National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Info Center v7.1 with Cisco WebTop v2.0

Report Number:	**CCEVS-VR-VID10066-2008**
Dated:	**July 31, 2008**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, Maryland 20878

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6757
Fort George G. Meade, MD 20755-6757

Acknowledgements:

The TOE evaluation was sponsored by:

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95124-1706
USA

Evaluation Personnel:
Arca Common Criteria Testing Laboratory

Maria Tadeo
Ken Dill

Validation Panel:

Roberta Medlock, The MITRE Corporation
Dr. Patrick Mallett, The MITRE Corporation

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Info Center v7.1 with Cisco WebTop v2.0. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Cisco Info Center v7.1 with Cisco WebTop v2.0 was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during June 2008. The information in this report is largely derived from the Security Target (ST), written by Cisco Systems, Inc. and the Evaluation Technical Report (ETR) and associated Evaluation Team Test Report, both written by Arca CCTL. The evaluation team determined the product to be CC version 2.2 Part 2 and Part 3 conformant, including all Information Technology Security Evaluation Final Interpretations from January 2004 through March 25, 2004, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 2 have been met.

The TOE is made up of several (eight) components. Cisco Info Center is an enterprise network and service level management (NMS-SLM) system that collects enterprise-wide event information from many different network data sources and presents a simplified view of this information to operators and administrators. Cisco Info Center tracks alert information in a high-performance, in-memory database and presents information of interest to specifically identified and authenticated users through individually configurable filters and views. User activity can be accounted for and audited using the administration facilities provided by Cisco Info Center. Users can access the event information assigned to them from a client application or via a Java-enabled browser connecting to Cisco Webtop (an applet is available for greater functionality). Cisco Webtop is a web server application that processes network alert information and presents the data output to users so that they can monitor events in their CIC environment. The server publishes alert data from one or more Cisco Info Center data sources in real-time so that operatives can view pages that display this information in a web browser. Further details about the components of the TOE follow.

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

1.1.1 ObjectServer

The ObjectServer is a proprietary relational database server at the core of Cisco Info Center. Alert information is forwarded to the ObjectServer from external programs such as probes and gateways, stored and managed in database tables, and displayed in the event list. In a standard configuration, alerts are forwarded directly to the ObjectServer. The TOE is run in “secure” mode. The “secure” mode forces encryption and authentication among remote TOE components. Whilst secure mode is running the ObjectServer authenticates probe and gateway connection requests by requiring a user name and a password which are encrypted during transmission. The ObjectServer supports replication and persistence of data using disk-based checkpoints and logs. Checkpoints write all data to disk at system-defined intervals to enable data recovery if the server stops unexpectedly. Between checkpoints, additional modifications to the database are logged to disk. The ObjectServer stores administrator passwords in cipher text, and they are encrypted with UNIX *crypt*, which provides Data Encryption Standard (DES) encryption of the password.

1.1.2 Webtop

Cisco Webtop is an Apache Tomcat-based web server application that processes network alert information and presents the data output to users so that they can monitor events. The server publishes alert data from one or more Cisco Info Center ObjectServer data sources in real-time so that users can view this information in a web browser.

The Webtop users must go through the I&A mechanism to gain access. When they connect to Cisco Webtop they are presented with pages, defined by an administrator, that allow them to view alert data in a number of ways. The main event display components are described below:

a) The Java-based active event list (AEL) allows clients to execute actions such as acknowledging alerts, viewing alert journals, taking ownership of alerts, running tools, and so forth.
b) The dynamic HTML lightweight event list (LEL) provides clients with the data filtering, data sorting, and information drill-down capabilities of the AEL.
c) The HTML table view component provides clients with a static event list in the form of a table showing a defined set of alerts. The non-interactive table view provides an immediate snapshot of alert status within a monitored system.

1.1.3 ObjectServer Gateway

ObjectServer gateways are used to replicate table data (for example, alert-related data) between different Cisco Info Center ObjectServers. ObjectServer gateways consist of readers and writers. Readers extract alerts from a source ObjectServer. Writers send the alert data to a target ObjectServer.
A reader extracts alerts from an ObjectServer. There is only type of reader: the ObjectServer reader. Once the reader is started and the gateway attempts to open a connection to the source ObjectServer. If the gateway succeeds in opening the connection, it immediately starts to read alerts from the ObjectServer.

