National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

NetIQ Corporation

NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6

Report Number: **CCEVS-VR-VID10114-2008**
Dated: **March 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 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

NetIQ Corporation

Evaluation Personnel:
InfoGard Laboratories Inc.
Mr. Albert Chang

Validation Personnel:
Dr. Deborah Downs, The Aerospace Corporation
Mr. Daniel Faigin, The Aerospace Corporation

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the NetIQ Secure Configuration Manager (SCM) Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6 product was performed by InfoGard Laboratories, Inc., San Luis Obispo, CA in the United States and was completed on October 29, 2007. The information in this report is largely derived from the Security Target, Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation (CCITSE), Version 2.2, January 2004 Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2, January 2004.

The NetIQ Secure Configuration Manager (SCM) Version 5.6 (hereafter NetIQ SCM) is a software application that enables organizations to determine organizational security policy compliance, to identify security vulnerabilities and potential threats, and to assist in correcting exposures in a timely manner to reduce the risk of security breaches, failed compliance audits or downtime. NetIQ SCM also provides reporting capabilities, risk scoring to assist with prioritizing the discovered potential threats and vulnerabilities, and an update service that integrates new expertise and security knowledge[1] by providing new security checks for the latest vulnerabilities, updated policy templates, and current manufacturer-recommended patches.

The NetIQ SCM can assess and report on multiple systems; however, only its use on Windows and Solaris platforms was covered by this evaluation.

NetIQ SCM uses both host-based and network-based vulnerability assessment techniques. The NetIQ SCM can leverage NetIQ Security Agents[2] installed on the systems or use "audit by proxy," which does not require an agent.

The cryptography used in this product has not been FIPS-140 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.

The product type of the TOE is a vulnerability manager and security assessment software application. It is used to determine policy compliance and to identify security vulnerabilities and potential threats. The TOE can also provide recommendations for correcting exposures. NetIQ SCM uses configurable security knowledge to perform these functions.

The user interface to the TOE is the user console, which is a Win32 application that is a required component. In the evaluated configuration, the user console must be executed remotely (i.e., the

[1] The term "security knowledge" refers to IT data used to categorize and detect potential vulnerabilities and threats (e.g., object ownership, configuration settings, object permission).
[2] The term "Agent" refers to the software used to evaluate or assess a system.

user console must not be installed on the middleware host). The middleware component (also known as SCM Core Services) can also be administered via the Core Services Configuration Utility. This utility can only be executed on the SCM Core Services system. The Core Services Configuration Utility provides minimal administrative functions that allow an administrative user to change settings for the Core Services component of SCM.

The middleware component handles communications and data flow for the SCM Agent and SCM database. SCM Agents assess endpoints as requested in the executed security check and send the results to SCM Core Services to be processed and stored in the SCM database. Users can assess and report on multiple endpoints[3], including Windows and Solaris from SCM Core Services.

An AutoSync client resides on the SCM Core Services system[4] and provides a mechanism for NetIQ Corporation to regularly update SCM Core Services with current security knowledge. The AutoSync client provides a common pipe for publishing and delivering security knowledge including patch databases, regulation templates and sample policy templates. AutoSync can be configured to check for new updates hourly or daily to ensure that security checks aren't using outdated knowledge. The customer has the ability to determine whether or not the updates are downloaded from the AutoSync server.

The SCM database maintains product configuration information (such as an asset map, permissions, report templates) and maintains security data reported by agents. The SCM database is not included in the TOE, and is a required part of the IT environment. In the evaluated configuration, the SCM database must be installed on the middleware component.

NetIQ SCM Windows agents can be deployed in two ways. In the first case, a Windows agent is installed on each of the computers being protected. When running locally, the Windows agent service must run as a local account that is a member of the Administrator group or a member of the Domain Administrator group in the domain of the managed computer. The second case is a proxy configuration where the Windows agent service must run under an account that is a member of the Domain Administrator group in the domain of the managed computer. The Windows agent in this configuration acts as a proxy agent and can access information from the Windows computers registered as endpoints in its domain. NetIQ security agents for Unix can only be deployed by installing an agent on each computer being managed.

Table 1 identifies software components of the system and indicates whether each component is in the TOE or in the Environment. The TOE executes on top of an operating system to perform its security assessments. The security checks and interfaces between the operating system, applications, and the NetIQ security agents are vendor and operating system specific.

Table 1. Software Scope and Boundary

TOE or Environment	Component	Description
TOE	SCM User Console Version 5.6	A Win32 application that runs on a Windows 2003, 2000 or XP system. SCM User Console is used to manage the NetIQ security agents, including the Windows and Solaris agent.

[3] An endpoint is an entity that an agent manages and audits. An endpoint could be a computer, database, or application.

[4] The AutoSync client can also be deployed on another computer. In this case, SCM Core Services communicates with the AutoSync client to obtain the updates. This feature is not included in the evaluated configuration.

TOE or Environment	Component	Description
TOE	NetIQ Security Agent for Windows Version 5.6	The NetIQ Security Agent for Windows runs on Windows 2000, XP, and 2003 operating systems. This agent always ships with NetIQ SCM. The Windows Agent also supports the Active Directory, Domain Infrastructures, IIS and SQL database applications that run on the Windows OS.
TOE	NetIQ Security Agent for Unix Version 5.6 – Solaris executable	The NetIQ Security Agent for Unix supports multiple brands of Unix, but only the Solaris Agent (executable) is included in the evaluated configuration. This Agent runs on Solaris 7, 8, 9, and 10. The Unix Agent is purchased separately.
TOE	SCM Core Services (Middleware) Version 5.6	The SCM Core Services application, which runs on Windows 2000 and 2003 Server. The Core Services computer must be connected to the Internet, with appropriate boundary protection between the Core Services system and the Internet.
TOE	SCM AutoSync Client Version 5.6	The client software of a service provided by NetIQ Corporation to update its customers with current security knowledge. The AutoSync client executes on the SCM Core Services system.
Environment	SCM Database software and underlying hardware and operating system (Windows 2000 Server with Service Pack 2 or later or Windows 2003 Server)	The SCM Database software is the Microsoft SQL Server 2000 with Service Pack 3 or later database. Note that in the evaluated configuration, the SCM database is co-located on the same machine as the SCM Core Services, so the hardware and operating system upon which the SCM Database resides is in the environment.
Environment	SCM User Console Hardware and Windows 2000, 2003 Workstation or Windows XP operating system	This includes the hardware and operating system upon which the User Console runs.
Environment	SCM Core Services (Middleware) hardware and Windows 2000 Server or 2003 Server Operating System	This includes the hardware and the operating system upon which the SCM Core Services runs.

TOE or Environment	Component	Description
Environment	Agent/Endpoint Hardware and Operating System Windows 2000, XP, 2003. Solaris 7, 8, 9, and 10	This includes the hardware and the operating system of the system being assessed (the endpoint).
Environment	NetIQ AutoSync Server	The network server maintained by and located at NetIQ Corporation, which is used to update customers with current security knowledge.
Environment	Mail Server	If the TOE is configured to send email alerts or the administrative users want to export/distribute the results of running a security check or policy template, the IT environment must include an SMTP server.

