NetIQ Secure Configuration Manager Version 5.6
EAL2 Security Target

Release Date:	March 31, 2008
Document ID:	05-534-R-0067
Version:	1.4

Prepared By: InfoGard Laboratories, Inc.

Prepared For:

NetIQ Corporation
1233 West Loop South
Suite 1800
Houston, TX 77027

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:	NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6
ST Identification:	NetIQ Secure Configuration Manager Version 5.6 EAL2 Security Target
ST Version:	1.4
ST Publish Date:	March 31, 2008
ST Authors:	Michelle Ruppel
Assurance Level:	EAL2
PP Identification:	None

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.2[1] Part 2 extended and Part 3 conformant at EAL2. The TOE is also compliant with all International interpretations with effective dates on or before July 21, 2005.

The TOE is compliant with selected NIAP Interpretations. The selected NIAP Interpretations are identified as they are applied to the security requirements in Section 5.

This TOE is not conformant to a Protection Profile (PP).

1.3 Overview

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[2] 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 Windows and Solaris

[1] