_EXP_TOE.1 Partial Non-bypassability of the TSP: TOE, which requires that TSP enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

10. O.PartialSelfProtection: The TSF must maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. O.PartialSelfProtection is addressed by:

- FPT_SEP_EXP_TOE.1 Partial TSF domain separation: TOE, which requires that the TSF provide a domain that partially protects itself from interference and tampering by untrusted users. This requires that the TOE provide partial protection to maintain separation between code executing on behalf of different users.

11. O.PartialProtectComm: The TOE must provide a trusted communication path between the endpoints which aids in identifying the endpoints and provides protection from modification or disclosure of the data being exchanged between the endpoints using encryption and certificate services provided by the TOE's environment. O.PartialProtectComm is addressed by:

- FTP_ITR_EXP_TOE.1 Partial Intra-TSF trusted channel among distributed TOE components, which requires the TSF to provide a trusted communication channel among the distributed components of the TOE using the encryption and certificate services required in the IT Environment.

12. O.Roles: The TOE must support multiple roles. O.Roles is addressed by:

- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple roles.

Note: The table below has been provided for completeness to show that all security functional requirements map to at least one TOE security objective.

Table 8-6: Reverse mapping of TOE SFRs to TOE Security Objectives

Item	Component	TOE Security Objective
1	FAU_GEN.1	5-O.Audit
2	FAU_SAR.1	5-O.Audit
3	FAU_SAR.2	1-O.Access 6-O.AuditProtect
4	FAU_SAR.3	5-O.Audit
5	FAU_STG_EXP_TOE.1	6-O.AuditProtect
6	FAU_ARP_EXP.1	3-O.Alert
7	FIA_ATD.1-1	4-O.Attributes
8	FIA_ATD.1-2	4-O.Attributes
9	FIA_ATD.1-3	4-O.Attributes
10	FIA_ATD.1-4	4-O.Attributes
11	FIA_UID.1	8-O.IDAuth
12	FIA_UAU.1	8-O.IDAuth
13	FIA_UAU_EXP_TOE.5	7-O.Collect_I&A
14	FMT_MTD.1	1-O.Access
15	FMT_SMF.1-1	1-O.Access 2-O.Admin
16	FMT_SMR.1	12-O.Roles
17	FPT_RVM_EXP_TOE.1	9-O.PartialNonBypass
18	FPT_SEP_EXP_TOE.1	10-O.PartialSelfProtection
19	FTP_ITR_EXP_TOE.1	11-O.PartialProtectComm

8.2.2 Requirements for the IT Environment

Table 8-7 shows that all of the security objectives for the IT Environment are satisfied. Rationale for each objective is included below the table.

Table 8-7: All Objectives for the IT Environment map to Requirements in the IT Environment

Item	Objective	Objective Description	Requirement for the IT Environment
E1	OE.Admin	The IT Environment must include a set of functions that allow effective management of user attributes required to support TOE functionality.	28-FMT_SMF.1-2 Specification of Management Functions
E2	OE.Attributes	The IT Environment must be able to maintain user security attributes.	21-FIA_ATD.1-5 User attribute definition [UMP Users] 22-FIA_ATD.1-6 User attribute definition [MCC Users] 23-FIA_ATD.1-7 User attribute definition [Local Users] 24-FIA_ATD.1-8 User attribute definition [Performance Users]
E3	OE.AuditProtect	The IT Environment must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces.	20-FAU_STG_EXP_ENV.1 Partial protected audit trail storage: IT Environment
E4	OE.IDAuth	The IT Environment must provide identification and authentication mechanisms for UMP Users, MCC Users, Local Users, and Performance Users prior to allowing any other TSF-mediated actions on behalf of that user.	25-FIA_UID.2 User identification before any action 26-FIA_UAU.2 User authentication before any action 27-FIA_UAU_EXP_ENV.5 Multiple authentication mechanisms: IT Environment
E5	OE.PartialProtect	The IT Environment must protect itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control.	29-FPT_RVM_EXP_ENV.1 Partial Non-bypassability of the TSP: IT Environment 30-FPT_SEP_EXP_ENV.1 Partial TSF domain separation: IT Environment

Item	Objective	Objective Description	Requirement for the IT Environment
E6	OE.PartialProtect Comm	The IT Environment, in conjunction with the TOE, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.	32-FTP_ITR_EXP_ENV.1 Partial Intra-TSF trusted channel among distributed TOE components: IT Environment
E7	OE.Time	The underlying Operating System (OS) must provide reliable time stamps.	31-FPT_STM.1 Reliable time stamps

E1. OE.Admin: The IT Environment must include a set of functions that allow effective management of user attributes required to support TOE functionality. OE.Admin is addressed by:

- FMT_SMF.1-2 Specification of Management Functions, which requires that the IT Environment shall be capable of performing the security management functions as specified in Table 5-8.