The items listed in Table 2 are included with or provided by the product, but are specifically excluded from the evaluated configuration. These items include hardware components, software components, configuration options, and security features.

Table 2. Components Excluded from the TOE

Item	Description
NetIQ Security Agent for Windows NT Version 5.0	The Windows NT Agent is purchased separately and is not included in the evaluated configuration.
NetIQ Security Agent for Unix Version 5.6: HP-UX AIX v4.x AIX v5.x Red Hat Linux SuSe Linux Tru64 OSF4 Tru64 OSF5 IRIX	The Unix Agent supports all the operating systems listed in this row, but they are not included in the evaluated configuration. Only the Solaris executable is included in the evaluated configuration. The Unix Agent is purchased separately.
NetIQ Security Solutions for iSeries Version 8.0	The iSeries Agent is purchased separately and is not included in the evaluated configuration.
NetIQ Security Agents for: Oracle Version 2.0 Sybase Version 1.0.4	These agents are purchased separately and are not included in the evaluated configuration.
NetIQ Security Agent for NetWare Version 1.3.2	The NetWare Agent is not included in the evaluated configuration.
NetIQ Security Agent for Apache Version 3.01	The Apache Agent is not included in the evaluated configuration.
SCM Web Console Version 5.5 and Version 5.6	This web application is an optional user interface to the TOE that is not included in the evaluated configuration.
Unix Manager Console	Provides an additional management mechanism for the Unix/Linux Security agents. The UNIX Manager Console is optional software for Unix agents.
Support for Series 3 agent protocols	Series 3 agent protocols are legacy protocols for communications between the SCM core services and SCM Agents and are not include in the evaluated configuration.
External Authentication servers	The use of external authentication, including Windows and SQL for identification and authentication to the NetIQ SCM. (Note: This does not include database authentication, which allows either Windows or SQL authentication.)

Trial deployment of Secure Configuration Manager	This is the evaluation (trial) configuration of Secure Configuration Manager.
Multiple instances of Core Services	The ability to run more than one Core Services is not included in the evaluated configuration.
AutoSync client installed on a machine other than the middleware component	In the evaluated configuration, the AutoSync client must be installed on the middleware component (the machine hosting the Core Services).
Core Services deployed on a machine that is not also hosting the SCM database SCM database installed on a machine other than the Core Services machine.	In the evaluated configuration, Core Services and the SCM database must be co-located on the same computer.
User Console installed on the middleware component	In the evaluated configuration, the User Console must be installed on its own host machine.
Standalone AutoSync client	In the evaluated configuration, the AutoSync client must be installed on the same computer as the Core Services.
Connecting to the AutoSync Server through a proxy	In the evaluated configuration, the AutoSync web site must not be accessed through an Internet proxy server.
Exceptions	The ability for the administrator to create temporary waivers to prevent a violation in a secure checkup report.
Baselines	Establishing baselines for endpoints such that once a baseline is established, a baseline comparison can be run to determine what changes have been made to the endpoint. (Note: This feature is distinct from the Solaris file content integrity checking and Solaris Network Security Checks that are included in the TSF.)
Security Checkup Results Viewer	A tool to assist with keeping track of the compliance status of all endpoints.
Running Reports from the Database	Reports can be based from information gathered from the database, instead of information gathered directly from the agent computer. Reports run from data on the database are based on data previously collected by the agents.
Agent Configuration	The ability to configure the agents is provided by the IT environment (e.g., the Windows Registry).
Remediation of Exceptions	NetIQ SCM provides the customer with the ability to submit commands to correct issues identified in the security check reports. The issues that can be corrected differ for each type of host. Examples of remediation actions including disabling a user, changing file permissions, and changing network share permissions. The ability for the TOE to issue commands to correct issues identified in the security check reports is not part of the TOE.

2 Identification

The Common Criteria Evaluation and Validation Scheme (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 3 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 3. Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6, as configured in accordance with Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6 (AGD_ADM)
Protection Profile	N/A
Security Target	NetIQ Secure Configuration Manager Version 5.6 EAL 2 Security Target, Version 1.4, March 31, 2008
Dates of Evaluation	June 2005 - March 2008
Evaluation Technical Reports	Evaluation Technical Report NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6, Version 1.3, March 21, 2008
Conformance Result	EAL 2
Version of CC	Common Criteria for Information Technology Security Evaluation Version 2.2, January 2004 CEM version 2.2, January 2004
Applicable interpretations and precedents	The TOE is compliant with all International interpretations with effective dates on or before July 21, 2005 (although none are directly applicable).
Sponsor/Developer	NetIQ Corporation
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories
CCTL Evaluator	Albert Chang
CCEVS Validator(s)	Deborah Downs, Daniel Faigin

3 Security Policy

The Security Functional Policies (SFPs) implemented by the NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6 provide a mechanism so that only the identified/authenticated administrator has access to TOE resources, provides accountability for actions by logging security events, a protection mechanism that provides the security policies, and provides security assessment templates.

The NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6 performs the following security functionality:

- Secure Assessment
- Identification and Authentication
- Secure Communications
- Cryptographic Operations
- Audit
- Security Management
- Protection of TOE Functions

The specific policies enforced by the TOE are as follows:

3.1 Security Assessments

NetIQ SCM performs security assessments that check endpoint (operating system or software application) configurations and compare them against a set of expected values. These assessments can be used to conduct policy and regulatory compliance auditing, security patch identification, object security attribute integrity, Solaris file content integrity, and vulnerability scanning[5]. NetIQ SCM provides the tools necessary to audit security controls across Windows and Solaris systems, aiding an organization in ensuring compliance with company policies and regulations. On Solaris systems, NetIQ SCM can also detect changes in network services capabilities. When a change is detected, the differences can be logged and, if configured, an alert sent to the user via e-mail.

NetIQ provides hundreds of out-of-the-box security checks to evaluate the most common security controls. Additionally, NetIQ SCM provides templates organized by regulations such as Sarbanes-Oxley, HIPAA, FERC and GLBA or by best practices such as SANS Top 20, Center for Internet Security, and other operating system baselines. Security checks can be run as needed or scheduled to occur regularly to ensure on-going policy compliance. Note that although the checks used in the templates were covered by the evaluation, there has been *no assessment* of whether the provided templates actually conform to the requirements of their associated regulations.

NetIQ also provides vulnerability alert content, including actionable templates that enable immediate assessment of the network environment to determine which systems are exposed and which systems, if any, have already been exploited.

Risk-based reporting is provided to highlight the most critical and most at-risk systems, provide executive-level summaries, and supply the information necessary for taking corrective actions.

