National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

CA Unicenter® Network and Systems Management, r11.1 SP1 CCV

Report Number: CCEVS-VR-VID10120-2008
Dated: May 9, 2008
Version: Version 0.9

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the CA Unicenter® Network and Systems Management, r11.1 SP1 CCV (Unicenter NSM r11.1 SP1 CCV), a product of CA, Islandia, NY 11749.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The TOE, CA Unicenter NSM, Version r11.1 SP1 CCV, is a software tool for the administration of enterprise IT Environments.

The TOE 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, and databases.

Unicenter NSM's components are modular and can be deployed on shared or distributed platforms.

The TOE's management capabilities provide the ability to identify resources throughout an enterprise and organize, monitor, and manage them. The user interfaces are either role-based or are restricted to users granted permission to use their functionality. Unicenter NSM uses visualization models to display resource information to the administrator. 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.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during April 2008 The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.2 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.2, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document CA Unicenter® Network and Systems Management, r11.1 SP1 CCV.

2. Identification

Target of Evaluation:	CA Unicenter® Network and Systems Management, r11.1 SP1 CCV
Evaluated Software:	CA Unicenter® Network and Systems Management, r11.1 SP1 CCV
Developer:	CA 1 CA Plaza Islandia, NY 11749
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Evaluators	Herbert Markle, Cygnacom Solutions
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

- **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 by 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 mostly GUI based interfaces, with the exception of a small number of additional CLIs. 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.

A summary of the SFRs for the TOE and IT environment are included in the following tables.

TOE Security Functional Requirements

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

IT Environment Security Functional Requirements

No.	SFR Component	SFR Component Name
1	FAU_STG_EXP_ENV.1	Partial protected audit trail storage: IT Environment
2	FIA_ATD.1-5	User attribute definition [UMP Users]
3	FIA_ATD.1-6	User attribute definition [MCC Users]
4	FIA_ATD.1-7	User attribute definition [Local Users]
5	FIA_ATD.1-8	User attribute definition [Performance Users]
6	FIA_UID.2	User identification before any action
7	FIA_UAU.2	User authentication before any action
8	FIA_UAU_EXP_ENV.5	Multiple authentication mechanisms: IT Environment
9	FMT_SMF.1-2	Specification of Management Functions
10	FPT_RVM_EXP_ENV.1	Partial Non-bypassability of the TSP: IT Environment
11	FPT_SEP_EXP_ENV.1	Partial TSF domain separation: IT Environment
12	FPT_STM.1	Reliable time stamps
13	FTP_ITR_EXP_ENV.1	Partial Intra-TSF trusted channel among distributed TOE components: IT Environment

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- An administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
- 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.
- There will be no untrusted users and no untrusted software on the systems that host the Unicenter NSM components.
- Appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
- Users will protect their authentication data.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. There are CA Unicenter NSM r11.1 SP1 CCV software components that 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. The evaluated TOE does not include the product components that are optionally installed. See Section 8 for details.
5. TOE depends on the IT environment for the following:
    - Physical Protection of TOE component host platforms that are critical to the security policy enforcement.
    - Support for secure communications for trusted channels (in conjunction with the TOE) among the TOE (Unicenter NSM) components.
    - Support for certificate-based mechanisms used in establishing the trusted channels.
    - Reliable time stamps from the platform.
    - File protection of TOE executables, configuration files, data, and audit logs.

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

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The TOE consists of the following components (refer to figures 1 and 2):

- User Interfaces [Yellow filled boxes]
    - 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
    - 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.
    - Classic Interface – The only Classic Interface applications required to support the evaluated configuration (in-scope) are:
        - EM Classic (WIN32 executables GUI)
        - secadmin (DOS CLI)
    - Performance Monitoring User Interfaces

      - provides GUI applications which are used to visualize, analyze, report, and configure performance and resource usage data. These applications are as follows:
        - Performance Scope
        - Performance Trend
        - Performance Chargeback
        - Performance Configuration

      - 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.
- NSM Security - provides the access control (NSM Security Policy) decision for the Manager components
- Managers
    - WorldView Manager (WV or WV Manager) – an abstraction between the MCC and UMP User interfaces and the MDB Managed Object data.
    - Distributed State Machine Manager (DSM or DSM Manager) - serves as the Unicenter NSM Agent Manager
    - Event Manager (EM) – used to categorize, log, and process events received from Event Agents throughout the IT Environment.
    - Alert Manager System (AMS or Alert Manager) tracks the most important events occurring in an enterprise (or a logical segment of an enterprise).
    - 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
- 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
    - Dashboard Services - provides the security functionality for Agent configuration to authorized MCC Users.
    - Web Reporting Services (WRS) - provides the administrators with the ability to customize reports on different aspects of the enterprise being managed.
- Performance Monitoring Components (PM)
    - Performance Domain Server component - holds all the performance configuration information for an entire domain and manages the Performance Distribution Servers within its domain.
    - Performance Distribution Server component - requests configuration data from the Performance Domain Server and delivers it to the Performance Agents
- Agents

- 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.
    - Historical Performance Agents.

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) [Blue Lines]
- CA International Common Communications Interface (CACCI, also referred to as CCI for short) [Orange Lines]
    - CCISSF transmits any data from components or products using CCI over a Secure Sockets Layer (SSL) connection.
- CA Messaging (CAM) [Pink Lines]
    - CAFT is a simple file transfer protocol (similar to FTP

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.