E2. OE.Attributes: The IT Environment must be able to maintain user security attributes.

- FIA_ATD.1-5 User attribute definition [UMP Users], which requires that the IT Environment maintain security attributes for UMP Users.
- FIA_ATD.1-6 User attribute definition [MCC Users], which requires that the IT Environment maintain security attributes for MCC Users.
- FIA_ATD.1-7 User attribute definition [Local Users], which requires that the IT Environment maintain security attributes for Local Users.
- FIA_ATD.1-8 User attribute definition [Performance Users], which requires that the IT Environment maintain security attributes for Performance Users.

E3. OE.AuditProtect: The IT Environment must provide the capability to protect audit information from unauthorized deletion, modification, and viewing through its own interfaces. OE.AuditProtect is addressed by:

- FAU_STG_EXP_ENV.1 Partial protected audit trail storage: IT Environment, which requires that the IT Environment protect the stored audit records in the audit trail from unauthorized deletion and prevent unauthorized modifications to the records in the audit trail initiated through its own TSFI.

E4. OE.IDAuth: The IT Environment must provide identification and authentication mechanisms for UMP Users, MCC Users, Local Users, and Performance Users prior to allowing any other TSF-mediated actions on behalf of that user. OE.IDAuth is addressed by:

- FIA_UID.2 User identification before any action, which require that the IT Environment requires each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.2 User authentication before any action, which require that the IT Environment requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

- FIA_UAU_EXP_ENV.5 Multiple authentication mechanisms: IT Environment, which require that the IT Environment requires each user to be successfully authenticated by invoking authentication mechanisms in the IT Environment before allowing any other TSF-mediated actions on behalf of that user. The IT Environment also ensures that each user's claimed identity and authentication information is collected and is then authenticated mechanism rules listed in Section 5.4 under the heading FIA_UAU_EXP_ENV.5.

E5. OE.PartialProtect: The IT Environment must protect itself and the TOE from external interference or tampering, including unauthorized modifications and access to its functions and data within the TOE and/or, through the IT Environment's interfaces within its scope of control. OE.PartialProtect is addressed by:

- FPT_RVM_EXP_ENV.1 Partial Non-bypassability of the TSP: IT Environment, which requires that the OS's Security Policy is invoked and succeeds before a security-relevant function is allowed to proceed.
- FPT_SEP_EXP_ENV.1 Partial TSF domain separation: IT Environment, which requires the IT Environment to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the OS's Interface. The IT Environment must enforce separation between security domains of subjects in the OS's Scope of Control.

E6. OE.PartialProtectComm: The IT Environment, in conjunction with the TOE, must provide a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents. OE.PartialProtectComm is addressed by:

- FTP_ITR_EXP_ENV.1 Partial Intra-TSF trusted channel among distributed TOE components: IT Environment which requires the IT Environment to provide a communication channel among its distributed component applications that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure using the encryption and certificate services from the IT Environment. This trusted channel is used for all communication among its distributed application components.

E7. OE.Time The underlying Operating System (OS) must provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which require that time stamps be provided by the IT Environment.

Note: The table below has been provided for completeness to show that all IT security functional requirements map to at least one IT Environment security objective.