The product provides the ability to assign importance levels to IT assets. The importance levels should represent the importance of the asset to the company's business. The importance levels include Very Low, Low, Medium, High, and Very High. By default, assets are assigned an

[5] Vulnerabilities can be identified by a known set of configurations and parameter settings in the operating system or application.

importance level of medium. Each importance level is mapped to a percentage. The Risk Score is determined by multiplying the score and the importance level.

To combat against new vulnerabilities and comply with new best practices, the AutoSync component provides content updates on a frequent basis. NetIQ SCM is able to import content updates as necessary. The content available for update on the customer NetIQ SCM systems includes vulnerability alert information, patch databases, regulation templates, best practices templates, and administration reports.

Except for patch database files, all the content information is stored in the database (DB) [Note: The DB is in the IT environment]. The patch database files are stored on the Agent itself. The DB requires users to identify and authenticate themselves to the DB prior to allowing users to access the DB. The DB operating system requires users to identify and authenticate themselves to access the system and it protects the DB from unauthorized access via file system discretionary access controls. The Agent operating system also requires users to identify and authenticate themselves to access the system and it protects the patch database files from unauthorized access via file system discretionary access controls

The patch databases are downloaded onto the file system of the Core Services machine. The remaining new content is installed on the SCM database. The administrator must review the description(s) of the new content to determine if it applies prior to applying the content updates. The content updates from AutoSync can either be applied in the NetIQ SCM or declined. When the patch databases are pushed to the Agents, they are stored on the Agent computer. NetIQ SCM enables effective remediation of exceptions from policies by providing detailed recommendations for the administrative users to follow.

3.2 Identification and Authentication

NetIQ SCM requires each user to be identified and authenticated prior to performing any functions using the NetIQ SCM User Console. The SCM database stores the user account information, including their identity, authentication information, role, and permissions.

A role is a set of permissions that controls access to specific functionality from the NetIQ SCM User Console. Permissions provide users with the ability to perform a specific job function, such as audit all Solaris servers or run particular reports. Console users can obtain access to perform a specific job function by being assigned the necessary permission directly or by being assigned a defined role that contains the necessary permission. Permissions can be used to allow or deny the ability to perform certain actions or run certain reports.

NetIQ SCM has the ability to perform local, password-based authentication or use an external authentication service (such as LDAP). The use of an external authentication is not allowed in the evaluated configuration.

NetIQ SCM includes a set of password policies that include the ability to define the password length, password composition requirements, password age, password reuse, number of allowed failed authentication attempts prior to lockout, and duration of the lockout.

The TOE does not control who can execute the Core Services Configuration Utility. Use of this utility must be protected by the IT environment.

3.3 Secure Communications

The TOE provides for secure communications between the separate portions of the TOE. The TOE uses a combination of 56-bit DES and Diffie-Hellman key exchange to secure the communications between the Core Services and the user console, when initiated by the user console. The TOE uses SSL to secure communications between the Core Services and user

console, when initiated by the Core Services. Most communications between the Core Services and user console are initiated by the user console.

The SCM User Console uses SSL to secure communications with the SCM DB.

The TOE uses TLS to secure communications between the middleware and the agents. (For backwards compatibility, the TOE is capable of negotiating an SSL session with an authorized 3rd party.)

3.4 Cryptographic Operations

The TOE verifies the integrity of files on Solaris endpoints using a message digest calculated for the files.

The AutoSync Client verifies the integrity and authenticity of updated content information[6] received from NetIQ Corporation. The downloaded updates are encrypted and digitally signed by NetIQ. The AutoSync Client decrypts the information and verifies the digital signature. The TOE will not accept updates that are not encrypted with the NetIQ private key.

3.5 Audit

The audit policy generates audit records when security-relevant events occur from actions taken within the SCM User Console. The audit information is transmitted to the SCM database for storage and tools are provided by the SCM User Console to allow users to review the audit records.

Audit records include the date and time of the event, the type of event, subject/user identity (e.g., Console User), success or failure indicator, endpoint on which the event occurred. In the case of authorized users, the subject/user identity is the user identifier. In all other cases, the subject/user identity is based on the endpoint identifier, which is presumed to be the correct identity, but cannot be confirmed as these subjects are not authenticated.

Protection of the audit trail is provided by both the TOE and the database. The TOE controls the insertion of audit events into the audit log and the deletion of audit events from the audit log via its own interfaces. The DB requires users to identify and authenticate themselves to the DB prior to allowing users to access the DB. The DB operating system also requires users to identify and authenticate themselves to access the system. The DB OS also protects the DB from unauthorized access via file system discretionary access controls.

The TOE does not generate audit records for actions performed within the Core Services Configuration Utility. Auditing for actions performed within the Core Services Configuration Utility is the responsibility of the IT environment.

3.6 Security Management

Security management functions of the NetIQ SCM execute on the middleware component. Authorized users manage the middleware component via the SCM user console or the Core Services Configuration Utility.

The TOE implements roles by assigning console permissions (also known as just permissions) directly to users or to defined roles that then assigned to users. The console permissions determine access to specific management functions (or tasks).

[6] The term “content information” is used to refer to security knowledge which includes patch databases, regulation templates and sample policy templates. Content information updates are received from the NetIQ AutoSync server. Content information is stored in content files.

NetIQ SCM provides management tools to define roles, assign permissions to roles and users, perform user management, configure the AutoSync client (auto or manual scheduling, set NetIQ AutoSync server URL), create custom security checks (build “where” clauses based on conditions and values and define regular check attributes including name, description, penalty, risk, remedy, explanation). The TOE also provides the ability to export the results of running a security check or policy template. Once the results are exported, the administrator is responsible for maintaining the security of the results, possibly with the assistance of the IT environment.

The information needed to establish secure communications between the Agents and the Core Services is provided during initial installation. The Agents are ready for use immediately following installation. Configuration of the Agents is provided by the IT environment (e.g., Windows Registry) or is not included in the scope of the evaluation (Unix Manager Console).

3.7 Protection of the TOE

Logical protection of the TOE is required to ensure the TOE security services are not bypassed or tampered with. The TOE and the operating system cooperate to provide this capability. The TOE is responsible for protecting access to the user console interface and protecting the interfaces used to communicate between the Core Services and the Agents. The operating system is responsible for protecting the TOE executables from tampering. The hardware and operating system implement process separation.

4 Assumptions and Clarification of Scope

4.1 Connectivity Assumptions

- **Internet Connection Required**

  The SCM Core Services middleware system must be connected to the Internet, behind appropriate boundary protection mechanisms, in order to receive updated content information from the NetIQ servers.

4.2 Physical Security Assumptions

- **Appropriate Physical Security**

  It is assumed that 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.

- **Controlled Access Facility**

  The SCM Core Services middleware system is located within in a controlled access facility, which only allows SCM Core Services console administrators to have access to the SCM Core Services middleware system.

4.3 Personnel Security Assumptions

- **Administrators Follow Published Guidance**

  The administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow and abide by the instructions provided in the guidance documentation.

4.4 Operational Security Assumptions

- **Only Administrators Use Middleware System**

  It is assumed that only SCM Core Services console administrators have user accounts on the underlying operating system of the SCM Core Services middleware system.

- **Core Services and Database Systems Are Dedicated**

  It is assumed that the SCM Core Services and SCM database systems are dedicated to their respective NetIQ SCM functions and do not provide any general-purpose or user data storage capabilities.

- **NetIQ Content Files are Reviewed Before Application**

  Administrators will implement procedures for reviewing and validating updated content files from NetIQ, and for applying the updates.

4.5 Threats Countered and Not Countered

The TOE or IT environment addresses the security threats identified below:

- Authorized users may not be accountable for their actions performed within the User Console because their actions were not audited, thus allowing the user to violate the security policy and escape detection.

- A user or process may gain unauthorized access to the audit trail and cause records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.

- An authorized user may install a content update that an attacker has intercepted and modified.

- A user or process may gain unauthorized access to content files and delete or modify the information in the content files.

- A user or process may masquerade as another entity in order to gain unauthorized access to TOE data or resources.

- An attacker may be able to access protected data due to a policy compliance failure.

- A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.

- A user or process may cause through an unsophisticated attack, TSF data transmitted between the separate parts of the TOE and the IT environment and TSF data or executable code stored in the IT environment to be inappropriately accessed (viewed, modified, or deleted).

- An administrator may not have the ability to notice potential security violations resulting from the User Console, thus limiting the administrator's ability to identify and take action against a possible security breach.

- An attacker may be able to access protected data due to an undiscovered system vulnerability.

4.6 Organizational Security Policies

There are no applicable organizational security policies

5 Architectural Information

The NetIQ SCM is broken into four components: user interfaces, middleware, SCM database, and NetIQ security agents (also known as Agents). Figure 1 depicts the TOE and the intended TOE environment.

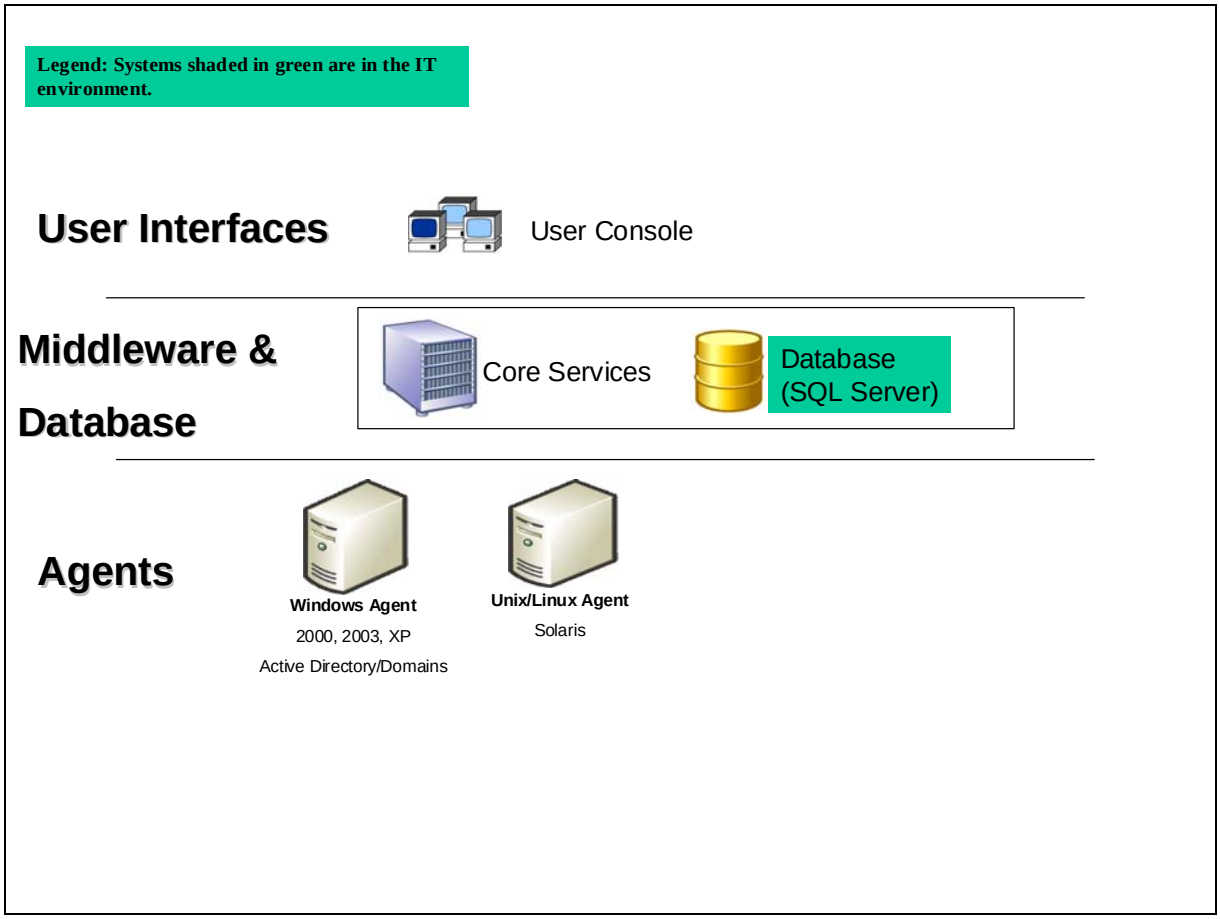

Figure 1. NetIQ SCM Network Environment

The user interface to the TOE is the user console, which is a Win32 application that is a required component. In the evaluated configuration, the user console must be executed remotely (i.e., the user console must not be installed on the middleware host). The middleware component (also known as SCM Core Services) can also be administered via the Core Services Configuration Utility. This utility can only be executed on the SCM Core Services system. The Core Services Configuration Utility provides minimal administrative functions that allow an administrative user to change settings for the Core Services component of SCM.

The middleware component handles communications and data flow for the SCM Agent and SCM database. SCM Agents assess endpoints as requested in the executed security check and send the results to SCM Core Services to be processed and stored in the SCM database. Users can assess and report on multiple endpoints[7], including Windows and Solaris from SCM Core Services.

An AutoSync client resides on the SCM Core Services system[8] and provides a mechanism for NetIQ Corporation to update SCM Core Services with current security knowledge. The AutoSync client provides a common pipe for publishing and delivering security knowledge including patch databases, regulation templates and sample policy templates. AutoSync can be configured to check for new updates hourly or daily to ensure that security checks aren't using outdated knowledge. The customer has the ability to determine whether or not the updates are downloaded from the AutoSync server.

As depicted in Figure 2 below, the SSL/TLS ports to and from the SCM Core Services system are not the standard SSL port 1443. Integrators, installers, etc. need to take the use of non-standard port numbers for SSL/TLS connections into consideration when configuring the boundary protection mechanisms.