Writers send the alerts acquired by a reader to the destination application or ObjectServer. Once the writer is started, the gateway attempts to establish the connection to the alert destination ObjectServer. The writer sends alerts received from the source ObjectServer.

Routes create the link between readers and writers. Once the route has been created, the connection between a reader and writer is established. Any alerts received by the source ObjectServer are read by the reader, passed through the route to the writer, and written into the destination ObjectServer.

1.1.4 Administration Client

This TOE component is also known as “Administrator” during installation and appears as “Administrator Config” after installation.

The Administrator provides a simple graphical user interface from which to configure and manage the ObjectServers.

1.1.5 User Client

This TOE component is also known as “Desktop” during installation and appears as “Event List” after installation.

The desktop User Client is an integrated suite of graphical tools used to view and manage alerts and to configure how alert information is presented.

Alert information is delivered in a format that allows users to quickly determine the availability of services on a network. When an alert cause has been identified, desktop tools enable users to resolve problems quickly.

1.1.6 Probes

Probes detect and acquire event data, and forward the data to the ObjectServer as alerts. Probes use the logic specified in a rules file to manipulate the event elements before converting them into an alert, which is sent to the ObjectServer and populates the fields of the alerts.status table.

Each probe is uniquely designed to acquire event data from a specific source. Probes can acquire data from any stable data source, including devices, databases, and log files. The probes can be installed on the ObjectServer or on a remote host.

Caution: It should be noted that the probes use protocols that include Syslog, SNMPv1, SNMPv2c, & SNMPv3, some of which are non-secure (clear-text) protocols and those are Syslog, SNMPv1, & SNMPv2c for collecting raw data from monitored devices.

1.1.7 Flex License Server

Flex Licensing is a standalone server component that provides licensing functionality for the CIC suite of products. This component is based on the premise that license administration and maintenance can be simplified by centralizing license data on one or more designated license servers, with licenses being drawn from a server as necessary.

Before running any CIC product, Flex Licensing must be installed and configured on at least one license server in your environment. Users must ensure that the requisite license files containing license feature codes for the CIC products and related components are added. A license server can be shared between multiple CIC products.

1.1.8 Security Manager

The Security Manager is the repository for role and group information for Webtop. The Webtop uses the Security Manager as its only source of authentication. In this evaluation, the Security Manager points to ObjectServer for user authentication.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology (CEM) work unit verdicts), and reviewed successive versions of the ETR and test report.

The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 2 evaluation. Therefore the validation team concludes that the Arca CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a National Security Agency (NSA) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) or candidate CCTLs using the CEM for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs and candidate CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Cisco Info Center v7.1 with Cisco Webtop v2.0
Security Target	Cisco Info Center v7.1 with Cisco Webtop v2.0 Security Target, version 2.9 date July 28, 2008
Evaluation Technical Report	• ASE (Security Target Evaluation): ASE Evaluation Technical Report for Cisco Info Center v7.1 with WebTop v2.0, document Version 0.2, released July 31, 2008. • ACM (Configuration Management Evaluation): ACM_CAP.2; Evaluation Technical Report for Cisco Info Center v7.1 with Webtop v2.0 EAL2, document Version 0.1, released June 30, 2008. • ADO (Delivery and Installation Evaluation): ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Cisco Info Center v7.1 with WebTop v2.0 & Netcool/OMNIbus v7.1 with Netcool WebTop v2.0, document Version 0.2, released July 31, 2008. • ADV (Development Evaluation): ADV_FSP.1; ADV_HLD.1; ADV_RCR.1; Evaluation Technical Report for Cisco Info Center v7.1 with WebTop v2.0 & Netcool/OMNIbus v7.1 with Netcool WebTop v2.0 EAL2, document Version 0.2 released July 31, 2008. • AGD (Administrative and User Guidance Evaluation): AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Cisco Info Center v7.1 with WebTop v2.0 & Netcool/OMNIbus EAL3, document Version 0.1, released June 30, 2008. • ATE (Functional Testing, Testing Coverage, Testing Depth and Independent Testing Evaluation): ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Cisco Info Center v7.1 with WebTop v2.0 & Netcool/OMNIbus v7.1 with Netcool WebTop v2.0 EAL2, document Version 1.0, released June 30, 2008. • AVA Vulnerability Assessment Evaluation): AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for Netcool/OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with WebTop v2.0, document Version 1.2, released June 30, 2008.
Protection Profile	None
Conformance Result	CC Part 2 extended and CC Part 3 conformant, EAL 2
Applicable interpretations and precedents	Compliant with all international interpretations with effective dates on or before December 14, 2004.
Sponsor	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95124-1706
Common Criteria Testing Lab (CCTL)	SAVVIS Communications Arca Common Criteria Testing Laboratory NVLAP Lab Code 200429 45901 Nokes Boulevard Sterling, VA 20166
CCEVS Validator(s)	Roberta J. Medlock The MITRE Corporation 7515 Colshire Drive McLean, VA 22102 Dr. Patrick W. Mallett The MITRE Corporation 7515 Colshire Drive McLean, VA 22102

3 Security Policy

The TOE addresses the following features which are relevant to the secure configuration and operation of the Cisco Info Center v7.1 with WebTop v2.0.

3.1 Security Policy

3.1.1 Identification/Authentication

The TOE supports two types of users: An Administrator with complete control over all aspects of configuration and TSF Data, and a User whose access is limited to viewing and managing alerts to determine the availability of services on a network. Both of these user types are maintain in the ObjectServer. The internal ObjectServer authentication mechanism is used to perform I&A. The Object Server stores unique usernames, application ID and encrypted passwords. Once these authentication parameters are collected, the ObjectServer compares it with the stored encrypted password, based on the result of this comparison, the authentication is either successful or denied. The Administration Client, the User Client and the Webtop require operators to identify and authenticate before accessing the system. The TOE maps the operator to a set of permissions defined by the Administrator.

3.1.2 Discretionary Access Control

When an operator authenticates, the TOE controls the level of access granted to that operator. These permissions are contained within the assigned group of the operator and are configured by the Administrator.

3.1.3 Audit

Actions taken by operators generate audit records. These records contain the date, time, event type, identity of the analyst, and outcome of the action. Only the Administrator has the ability to review and clear these records. Auditable events include the following: start-up and shutdown of audit functions; logon attempts; creation, deletion and modification of administrator / user account; and other events discussed in the Security Functions section of this document.

3.1.4 Communications

The TOE provides robust, secure communications between components. Components must successfully identify and authenticate to an ObjectServer prior to transferring data. If a Probe cannot establish a connection with its primary ObjectServer, then it will attempt to establish a connection to a secondary ObjectServer. If a secure communications establishment to the primary and secondary ObjectServers, the Probe will store data locally and not transmit to the ObjectServer.

3.1.5 Management (MAN)

The TOE offers various methods of management of security functions, including user account management, accounting and audit management, cryptographic management and replication management.

3.1.6 Replication (REP)

The TOE replicates data between ObjectServers to ensure consistency of data. As a result, if a Probe fails to connect to its primary ObjectServer, the connection to the secondary ObjectServer will allow the operators to assume regular operations without downtime or loss of configuration.

3.2 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. This includes information about the physical, personnel, and connectivity aspects of the environment.

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 2 – Assumptions for Secure Use

NAME	DESCRIPTION
A.INSTALL	The TOE is delivered, installed, managed and operated in a secure manner via an internal network only.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.PHYSEC	The ObjectServers, Webtop Server (if used) and Gateway components, and network connections between them, must be located in a physically secure environment.
A.PROBE	To enable a Probe to securely store network event data on their local platform in the event of a connectivity interruption between the Probe and the ObjectServer (when the Probe goes into "Store-and-Forward" mode), the Probe log destination must be on a separate, secure volume. This log is secured by the administrator with access controls.
A.SOLARIS	When PAM authentication is used, the ObjectServer will be able to connect to the PAM module on the Solaris machines hosting the ObjectServers.
A.TRUSTED	The TOE will be administered by competent and trusted personnel who will ensure that every user knows that all access credentials must be protected.
A.SEL_PRO	The TOE environment will be configured in such a manner as to prevent an unauthorized person from reading, modifying or destroying security critical TOE configuration data.
A.OSLOGIN	The TOE environment will be configured in such a way to require administrators and users to authenticate prior to performing security-relevant tasks.