Table 8-8: Reverse Mapping of Environment SFRs to Environment Security Objectives

Item.	Environment SFRs	Environment Security Objectives
20	FAU_STG_EXP_ENV.1	E3-OE.AuditProtect
21	FIA_ATD.1-5	E2-OE.Attributes

Item.	Environment SFRs	Environment Security Objectives
22	FIA_ATD.1-6	E2-OE.Attributes
23	FIA_ATD.1-7	E2-OE.Attributes
24	FIA_ATD.1-8	E2-OE.Attributes
25	FIA_UID.2	E4-OE.IDAuth
26	FIA_UAU.2	E4-OE.IDAuth
27	FIA_UAU_EXP_ENV.5	E4-OE.IDAuth
28	FMT_SMF.1-2	E1-OE.Admin
29	FPT_RVM_EXP_ENV.1	E5-OE.PartialProtect
30	FPT_SEP_EXP_ENV.1	E5-OE.PartialProtect
31	FPT_STM.1	E7-OE.Time
32	FTP_ITR_EXP_ENV.1	E6-OE.PartialProtectComm

8.2.3 Dependencies

Table 8-9 and Table 8-10 show that all the dependencies between the functional requirements are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT Environment an “E” will be next to the reference number.

FAU_ARP_EXP.1 is modeled on FAU_ARP.1 and FAU_SAA.1. While FAU_ARP.1 and FAU_SAA.1 have dependencies on audit requirements, the FAU_ARP_EXP.1 includes only the collection aspect for the event data to which it refers; therefore, it has no dependencies.

Table 8-9: TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	31(E)
2	FAU_SAR.1	Audit review	FAU_GEN.1	1
3	FAU_SAR.2	Restricted audit review	FAU_SAR.1	2
4	FAU_SAR.3	Selectable audit review	FAU_SAR.1	2
5	FAU_STG_EXP_TOE.1	Partial protected audit trail storage: TOE	FAU_GEN.1 FAU_STG_EXP_ENV.1	1 32(E)
6	FAU_ARP_EXP.1	Alerts on event data	None	None
7	FIA_ATD.1-1	User attribute definition [UMP Users]	None	None
8	FIA_ATD.1-2	User attribute definition [MCC Users]	None	None
9	FIA_ATD.1-3	User attribute definition [Local Users]	None	None
10	FIA_ATD.1-4	User attribute definition [Performance Users]	None	None
11	FIA_UID.1	Timing of identification	None	None
12	FIA_UAU.1	Timing of authentication	FIA_UID.1	11(H)
13	FIA_UAU_EXP_TOE.5	Multiple authentication mechanisms: TOE	FIA_UAU_EXP_ENV.5	27(E)
14	FMT_MTD.1	Management of TSF data: TOE	FMT_SMF.1 FMT_SMR.1	15 16
15	FMT_SMF.1-1	Specification of Management Functions	None	None
16	FMT_SMR.1	Security roles	FIA_UID.1	10
17	FPT_RVM_EXP_TOE.1	Partial Non-bypassability of the TSP: TOE	FPT_RVM_EXP_ENV.1	29(E)
18	FPT_SEP_EXP_TOE.1	Partial TSF domain separation: TOE	FPT_SEP_EXP_ENV.1	30(E)
19	FTP_ITR_EXP_TOE.1	Partial Intra-TSF trusted channel among distributed TOE components: TOE	FTP_ITR_EXP_ENV.1	32(E)

Table 8-10: IT Environment Dependencies are Satisfied

No.	Component	Component Name	Dependencies	Reference
20	FAU_STG_EXP_ENV.1	Partial protected audit trail storage: IT Environment	FAU_STG_EXP_TOE.1	5
21	FIA_ATD.1-5	User attribute definition [UMP Users]	None	None
22	FIA_ATD.1-6	User attribute definition [MCC Users]	None	None

No.	Component	Component Name	Dependencies	Reference
23	FIA_ATD.1-7	User attribute definition [Local Users]	None	None
24	FIA_ATD.1-8	User attribute definition [Performance Users]	None	None
25	FIA_UID.2	User identification before any action	None	None
26	FIA_UAU.2	User authentication before any action	FIA_UID.2	25
27	FIA_UAU_EXP_ENV.5	Multiple authentication mechanisms: IT Environment	FIA_UAU_EXP_TOE.5	13
28	FMT_SMF.1-2	Specification of Management Functions	None	None
29	FPT_RVM_EXP_ENV.1	Partial Non-bypassability of the TSP: IT Environment	FPT_RVM_EXP_TOE.1	17
30	FPT_SEP_EXP_ENV.1	Partial TSF domain separation: IT Environment	FPT_SEP_EXP_TOE.1	18
31	FPT_STM.1	Reliable time stamps	None	None
32	FTP_ITR_EXP_ENV.1	Partial Intra-TSF trusted channel among distributed TOE components: IT Environment	FTP_ITR_EXP_TOE.1	19

8.2.4 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements.

FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3 ensure that audit records are generated and are restricted to users with allowed privileges to review the audit trail and have the ability to search, sort and order. FAU_STG_EXP_TOE.1 works in concert with FAU_STG_EXP_ENV.1 to ensure that the audit trail is protected from unauthorized deletion.

FAU_ARP_EXP.1 ensures that the TSF applies a set of rules in monitoring the event data and based on the rules sends notification in a method and form specified by the user.

FIA_ATD.1-1, FIA_ATD.1-2, FIA_ATD.1-3, and FIA_ATD.1-4 specify the security attributes belonging to individual UMP, MCC, Local Users and Performance Users that are stored by the TOE. These operate in conjunction with FIA_ATD.1-5, FIA_ATD.1-6, FIA_ATD.1-7, and FIA_ATD.1-8, which specify the security attributes that are stored by the IT Environment. These combined requirements provide a complete picture of the security attributes needed to support the user operation of the TOE.

FIA_UAU_EXP_TOE.5 works in concert with FIA_UAU_EXP_ENV.5 to require that the MCC, UMP, Local Users and Performance Users authenticate using a password-based authentication either provided by the TOE or the IT Environment. FIA_UID.1 specifies what functions the TSF allows before identification while FIA_UAU.1 specifies what the TSF allows before authentication.

The management requirements (FMT_) are related to many of the mechanisms involved with other requirements. FMT_MTD.1 defines the requirements for management of TSF data representing the requirement for access control over the trusted data, including the TSF data which is used by other security requirements.

FMT_SMF.1 specifies the security management functions of the TSF. In many cases, other mechanisms will enforce the settings made through management functions. Installation mechanisms (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM.1) documents the management functions. The management roles are also defined in FMT_SMR.1.

FPT_RVM_EXP_TOE.1 works in concert with FPT_RVM_EXP_ENV.1 to make certain the TSP enforcement functions are invoked and succeed before any other functions within the TOE's Scope of Control are allowed to proceed.

FPT_SEP_EXP_TOE.1 works in concert with FPT_SEP_EXP_ENV.1 and relies partly on FMT_MTD.1 to provide protection against unauthorized subjects from gaining access to the TOE's administrative interface.

FTP_ITR_EXP_TOE.1 works in concert with FTP_ITR_EXP_ENV.1 to ensure that the TSF provides a trusted communication channel among the distributed TOE components.

8.2.5 Mutual Support Rationale

The requirements are mutually supportive.

Sections 8.2.1 and 8.2.2 show that all of the security objectives are satisfied and all of the security requirements trace to objectives.

Section 8.2.3 shows that all dependencies are satisfied.

Section 8.2.4 shows that the requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements.

Even when no dependency between these requirements is indicated, the security requirements support each other where necessary in the following ways:

- FPT_RVM_EXP_TOE.1 and FPT_RVM_EXP_ENV.1 prevent bypass of other security functional requirements.
- FPT_SEP_EXP_TOE.1 and FPT_SEP_EXP_ENV.1 prevent tampering with other security functional requirements.
- FMT_SMF.1 prevents de-activation of other security functional requirements.
- FAU_ARP_EXP.1 enables detection of attacks aimed at defeating other security functional requirements.

8.2.6 Explicitly Stated Requirements Rationale

FPT_RVM_EXP_TOE.1, FPT_SEP_EXP_TOE.1, FPT_RVM_EXP_ENV.1, FPT_SEP_EXP_ENV.1, FAU_STG_EXP_TOE.1 and FAU_STG_EXP_ENV.1 had to be explicitly stated because the TOE is a software-only TOE and therefore can only provide partial TOE self-protection while relying on the OS and hardware platforms to provide the

full protection. The approach used for these requirements is according to the NIAP policy requiring software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documented in: *'Consistency Instruction Manual For development of US Government Protection Profiles For use in Basic Robustness Environments, Release 3.0, 1 February 2005 '*.

FAU_STG_EXP_TOE.1 has a dependency of FAU_GEN.1 and its IT Environment counterpart, FAU_STG_EXP_ENV.1.