The SCM database maintains product configuration information (such as an asset map, permissions, report templates) and maintains security data reported by agents. The SCM database is not included in the TOE and is a required part of the IT environment. In the evaluated configuration, the SCM database must be installed on the middleware component.

[7] An endpoint is an entity that an agent manages and audits. An endpoint could be a computer, database, or application.

[8] The AutoSync client can also be deployed on another computer. In this case, SCM Core Services communicates with the AutoSync client to obtain the updates. This feature is not included in the evaluated configuration.

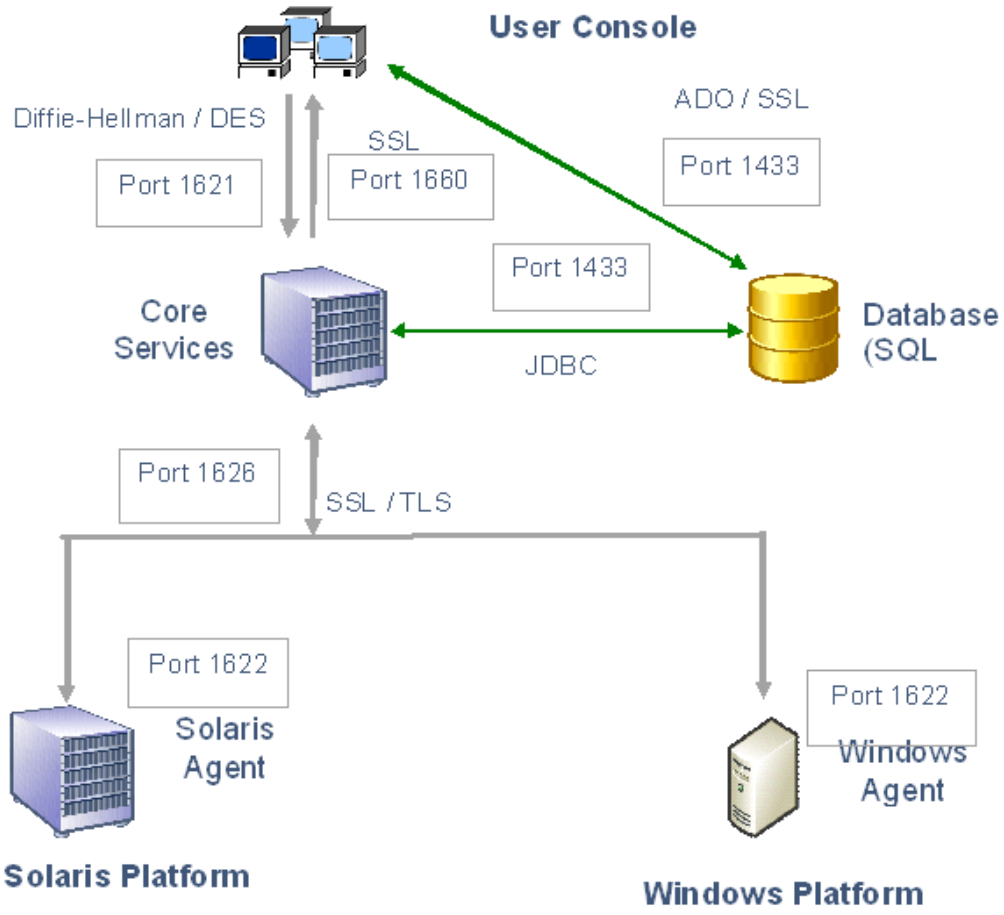

Figure 2. SCM Architecture and Data Flow

NetIQ SCM Windows agents can be deployed in two ways. In the first case, a Windows agent is installed on each of the computers being protected. When running locally on the Windows agent machine, the Windows agent service must run as a local account that is a member of the Administrator group or a member of the Domain Administrator group in the domain of the managed computer. The second case is a proxy configuration where the Windows agent service must run under an account that is a member of the Domain Admininistrator group in the domain of the managed computer. The Windows agent in this configuration acts as a proxy agent and can access information from the Windows computers registered as endpoints in its domain. NetIQ security agents for Unix can only be deployed by installing an agent on each computer being managed.

NetIQ SCM operates with any of the following NetIQ security agents:

- Windows Agent (Windows 2000, 2003, XP , Active Directory, Domain Infrastructures, IIS, and SQL server)
- Unix/Linux Agent (Solaris, AIX, HP-UX, RedHat, SuSE, Tru64, & IRIX) (only Solaris is included in the evaluation)

- iSeries Agent (not included in the evaluation)
- Database Agent (Oracle, Sybase) (not included in the evaluation)

NetIQ SCM Version 5.6 supports both Series 4 and Series 3 agent protocols for transmissions between the SCM Core Services and SCM Agents. However, the evaluated configuration only includes the Series 4 Agents for Solaris and Windows. The Series 4 agents are issued an authentication key at registration. The Series 4 agent protocol communicates using 128-bit RC4 over Transport Layer Security (TLS).

The Windows Agent is capable of collecting security information from the machine upon which it is installed or from another Windows machine. When a Windows Agent collects security information from another Windows machine, it is called proxy auditing.

In terms of logical boundaries, Table 4 enumerates the division between services provided by the TOE. The TOE itself does not rely on any services provided by the Operating Environment:

Table 4. TOE Security Functions

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE by the IT or Non-IT Environment
Security Assessment	Security assessments check endpoint (operating system or software application) configurations and compare them against a set of expected values.	None
ID and Authentication	User console authentication validates the username and password against hashed credentials stored in the SCM database. NetIQ SCM provides a password policy that is enabled by default and offers password rules that apply to all accounts. The password mechanism of the Identification and Authentication security function satisfies the claim of SOF-basic.	The TOE environment helps store authentication data.
Cryptographic Operations	The NetIQ SCM provides the ability to protect the AutoSync content updates from unauthorized disclosure and to verify the integrity of the content updates so administrators can trust the current security knowledge received from NetIQ Corporation by the AutoSync client. The ability to verify the content integrity of selected files on Solaris endpoints is also provided by the TSF.	None

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE by the IT or Non-IT Environment
Audit	NetIQ SCM provides security checkup reports to assess how well the assets comply with the organization's security standards (assess the vulnerability of the endpoints/assets). Users can view the audit records for history of their own actions taken within the User Console. Only console administrators can view/sort the history of other users.	The IT environment helps protect the audit trail and storage. The IT environment also provides reliable time stamps. The IT environment is responsible for any auditing of the core services component, to the extent that it is possible from the OS.
Security Management	The TOE provides security management functions and tools to manage the security features it provides. In addition, the TOE supports roles and permissions to determine what security management functions a particular user can perform.	None
Protection of TOE Functions	Protection of the TOE from physical and logical tampering from other methods is ensured by the physical security assumptions and by the domain separation requirements on the hardware and operating system in the environment.	The IT environment provides protection for the Core Services Configuration Utility by requiring that the SCM Core Services middleware system be physically secured and provide user accounts only to SCM Core Services administrative users. The IT environment is responsible for domain separation and non-bypassability of the TSP.
Secure Communications	The TOE uses TLS over TCP/IP to provide secure communication channels between the SCM Core Services and the SCM Agent. (For backwards compatibility, the TOE is capable of negotiating an SSL session with an authorized 3rd party) The transmitted data is encrypted to ensure confidentiality. A message authentication code (MAC) is generated for the transmitted data. This MAC is transmitted with the data to ensure integrity of the transmitted data and provide the ability to detect modification to the transmitted data. TLS/SSL can resend data if modifications are detected.	None.

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6. Note that not all evidence is available to customers.

The TOE is physically delivered to the end User or the User can download the TOE via the web through a secure channel. The mandatory configuration guidance is a TOE component and is either delivered with the TOE on CD labeled "Documentation CD" or downloaded through the web. Only the documents referenced under Guidance Documentation and the Security Target are publicly available by the end users. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.

6.1 Design Documentation

Document	Revision	Date
NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation (ADV_HLD)	0.7	1/28/08
NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation (ADV_FSP)	0.7	1/28/08
NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation (ADV_RCR)	0.7	1/28/08

6.2 Guidance Documentation

Document	Revision	Date
Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6 (Getting Started Guide)	0.5	1/16/08
Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6 (Quick Start)	0.5	1/16/08
User Guide - NetIQ Secure Configuration Manager	N/A	11/15/2006
Installation Guide - NetIQ Secure Configuration Manager	N/A	11/15/2006
NetIQ Security Agent for Unix Installation and Configuration Guide. Net IQ Security Manager, NetIQ Security Configuration Manager	N/A	11/1/2006
Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6 (AGD_ADM)	0.5	1/16/08

6.3 Configuration Management and Lifecycle

Document	Revision	Date
EAL 2 Configuration Management Documentation NetIQ Secure Configuration Manager 5.6 (ACM_CAP)	0.2	10/15/07

6.4 Delivery and Operation Documentation

Document	Revision	Date
NetIQ Product Delivery and Operations Process (ADO_DEL)	0.4	January 2007

6.5 Test Documentation

Document	Revision	Date
NetIQ Secure Configuration Manager Version 5.6 EAL 2 Independent Test Plan (ATE_IND.2)	1.1	2/20/08
EAL 2 Test Activity ATE NetIQ Secure Configuration Manager 5.6 (ATE_COV.1)	0.7	1/22/08

6.6 Vulnerability Assessment Documentation

Document	Revision	Date
NetIQ Secure Configuration Manager 5.6 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL2 (AVA_VLA)	0.4	1/24/08

6.7 Security Target

Document	Revision	Date
NetIQ Secure Configuration Manager Version 5.6 EAL2 Security Target	1.4	3/31/08

7 IT Product Testing

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

7.1 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. During the evaluation of the ATE_FUN.1, the evaluation team identified inconsistencies in the test cases and worked with the Developer to create accurate test cases. Inconsistencies included missing/misleading test procedures, ambiguous expected results, and inconsistent actual results.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

During the final review process, a security concern was raised regarding the deployment configuration of TOE and IT environment components. The Developer changed the TOE configuration and exercised the secure communication interfaces to ensure the confidentiality of the communication. The CC supplement was updated to reflect the new installation instructions.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

7.2 Evaluation Team Independent Testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team reran 90% of the Sponsor's test cases and specified additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

The following TOE Security Functions were added to the Security Target to better enumerate the security functions provided by the TOE. Because the TOE is validated at EAL 2, complete testing of all TOE SFRs is not required. As such, the following SFRs have not been tested by the developer *or* the evaluation Team.

- FPT_ITC.1 – Inter-TSF confidentiality during transmission
- FPT_ITI.1 – Inter-TSF detection of modification
- FMT_MTD_EXP.1e – Explicit Management of TSF data – Export

Functional testing conducted by the Developer and the CCTL emphasized only the TOE's ability to create and run security policy templates and not the correctness of each security policy templates.

The Evaluation team installed and configured the TOE per the supplied Administrative Guidance, CC configuration guidance and the Security Target. Figure 3 and Table 5 describes the TOE's test setup.