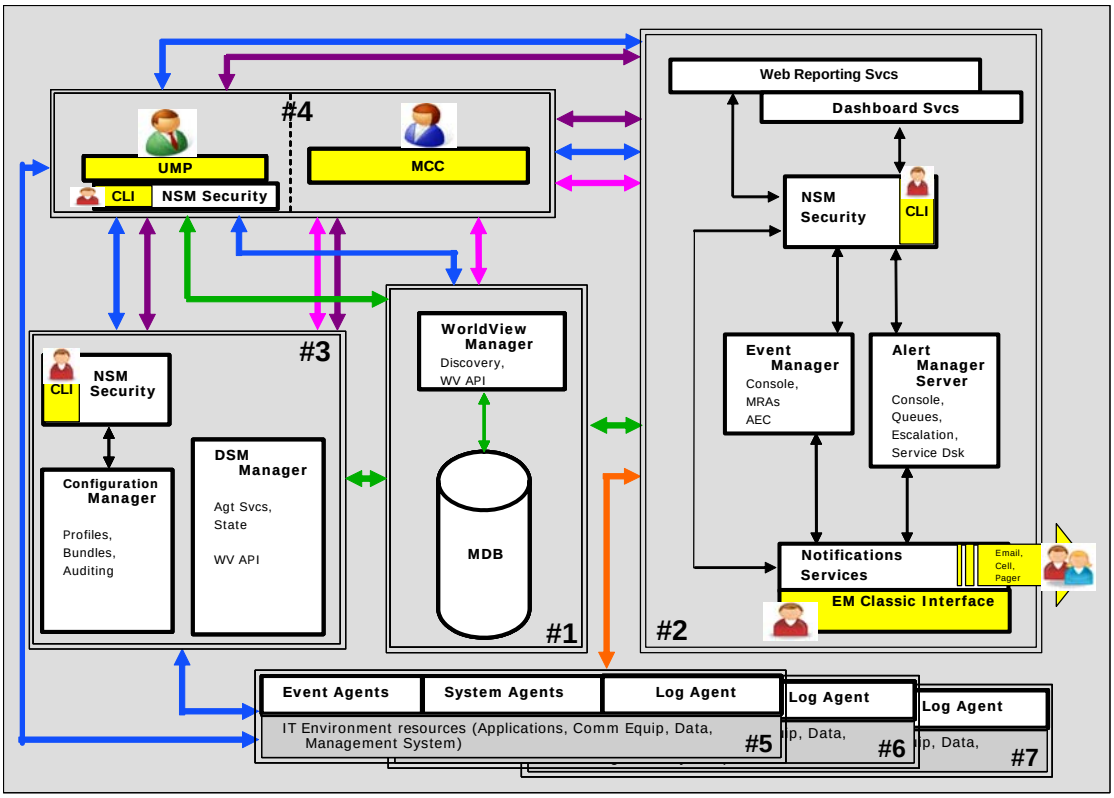

Figure 1 - TOE Boundary for Non Performance Monitoring Components

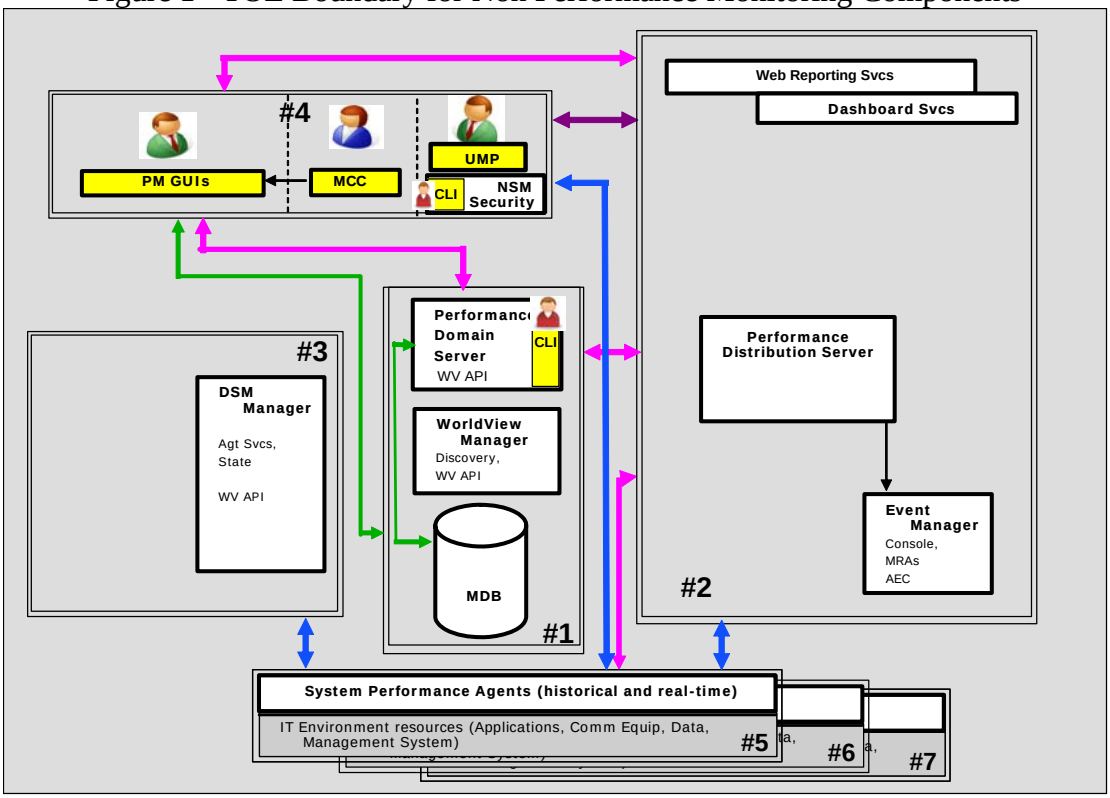

Figure 2 - TOE Boundary for Performance Monitoring Components only

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

CC Evaluation Evidence:

1. CA Unicenter® Network and Systems Management, Version r11.1 SP1 CCV Common Criteria Security Target, Version 2.7, April 24 2008.
2. Unicenter NSM r11.1 SP1 CCV Common Criteria Supplement to the Administrative Guidance, V1.0, March 20 2008
3. Common Criteria Installation Manual for Unicenter NSM r11.1 SP1 CCV, V1.0, March 20 2008

Product Manuals:

Unicenter NSM BookShelf:

1. MDB Overview, 05/08/2006
2. Administrator Guide, 12/12/2006
3. Agent Technology Support for SNMPv3, 05/30/2006
4. CA SDK Developer Guide, 05/30/2006
5. Getting Started, 05/09/2006
6. Implementation Guide, 05/30/2006
7. Inside Event Management and Alert Management, 12/12/2006
8. Inside the Performance Agent, 05/30/2006
9. Inside Systems Management, 05/30/2006
10. Inside Systems Monitoring, 05/30/2006
11. Inside Systems Performance, 05/30/2006
12. MIB Reference Guide, 05/30/2006
13. Unicenter Management Portal Getting Started Guide, 12/12/2006

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings

are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The test approach consists of manual tests that were grouped together under the TOE component being tested. The tests were designed to cover all of the security functions as described in the SFR and TSS section of the ST.