As with FPT_RVM.1, and FPT_SEP.1, on which they were based, the explicit requirements FPT_RVM_EXP_TOE.1, FPT_SEP_EXP_TOE.1, FPT_RVM_EXP_ENV.1, and FPT_SEP_EXP_ENV.1, have no dependencies other than their counterparts.

FAU_ARP_EXP.1 is modeled on FAU_ARP.1 and FAU_SAA.1. While these model SFRs have dependencies on audit requirements, this component includes the collection aspect for the event data it refers to, therefore there are no dependencies. FAU_ARP_EXP.1 had to be explicitly stated because a refinement of FAU_ARP.1 & FAU_SAA.1 would have narrowed the scope of the original SFRs. According to CCIMB RI #19, if the scope of the SFR is narrowed, then all iterations must be within the TOE boundary and meet the original scope of the SFR.

FTP_ITR_EXP_TOE.1 and FTP_ITR_EXP_ENV.1 are modeled on FTP_ITC.1 and similarly do not have any dependencies other than their namesake counterparts. FTP_ITR_EXP_TOE.1 indicates the portion of the trusted channel provided by the TOE. These SFRs are identified and described in the same manner as required for the FPT_RVM_EXP_TOE.1, FPT_SEP_EXP_TOE.1, FPT_RVM_EXP_ENV.1, and FPT_SEP_EXP_ENV.1 SFRs above.

FIA_UAU_EXP_TOE.5 and FIA_UAU_EXP_ENV.5 are modeled on FIA_UAU.5 and similarly does not have any dependencies. FIA_UAU_EXP_TOE.5 and FIA_UAU_EXP_ENV.5 is an explicit requirement created for the environment to reflect the IT services required by the environment to support the TOE Identification and Authentication. These SFRs are identified and described in the same manner as required for the FPT_RVM_EXP_TOE.1, FPT_SEP_EXP_TOE.1, FPT_RVM_EXP_ENV.1, and FPT_SEP_EXP_ENV.1 SFRs above.

8.2.7 Strength of Function Rationale

As stated in Sections 5.3 and 6.8, the mechanism defined in FIA_UAU_EXP_TOE.5 has a claim of SOF-Basic.

8.2.8 Assurance Requirements

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

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 IT Security Functions

Table 8-11 shows that the IT security functions in the TOE Summary Specification (TSS) address all of the TOE security functional requirements.

Table 8-11: Mapping of Functional Requirements to TOE Summary Specification

Item	Component	Component Name	Security Function	Rationale
1	FAU_GEN.1	Audit data generation	AUDIT	Specifies that the TOE generates audit records.
2	FAU_SAR.1	Audit review	AUDIT	Specifies that the TOE users are allowed to review the audit records.
3	FAU_SAR.2	Restricted audit review	AUDIT MANAGEMENT	AUDIT - Specifies that the TOE prohibits access to the audit records unless users have been granted explicit read-access. MANAGEMENT - Specifies the security management functions that are provided by the TOE and the management roles that are maintained
4	FAU_SAR.3	Selectable audit review	AUDIT	Specifies that the TOE users can search, sort and order the audit data when reviewing.
5	FAU_STG_EXP_TOE.1	Partial protected audit trail storage: TOE	PROT	Specifies that the TOE protects the audit trails from unauthorized deletion.
6	FAU_ARP_EXP.1	Alerts on event data	ALERTS	Specifies that the TOE generates and processes internal alerts and provides notifications based on the user specified rules and parameters.
7	FIA_ATD.1-1	User attribute definition [UMP Users]	ATTRIBUTE	Specifies that security attributes are maintained for each UMP User.
8	FIA_ATD.1-2	User attribute definition [MCC or Classic Interface users]	ATTRIBUTE	Specifies that security attributes are maintained for each MCC User.
9	FIA_ATD.1-3	User attribute definition [Local Users]	ATTRIBUTE	Specifies that security attributes are maintained for each Local User