4 Architectural Information

The diagram below shows how the TOE components are interconnected. This is software only TOE. The underlying hosts' hardware and OS of any of the TOE components are not part of the TOE. The monitored devices are not part of the TOE either. The TOE components shown in below diagram are the User Client, Administration Client, Webtop Server, ObjectServer, Gateway, Flex License Server and Probes.

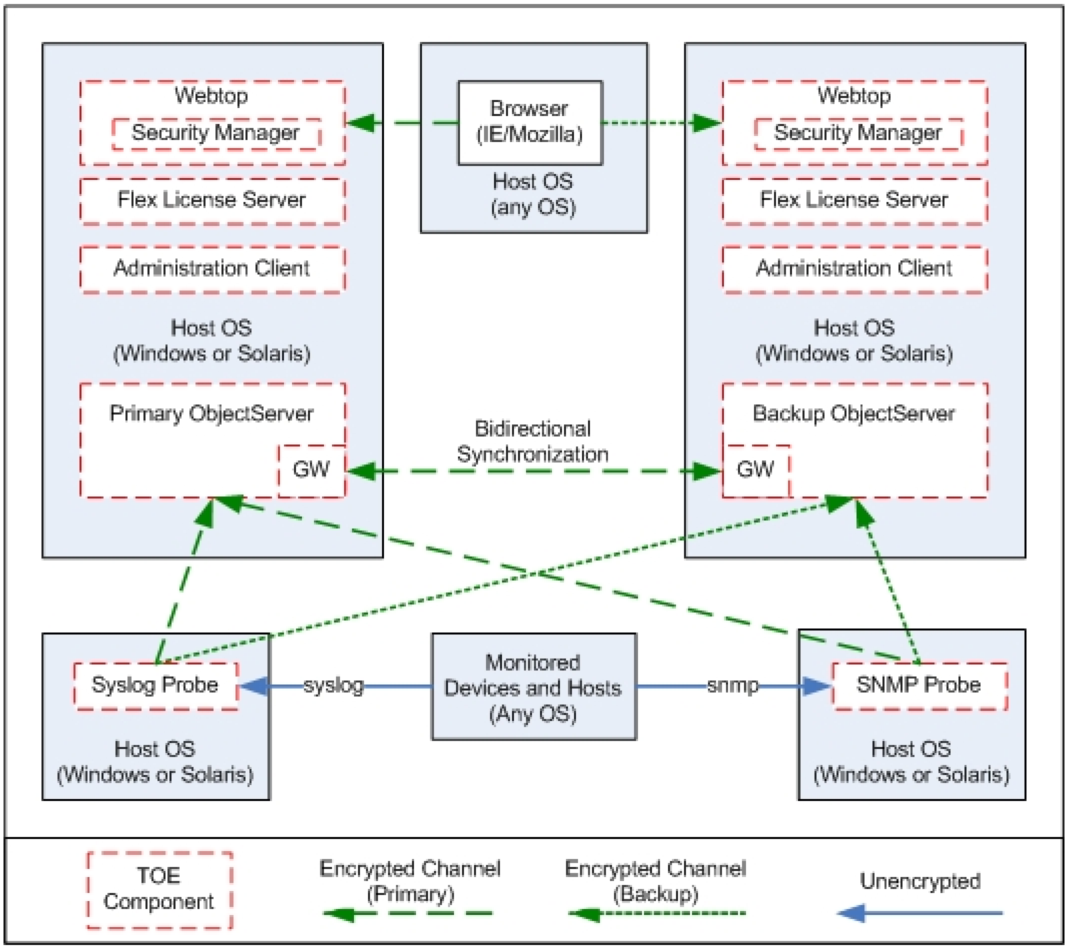

Figure 1 – Deployment Scenario 1 and TOE Boundary

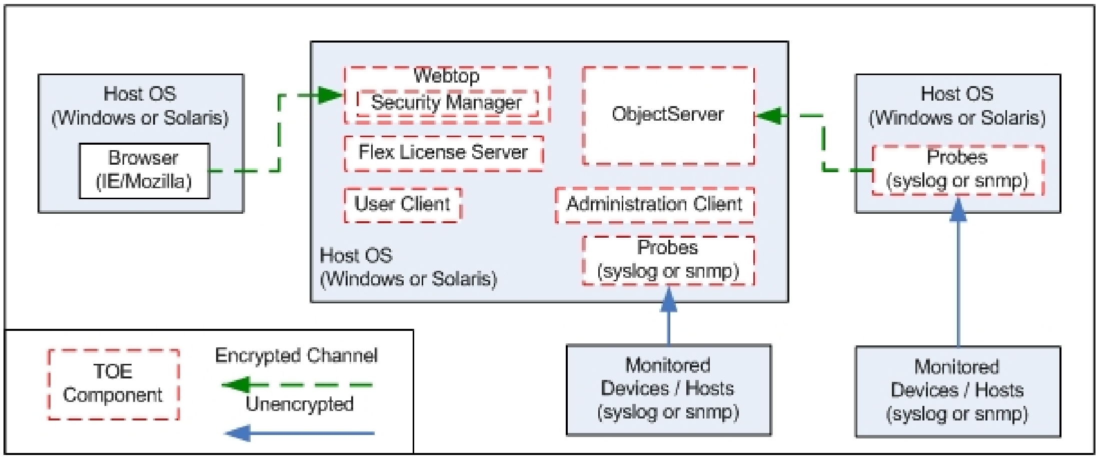

Figure 2 – Deployment Scenario 2 and TOE Boundary

4.1 TOE Components, TOE Environment and Evaluated Configuration

4.1.1 ObjectServer

Table 3 – ObjectServer Evaluated Configuration

TOE Components	
Software	Cisco Info Center v7.1, Flex License Server v1.0.31
Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Network Interface Card	Any capable of handling TCP/IP connections.

4.1.2 Webtop

Table 4 – Webtop Evaluated Configuration

Server	
TOE Components	
Software	Cisco Webtop v2.0, Cisco Security Manager v1.3.939.0
Non-TOE Components	
Software	JRE v1.4.2 or 1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Professional, Windows 2000 Advanced Server, Windows XP Professional, Windows 2003 Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Client	
Software	Windows: MS Internet Explorer 6 or Mozilla Firefox 1.5 and 1.07 Solaris: Mozilla Firefox 1.5 and 1.07
Java Version	Java Virtual Machine Plug-in 1.4.2 or 1.5
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Network Interface Card	Any capable of handling TCP/IP connections.

Note: If Webtopv2.0 is installed on the same machine as ObjectServer, the minimum requirements listed for both components must be added up/combined. The OS options will be restricted to the common OS listed.