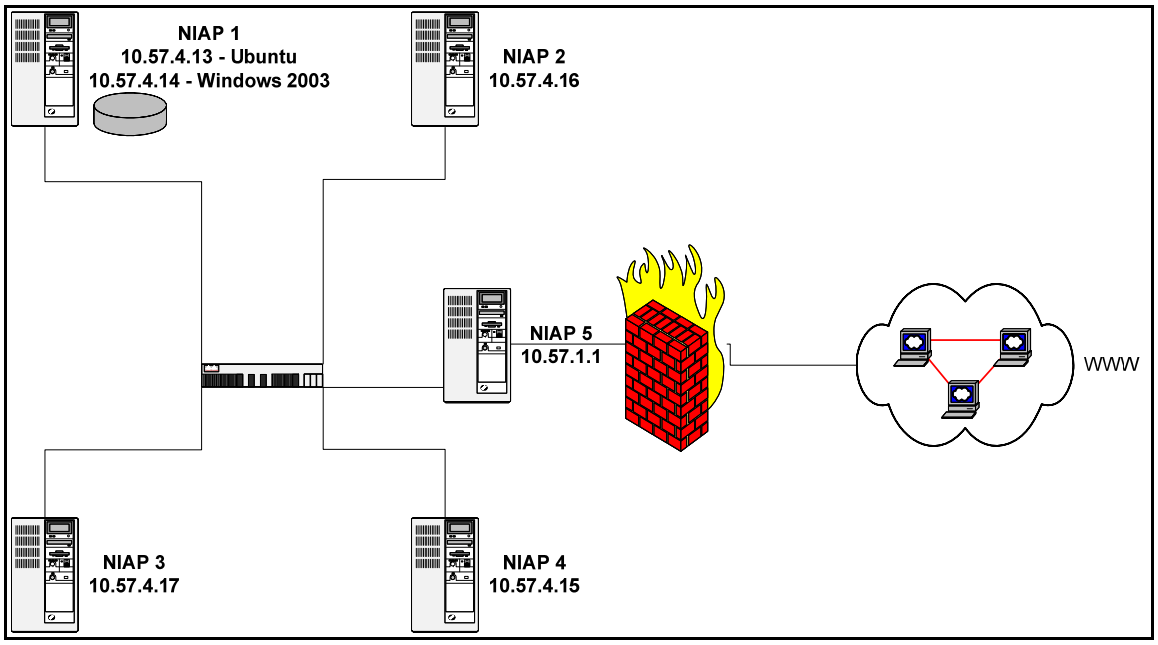

Figure 3. NetIQ Test Network Setup

Table 5. Test Configuration

Quantity	Description	Purpose
1	Dell PowerEdge 840 machine (NIAP1)	Host system running the following OS and application(s): 1. Ubuntu OS Version 6.06 LTS – Linux 2.6.15-51-389 kernel 2. VMware Server 1.0.4 (Build 56528) running a Windows 2003 Server (with SQL) image. 3. Wireshark version 0.99.6a (SVN Rev 22276) 4. Domain Controller 5. DNS Server 6. DHCP Server 7. SMTP Server 8. POP3 Server Supports the following TOE component(s): 1. SCM Core Services Version 5.6 2. Core Services Configuration Utility 3. SCM AutoSync Client Version 5.6
1	Dell Optiplex GX270 machine (NIAP3)	Host system running the following OS and application(s): 1. Windows 2003 SP2 2. Wireshark version 0.99.6a (SVN Rev 22276) Supports the following TOE component(s): 1. SCM User Console Version 5.6
1	Dell Precision 340 machine (NIAP2)	Host system running the following OS and application(s): 1. Windows 2000 SP4 – 5.00.2195 2. Wireshark version 0.99.6a (SVN Rev 22276) Supports the following TOE component(s): 1. NetIQ Security Agent for Windows Version 5.6
1	Dell Inspiron 4150 machine (NIAP4)	Host system running the following OS and application(s): 1. Solaris 10 2. Wireshark version 0.99.6a (SVN Rev 22276) Supports the following TOE component(s): 1. NetIQ Security Agent for UNIX Version 5.6
1	Dell Optiplex GX270 machine machine (NIAP5)	Host system running the following OS and application(s): 1. Windows 2003 SP2 2. DNS Server 3. DHCP Server 4. SMTP Server 5. POP Server
1	5 ports Ethernet Switch	Supports test network

Table 6 provides a visual representation of all defined tests. These security functions were tested by exercising 90% of the vendor functional tests, 9 independent tests, and 3 penetration tests.

Table 6. TOE Tests

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
Vendor Tests				
TC-100	Identification & Authentication	Add user and verify password complexity settings.	FIA_ATD.1 FIA_SOS.1 FMT_SMF.1 FMT_MOF_EXP.1 FMT_MTD_EXP.1a	SCM I&A Interface | Password Policy Management

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
TC-110	Identification & Authentication	User lockout threshold, duration and reset counter	FIA_AFL.1 FMT_MOF_EXP.1 FIA_SOS.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1b FMT_MTD_EXP.1c	SCM I&A Interface | Password Policy Management
TC-120	Identification & Authentication	Delete users and Edit user account properties	FIA_ATD.1 FMT_SMF.1 FMT_MOF_EXP.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1b	SCM I&A Interface | Delete Console User/Modify Console User Properties
TC-130	Identification & Authentication	User account password change, password reuse, and password age.	FIA_ATD.1 FIA_SOS.1 FMT_SMF.1 FMT_MOF_EXP.1 FMT_MTD_EXP.1a,b,c,d	SCM I&A Interface | Reset Console User Properties/Reset Own Password
TC-140	Identification & Authentication	Verify that Admin user can add and copy roles	FIA_ATD.1 FMT_SMF.1 FMT_SMR.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1b	SCM Role Interfaces | Copy a Role
TC-141	Identification & Authentication	Verify that Administrator role user can edit and delete roles.	FIA_ATD.1 FMT_SMF.1 FMT_SMR.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1c FMT_MTD_EXP.1d	SCM Role Interfaces | Modify Role Assignment
TC-142	Identification & Authentication	Verify that user that is a member of the administrator role can assign and remove permissions to and from a user.	FIA_ATD.1 FMT_MTD_EXP.1a,b,c,d	SCM Role Interfaces
TC-143	Identification & Authentication	Verify that user that is a member of the Console Administrator role can edit role permissions.	FIA_ATD.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1b FMT_MTD_EXP.1c FMT_MTD_EXP.1d	SCM I&A Interfaces
TC-150	Identification & Authentication	Verify that non-Admin user cannot access user roles and permission settings.	FIA_ATD.1 FMT_SMF.1 FMT_SMR.1 FMT_MTD_EXP.1a,b,c,d	SCM Role Interfaces
TC-160	Identification &	Verify that user	FIA_UAU.1	Core Services

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
	Authentication	properly authentication to the system can start the SCM configuration utility.	FIA_UID.1 FPT_SEP_EXP.1	Agent Interface
TC-200	Security Management	Verify that user with proper permission via their role can add and copy security checks in the SCM console.	FMT_SMF.1 FMT_MTD_EXP.1a,b	SCM Assessment Interfaces
TC-201	Security Management	Verify that user with proper permission via their role can add and copy Windows and Solaris security check.	FMT_SMF.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1b	SCM Assessment Interfaces
TC-202	Security Management	Verify that Administrator with proper permission via their role can add and copy Windows checks.	FMT_SMF.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1b	SCM Assessment Interfaces
TC-210	Security Management	Verify that Console Administrator can edit and delete Windows security check	FMT_SMF.1 FMT_MTD_EXP.1a,c,d	SCM Assessment Interfaces
TC-211	Security Management	Verify that user with proper permission via its role can edit and delete Windows security check as a Console user.	FMT_SMF.1 FMT_MTD_EXP.1a,c,d	SCM Assessment Interfaces
TC-220	Security Management	Verify that admin user with proper permission via its role can add and copy Windows/Solaris template.	FMT_SMF.1 FMT_MTD_EXP.1a,b,c	SCM Assessment Interfaces

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
TC-221	Security Management	Verify that user with proper permission via its role can add and copy Windows/Solaris template.	FMT_SMF.1 FMT_MTD_EXP.1a,b,c	SCM Assessment Interfaces
TC-230	Security Management	Verify that console Administrator can edit and delete security policy templates	FMT_SMF.1 FMT_MTD_EXP.1a,c,d	SCM Assessment Interfaces
TC-240	Security Management	Verify that user without the proper permissions cannot access restricted items in the SCM console	FMT_SMF.1 FMT_MTD_EXP.1a,b,c,d	SCM Assessment Interfaces
TC-300	Security Assessment	Verify that console user with appropriate permission can run a standalone Windows security check, and a group of Windows checks as a console.	FMT_SMF.1 FMT_MTD_EXP.1a FSC_ASM_EXP.1 FSC_RPT_EXP.1 FSC_REV_EXP.1	SCM Assessment Interfaces
TC-310	Security Assessment	Verify that console user with appropriate permission can run a standalone Solaris security check, and a group of Windows checks as a console.	FMT_SMF.1 FMT_MTD_EXP.1a FSC_ASM_EXP.1 FSC_RPT_EXP.1 FSC_REV_EXP.1 FSC_SDI_EXP.1 FSC_SDI_EXP.2 FSC_SDI_EXP.3 FSC_NAL_EXP.1	SCM Assessment Interfaces
TC-320	Security Assessment	Verify that the Console administrator user can disable a user on Windows and Solaris.	FSC_RMT_EXP.1	SCM Assessment Interfaces
TC-400	Secure	Verify that the	FCS_COP.1a,b	Core Services to