The test plan & procedures do not cover every possible combination of parameters for a given interface and every possible combination of parameters for a given security function. However, the test plan & procedures do stimulate every external interface and all of the security functions.

The individual tests were performed and the results were collected and verified by the developer. The results were archived, recorded, and sent to the evaluator for review.

The vendor's testing purposefully intended to cover all the security functions of Audit, Alerts on Events, User attribute definition, Identification and Authentication, Administration and management of security, Partial Trusted Communication, and Partial TSF self-protection, as defined in Section 6 of the ST.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL2 evaluation.

7.2 Evaluator Independent Testing

The test approach consists of providing full coverage of all the TOE's security functions between the developer tests and team-defined functional tests as required under EAL 2.
The evaluation team performed the following activities during its on-site visit:

1. Installation of the TOE in its evaluation configuration (ADO_IGS.1)
2. Verification of the TOE Installation and configuration (Encompasses all of the below)
3. Execution of **a sampling of** the developer's functional tests (ATE_IND.2)
4. Independent Testing (ATE_IND.2)
5. Vulnerability Testing (AVA_VLA.1)
6. All captured output results can be found within the test report.

The environment and configuration for the Team-Defined testing is described in Section 8 of the VR. A distributed environment was selected to be able to test all of the functionality as described in the ST including optional features. This product can be installed in a number of configurations, including all on one machine.

The independent testing purposefully (directly) covered all of the security functions of Audit, Alerts on Events, User attribute definition, Identification and Authentication, Administration and management of security, Partial Trusted Communication, and Partial TSF self-protection, as defined in Section 6 of the ST.

All tests passed. No further obvious vulnerabilities were found.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access by administrative users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The overall strength of function (SOF) requirements claim for the TOE is SOF-Basic, which effectively requires resistance to password guessing attacks of greater than one day.

SOF analysis recommends that the administrator will enforce a password policy that meets the following criteria: a minimum of 8 characters and at least one each of a lower case, an upper case, a special character, and a numeric character. The validator assumed a worst case password guessing rate of 1000 guesses per second. To effectively resist password guessing attacks for 24 hours, the users must ensure that the passwords are sufficiently random (i.e., requiring more than 100 million guesses).

8. Evaluated Configuration

The Common Criteria testing was performed in a virtualization environment, using VMWare ESX application. The ESX server will be running on Dell PowerEdge and the HW spec/diagram lists below. As per the ST requirement, 7 machines are required for this project; the ESX server will be hosting 7 VM sessions to meet this requirement. The environment was configured to emulate the distributed environment depicted in Figure 1 and Figure 2 of this Section 5 report.

TOE components that are in-scope:

TOE Component	Testing Platform
Management Database (MDB) WorldView Manager (WV) Performance Domain Server	Platform #1
Event Manager (EM) Alert Manager (AMS) Unicenter Notification Services (UNS) Dashboard Services Web Reporting Services (WRS) NSM Security Performance Distribution Server	Platform #2
Distributed State Machine Manager (DSM) Configuration Manager (UCM) NSM Security	Platform #3
MCC	Platform #4
UMP NSM Security	Platform #4
Performance Monitoring GUIs	Platform #4
Unicenter NSM Agents: • System Agents • Log Agents • Event Agents • Performance Agents o Historical o Real-time	Platforms #5, #6 and #7

The IT Environment (out-of-scope) software and components:

Platform: Operating System, Software, Hardware	Testing Platform
OS: • Windows 2003 Software: • OpenSSL Cryptolibrary version 0.9.8g • MSSQL 2005 RDBMS Hardware: • Processor: Pentium 2 GHz • Memory: 2 GB • Disk Space: 6 GB	Platform #1