4.1.3 Gateway

Gateway is part of Cisco Info Center v7.1 software package and is installed with ObjectServer, see table 3 above in section 4.1.1.

There is no other additional hardware or software needed for this piece of TOE.

Note: The Gateway is installed with ObjectServer installation. The term ObjectServer is used in this document to mean ObjectServer + Gateway.

4.1.4 Administration Client

Table 5 – Administration Client Evaluated Configuration

TOE Components	
Software	Cisco Info Center v7.1
Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Network Interface Card	Any capable of handling TCP/IP connections.

Note: If Administration Client is installed on the same machine as ObjectServer, the minimum requirements listed for ObjectServer component must be followed and are sufficient for both components.

4.1.5 User Client

Table 6 – User Client Evaluated Configuration

TOE Components	
Software	Cisco Info Center v7.1
Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Professional, Windows 2000 XP, Windows 2003 Server Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Network Interface Card	Any capable of handling TCP/IP connections.

Note: If User Client is installed on the same machine as ObjectServer, the minimum requirements listed for ObjectServer component must be followed and are sufficient for both components.

4.1.6 Probes

The TOE includes only the common library (libopl), which is shared by the majority of the probes. Any probes not using libopl will be outside the scope of the evaluation. These Probes can be installed on the same machine on which one of the Cisco Info Center v7.1 software components are installed or on a remote machine. The only probes included in this evaluation are the ones that use Syslog and SNMP protocols to collect raw data from monitored devices.