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
	Communications & Cryptography	communication between the SCM Console and the Agents are secured.	FPT_ITT.1	Agent interface
TC-410	Secure Communications & Cryptography	Verify that Console user with appropriate permissions can run template against both Windows and Solaris machine.	FMT_SMF.1 FMT_MTD_EXP.1a FSC_ASM_EXP.1 FSC_RPT_EXP.1	SCM Assessment Interfaces
TC-420	Secure Communications & Cryptography	Verify that the TOE's Autosync feature to get update.	FMT_MOF_EXP.1 FMT_MTD_EXP.1a FMT_MTD_EXP.1c	AutoSync Get interface
TC-430	Secure Communications & Cryptography	Analyze the encrypted traffic during the Core Server update and verify that they are secure.	FCS_COP.1a,b FPT_ITT.1	AutoSync Get interface
TC-500	Audit	Verify that the TOE provides a history of audit records.	FAU_GEN.EXP.1 FAU_GEN.2 FAU_SAR.1a,b FAU_SAR.2 FAU_SAR.3	SCM Reporting Interfaces
Independent Functional Testing				
IGL-FAU-100	Audit	Verify that user with the role Console Administrator can delete audit record	FAU_GEN_EXP.1	SCM Reporting Interfaces
IGL-FAU-102	Audit	Verify that the TOE administrator can perform searches and sorting of audit data based on: user identity, date and time of event, endpoint, and type of event.	FAU_SAR.3	SCM Reporting Interfaces
IGL-FAU-103	Audit	Verify that the TOE user can read audit trail data produced by their own activity from the	FAU_SAR.1b FAU_SAR.2	SCM Reporting Interfaces

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
		audit records and that they can not be viewed by other non-administrative roles.		
IGL-FMT-100	Security Management	Verify that only user with the Administrator role can delete security checks and that user with the role Console User cannot delete security checks.	FMT_MTD_EXP.1d	SCM Assessment Interfaces
IGL-FMT-101	Security Management	This test verifies that a user that is a member of the Console Administrator role can edit role permissions. This test adds onto the Vendor Test TC-143.	FMT_MTD_EXP.1c	SCM Role Interface
IGL-FSC-100	Security Assessment	Verify that the TOE can run security check based on schedule set by the administrator.	FSC_ASM_EXP.1	SCM Assessment Interfaces
IGL-FSC-101	Security Assessment	Verify that the port scan security check against the Solaris Agent can scan all the ports available on that Agent machine.	FSC_SDI_EXP.3	SCM Assessment Interfaces
IGL-FSC-102	Security Assessment	Verify that the TOE monitors change permission action on the Windows machine.	FSC_SDI_EXP.1	SCM Assessment Interfaces
IGL-FIA-100	Identification & Authentication	Verify that the TOE password policy prohibits	FIA_SOS.1	SCM I&A Interface

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
		reuse of 8 previous passwords.		
Independent Penetration Testing				
IGL-PEN-100	Security Assessment	Attempt to schedule a policy template with invalid dates and times with the Console Administrator user.	FSC_ASM_EXP.1	SCM Assessment Interfaces
IGL-PEN-101	Identification & Authentication	Verify that the authentication mechanism to the SCM Console will not fail with null and long password attacks.	FIA_SOS.1	SCM I&A Interface
IGL-PEN-102	Security Management	Attempt to modify column values for Package Name, Package Type, and Package Location to force and error during an update to the table AS Table of Content in the Vigilent database.	FMT_SMF.1	AutoSync Get interface

7.3 Vulnerability analysis

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Strength of Function analysis, the Developer Vulnerability Analysis, the evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis, the evaluation team devised penetration testing (as listed in Table 6 above) to confirm that the TOE was resistant to penetration attacks performed by an attacker with an expertise level of unsophisticated. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing. This resulted in a set of three penetration tests.

8 Evaluated Configuration

The evaluated configuration of the NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6, as defined in the Security Target, consists of the several components. Please refer to Table 1 for the TOE's components.

The NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6 must be configured in accordance with the following Guidance Documents:

- Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6 Version 0.5, January 16, 2008

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

InfoGard Laboratories has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in October, 2007.

10 Validator Comments

- The TOE makes use of cryptographic modules in order to fulfill some security functions. The cryptography used in this product has not been FIPS 140-2 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.
- It is important to control access to the machine hosting the Core Services Configuration Utility, as this component has no I&A or Audit of its own and depends on the I&A of the host platform.
- The configuration of the product is limited, excluding **most** user agents, remote management, automatic AutoSync (as the administrator must manually check downloads), and even some capabilities delivered with the product. Integrators of the product must ensure that their desired capabilities were covered by the evaluation.
- The compliance aspects of the templates **were not tested**. In other words, the evaluation tested only that the security checks that *could* be included in a template check what they claim to test. The evaluation **did not verify** that the templates are in accordance with any claimed regulations. For example, the evaluation did not test that a HIPAA template is in accordance with the HIPAA regulations.
- It is important to keep any underlying host machines patched for reported vulnerabilities, as a security system is only as strong as its weakest link.
- The TOE does not have the capability to audit the deletion of user accounts.
- The TOE must have connectivity to the Internet in order to receive active updates.
- The TOE uses non-standard port numbers for connections. Integrators, installers, etc. need to take this non-standard usage into consideration when configuring the boundary protection mechanisms.

11 Security Target

NetIQ Secure Configuration Manager Version 5.6 EAL2 Security Target, Version 1.4, March 31, 2008.

12 List of Acronyms

AIX	IBM Variant of Unix
ATR	Actual Test Results
CA	California
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCITSE	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratories
CD	Compact Disc
CEM	Common Evaluation Methodology
DB	Database
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard
GLBA	Gramm-Leach-Billey Act
HIPAA	Health Insurance Portability and Accountability Act
HP-UX	Hewlett-Packard Unix
I&A	Identification and Authentication
IBM	International Business Machines
IIS	Internet Information Services
IRIX	Silicon Graphics Variant of Unix
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LTS	Long Term Support
MAC	Message Authentication Code
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSF	Open Software Foundation
POP3	Post Office Protocol, Version 3
SANS	System Administration, Networking, and Security Institute
SCM	Secure Configuration Manager
SFP	Security Functional Policies
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
SVN	Software Version Number
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
U.S.	United States
VR	Validation Report
Win32	Windows 32-bit Platform
XP	Not an acronym – Name for Windows Operating System

13 Bibliography

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 2.2, January 2004. CCIMB-2004-01-0001.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 2.2, January 2004. CCIMB-2004-01-002..

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 2.2, January 2004. CCIMB-2004-01-003.

[4] Common Criteria Project Sponsoring Organisations. Common Criteria Common Methodology for Information Technology Security Evaluation. January 2004 CCIMB-2004-01-004.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, January 2002.

[6] InfoGard Laboratories, Inc. NetIQ Secure Configuration Manager Version 5.6 EAL2 Security Target Version 1.3, March 21, 2008.

[7] InfoGard Laboratories, Inc. Evaluation Technical Report NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6, Version 1.3, March 21, 2008.