Item	Component	Component Name	Security Function	Rationale
10	FIA_ATD.1-4	User attribute definition [Performance Users]	ATTRIBUTE	Specifies that security attributes are maintained for each Performance User
11	FIA_UID.1	Timing of identification	I&A	Specifies the functions that users are allowed to perform before identification.
12	FIA_UAU.1	Timing of authentication	I&A	Specifies the functions that users are allowed to perform before authentication.
13	FIA_UAU_EXP_TOE.5	Multiple authentication mechanisms: TOE	I&A	Specifies how the users must authenticate to the TOE using the TOE provided authentication mechanisms.
14	FMT_MTD.1	Management of TSF data: TOE	MANAGEMENT (AC) MANAGEMENT	MANAGEMENT (AC) - Specifies the access control policies for TSF data. MANAGEMENT - Specifies the security management functions that are provided by the TOE and the management roles that are maintained
15	FMT_SMF.1-1	Specification of Management Functions	MANAGEMENT	Specifies the security management functions that are provided by the TOE and the management roles that are maintained
16	FMT_SMR.1	Security roles	MANAGEMENT	Specifies the management roles maintained.
17	FPT_RVM_EXP_TOE.1	Partial Non-bypassability of the TSP: TOE	PROT	Specifies that the TSP enforcement functions are invoked and succeed before any other functions within the TOE's Scope of Control are allowed to proceed.
18	FPT_SEP_EXP_TOE.1	Partial TSF domain separation: TOE	PROT	Specifies that the TSF provides a domain that partially protects itself from interference and tampering by untrusted users.
19	FTP_ITR_EXP_TOE.1	Partial Intra-TSF trusted channel among distributed TOE components	TC	Specifies how the TSF provides a trusted communication channel among the distributed application components of the TOE

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in the following table.

Table 8-12: Assurance Measures Rationale

Item	Component	Evidence Requirements	Rationale
1	ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	CM Proof • Shows the CM system is being used. Configuration Item List(s) • is comprised of a list of the source code files and version numbers; • is comprised of a list of design documents with version numbers; • is comprised of test documents with version numbers; • user and administrator documentation with version numbers.
2	ADO_DEL.1	Delivery Procedures	Provides a description of all procedures that are necessary to maintain security when distributing TOE to the customer's site. Applicable across all phases of delivery from packaging, storage, distribution.
3	ADO_IGS.1	Installation, generation, and start-up procedures	Provides detailed instructions on how to install the TOE.
4	ADV_FSP.1	Functional Specification	Provides rationale that TSF is fully represented. A bi-directional mapping of security functions to guidance documentation. Describes the TSF interfaces and TOE functionality.
5	ADV_HLD.1	High-Level Design	Describes the TOE subsystems and their associated security functionality.
6	ADV_RCR.1	Representation Correspondence	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design.
7	AGD_ADM.1	Administrator Guidance	Describes how to administer the TOE securely.
8	AGD_USR.1	User Guidance	Not applicable since there are no untrusted users and all users are administrators.
9	ATE_COV.1	Test Coverage Analysis	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
10	ATE_FUN.1	Test Documentation	Test documentation includes test plans and procedures and expected and actual results.
11	ATE_IND.2	TOE for Testing	The TOE will be provided for testing.
12	AVA_SOF.1	SOF Analysis	Provides the analysis of the SOF claim stated.

Item	Component	Evidence Requirements	Rationale
13	AVA_VLA.1	Vulnerability Analysis	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP CLAIMS RATIONALE

Not applicable. There are no PP claims.

9 REFERENCES

Reference	Description
[ADMIN]	*Unicenter® Network & Systems Management Administrator Guide*, r11.1, 2006 CA International, Inc.*Unicenter® Network & Systems Management Administrator Guide,* r11.1, 2006, J014202E, CA, Inc.
[CC]	*Common Criteria for Information Technology Security Evaluation Parts 1-3*, CCIMB-2004-01-001, Version 2.2, January 2004*Common Criteria for Information Technology Security Evaluation,* CCIMB-2004-01-002, Version 2.2, January 2004.
[CEM]	*Common Methodology for Information Technology Security Evaluation*, CCIMB-2004-01-004, Version 2.2, January 2004
[IMPL]	*Unicenter® Network and Systems Management Implementation Guide*, r11.1, 2006 CA International, Inc.
[SYSPERF]	*Unicenter® Network & Systems Inside System Performance*, r11.1, 2006 CA International, Inc.
[UMPGS]	*Unicenter® Management Portal Getting Started Guide*, r11.1, 2006 CA International, Inc.
[BASIC]	*Consistency Instruction Manual For development of US Government Protection Profiles For use in Basic Robustness Environments*
[START]	*Unicenter® Network and Systems Management Getting Started Guide,* r11.1, J014202E, 2006 CA, Inc.