4.1.7 Flex License Server

Flex License Server v1.0.31 is installed with ObjectServer, see Table 3 above in section 4.1.1. There is no other additional hardware or software needed for this piece of TOE.

4.1.8 Security Manager

The Cisco Security Manager v1.3 (with Interim Fix 1) is installed with the Webtop, see Table 3. There is no additional hardware or software needed for this piece of the TOE. The Security Manager works with the Webtop to authenticate Webtop users via ObjectServer. The term Security Manager v1.3 is used in this document to mean Security Manager v1.3 + Interim Fix 1. The Security Manager is installed with the Webtop installation. The term Webtop is used in this document to mean Webtop + Security Manager.

5 Documentation

The following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

Table 7: Evaluation Evidence

Component	Description
TOE (IGS/ADM) ReadMe for IBM Netcool\OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with Cisco WebTop v2.0 (ADM/IGS)	Version 1.2, July 28, 2008
Informal Functional Specification EAL2 for IBM Netcool/OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with WebTop v2.0 (FSP) and FSP Addendum	Version 1.5, July 28, 2008 Version 1.4 June 26, 2008
High Level Design for IBM Netcool\OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with WebTop v2.0 (HLD)	Version 1.2, July 28, 2008
Cisco's Configuration Management Plan and Delivery Procedures for Cisco Info Center v7.1 with Cisco Webtop v2.0	Version 1-2, July 28, 2008
Vulnerability Analysis for IBM Netcool OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with Cisco WebTop v2.0, (VLA) Strength of Function Analysis for IBM Netcool\OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with Cisco WebTop v2.0 (SOF)	Version 0.6, June 29, 2008 Version 0.7, June 26, 2008
Test Plan and Coverage Analysis for IBM Netcool OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with Cisco WebTop v2.0 (ATE)	Version 0.6 June 29, 2008
Cisco Cisco Info Center v7.1 with Cisco WebTop v2.0 Security Target (ST)	Version 2.9 July 28, 2008
Guidance documentation (AGD): Netcool/OMNIbus v7.1 Administration Guide, [Doc version 1.1, ©2004] Netcool®/OMNIbus v7.1 Installation and Deployment Guide, [Doc version 1.1, ©2004] Netcool®/OMNIbus v7.1 User Guide, [Doc version 1.1, ©2004] Netcool®/Webtop Version 2.0 Administration Guide [Doc ID SC23-6525-00, 05-17-2007] Micromuse Netcool®/OMNIbus™, Supporting Products, ObjectServer Gateway / Netcool®/OMNIbus™ Document Version 2.1, Supporting Products, ObjectServer Gateway, 13 October 2004 Netcool®/OMNIbus v7.1, Probe and Gateway Guide, [Doc version 1.1, ©2004] Micromuse Netcool®/OMNIbus™, Supporting Products, Multi-Thread Trapd Probe / Netcool®/OMNIbus™, Document Version 2.0, Supporting Products, Multi-Thread Trapd Probe, 17 September 2004 Micromuse Netcool®/OMNIbus™, Supporting Products, Syslog Probe / Netcool®/OMNIbus™, Document Version 1.4, Supporting Products, Syslog Probe, 16 July 2004 Netcool Licensing 1.0b31 Administration Guide[Doc ID: SC23-6389-00, 5-17-2007] Netcool Security Manager Installation Guide [Doc ID: GC23-8825-00, 10-26-2007]	

6 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

6.1 Developer Testing

The developer performed a testing and coverage analysis, which examined each SFR and developed one or more developer test cases that verify the function or command requirement. These tests were documented in the *Test Plan and Coverage Analysis for IBM Netcool OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with Cisco WebTop v2.0*.

The developer tested the following security functionality claimed by the TOE: Identification/Authentication (IA),Discretionary Access Control (AC), Audit (AU), Communications (COM), Management (MAN), Replication (REP) and Protection of TOE Functions (PTF). The TOE Security Function Interfaces (TSFIs) of the above functions comprise a subset of the TOE interfaces in an entirety.

6.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer by creating a mapping of test cases to subsystem and SFR's.

The evaluation team performed the developer's entire test suite and devised an independent set of team tests and penetration tests. The evaluation team reran a subset of the developer's test suite that tested all TSF, and 32 SFRs.