Platform: Operating System, Software, Hardware	Testing Platform
OS: • Windows 2003 Software: • OpenSSL Cryptolibrary version 0.9.8g • Tomcat/Apache Web Server v 4.1.29 Hardware: • Processor: Pentium 2.8 GHz • Memory: 2 GB • Disk Space: 8 GB	Platform #2
OS: • Windows 2003 Software: • OpenSSL Cryptolibrary version 0.9.8g • Tomcat/Apache Web Server v 4.1.29 Hardware: • Processor: Pentium 2 GHz • Memory: 1 GB • Disk Space: 4 GB	Platform #3
OS: (for MCC) • Windows 2003 Software: • OpenSSL Cryptolibrary version 0.9.8g Hardware: • Processor: Pentium 1.8 GHz • Memory: 512 MB • Disk Space: 1 GB	Platform #4
OS: (for UMP) • Windows 2003 Software: • OpenSSL Cryptolibrary version 0.9.8g • Tomcat/Apache Web Server v 4.1.29 • JRE plugin 1.4.2_16 • IE Browser 6.1 Hardware: • Processor: Pentium 2 GHz • Memory: 1 GB • Disk Space: 4 GB	Platform #4
OS: (for PM) • Windows 2003 Software: • OpenSSL Cryptolibrary version 0.9.8g • Microsoft Excel Hardware: • Processor: Pentium 2 GHz • Memory: 1 GB • Disk Space: 4 GB	Platform #4

Platform: Operating System, Software, Hardware	Testing Platform
OS: • Windows 2003 Software: • OpenSSL Cryptolibrary version 0.9.8g Hardware: • Processor: Pentium 550 MHz • Memory: 512 MB • Disk Space: 500 MB	Platforms #5, #6 and #7

Unicenter NSM Product Components included on the installation media that are not part of the scope:

- 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.

9. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name

ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

The evaluators concluded that:

The overall evaluation result for the target of evaluation is Pass. The evaluation team reached pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant for EAL2.
- Strength of Function Rating of SOF-Basic

10. Validator Comments/Recommendations

The following comments and recommendations are offered:

1. CA markets and sells NSM r11.1 SP1 CCV product as a package. Individual components are not sold separately.
2. The cryptography used in this product has not been FIPS validated nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.
3. Known vulnerabilities in the IT environment could be exploited to bypass the TOE's security policies. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer should coordinate with CA installing the latest security critical patches to components of the IT environment.
4. Post Installation documentation instructs the user to turn off SNMP (Simple Network Management Protocol) in the CC Installation Guide to force trusted channel communications using the product's DIA protocol. The SNMP option was not used in evaluated configuration and SNMP was not tested. It should be noted that the above referenced installation procedure does not change the default profile setup for the PM Historical Performance Agent, which collects data using SNMP from its host system ONLY. This SNMP (v2) collection was accomplished as a byproduct of testing the PM Historical Agent. According to the vendor/evaluator, SNMP V3 is not supported natively by MS Windows and therefore was not tested.
5. It is recommended that the administrator will enforce a strong password policy for all users that meets the following criteria: a minimum of 8 characters and at least

one each of a lower case, an upper case, a special character, and a numeric character.

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and an EAL2 certificate rating is issued for the CA Unicenter® Network and Systems Management, r11.1 SP1 CCV.

11. Security Target

CA Unicenter® Network and Systems Management, r11.1 SP1 CCV Common Criteria Security Target., Version 2.7, Apr 24, 2008. [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report and evaluation.

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**
API	**Application Programming Interfact**
ATE	**Tests**
AVA	**Vulnerability Assessment**
CAFT	**CA File Transport**
CAICCI	**CA International Common Communications Interface**
CAM	**CA Messaging**
CC	**Common Criteria for Information Technology Security Evaluation**
CCEVS	**Common Criteria Evaluation and Validation Scheme**
CCI	**CA International Common Communications Interface (CAICCI)**
CCISSF	**CAICCI Secure Sockets Family**
CEM	**Common Methodology for Information Technology Security Evaluation**
CLI	**Command Line Interface**
CM	**Configuration Management**
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	**Identification**

IP	**Internet Protocol**
IT	**Information Technology**
JDBC	**Java Database Connectivity**
JRE	**Java Runtime Environment**
MCC	**Management Command Center**
MDB	**Management Database**
NIAP	**National Information Assurance Partnership**
NIST	**National Institute of Standards and Technology**
NSA	**National Security Agency**
NSM	**Network and Systems Management**
OS	**Operating System**
PC	**Personal Computer**
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**
SNMP	**Simple Network Management Protocol**
SOF	**Strength of Function**
SP	**Service Pack**
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**

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- CA (http://www.ca.com/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.

- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004.

Other Documents

- [ST] CA Unicenter® Network and Systems Management, r11.1 SP1 CCV Common Criteria Security Target., Version 2.7, Apr 24, 2008.