The evaluation team also performed a penetration flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR to determine whether it was possible that the evaluated configuration could be susceptible to vulnerability. The specific penetration tests executed include the following:

- Used a port scanner against the target network device to determine whether the target device may have different services listening on multiple TCP/IP-enabled interfaces. Scanned each type of interface. Checked for open ports on the target host/device.
- Tested the different group levels and access to the different levels.
- Checked for known vulnerabilities on the target host/device using nessus.

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws were exploitable.

7 Evaluated Configuration

The evaluated configuration was tested in the configuration identified in Figure 3, below. The evaluation results are valid for all configurations of the TOE identified in section 4 of this report.

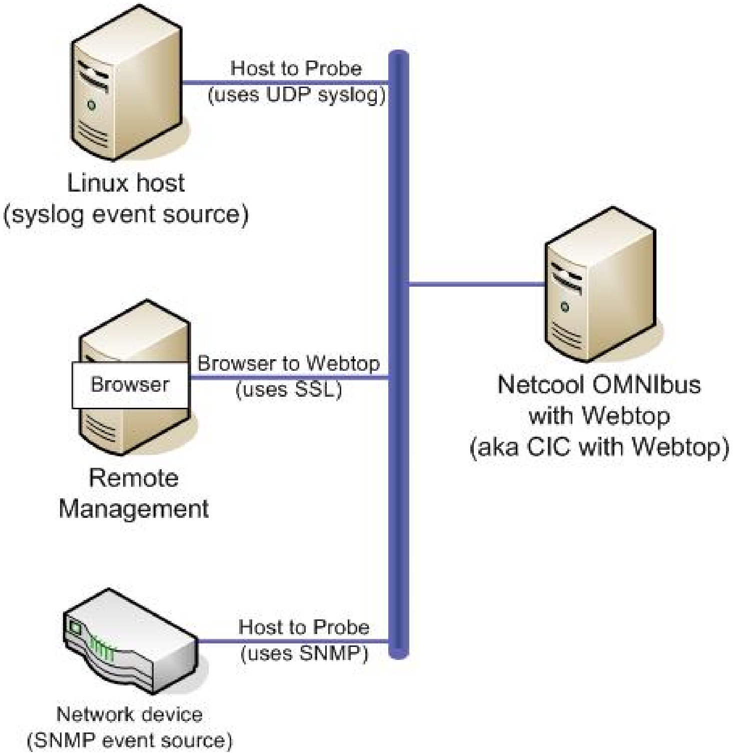

Figure 3: Testing Environment

Table 8: Software Components Tested

Description / TOE Components
Cisco Info Center v7.1 • **ObjectServer,** • **Flex License Server** • **Gateway,** • **User Client,** • **Administration Client,** • **SNMP Probe, and Syslog Probe** • **Webtop v2.0**

8 Validator Comments

The Validation Panel's observations support the evaluation team's conclusion that the Cisco Info Center v7.1 with Cisco WebTop v2.0 product meets the claims stated in the Security Target.

9 Security Target

Cisco Cisco Info Center v7.1 with Cisco WebTop v2.0 Security Target, Version 2.9, July 28, 2008.

10 List of Acronyms

ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CMS	Certificate Management System
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ID	Identifier
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
RFC	Request for Comment
SAR	Security Functional Requirement
SFR	Security Assurance Requirement
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator
VR	Validation Report

11 Bibliography

The following documents referenced during preparation of the validation report.

Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2.

Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 2004, Version 2.2.

Cisco Info Center v7.1 with Cisco WebTop v2.0 Security Target, Version 2.9, July 28, 2008.

Compliant with all international interpretations with effective dates on or before December 14, 2004

Test Plan and Coverage Analysis for IBM Netcool\OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with WebTop v2.0, Version 0.6, June 29, 2008

TOE (IGS/ADM) ReadMe for IBM Netcool/OMNIbus v7.1 with Netcool WebTop v2.0 & Cisco Info Center v7.1 with WebTop v2.0, version 1.2, July 28, 2008.

12 Interpretations

12.1 International Interpretations

Official start date of the evaluation was December 14, 2004. The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

12.2 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified. The TOE is also compliant with all International interpretations with effective dates on or before December 14, 2004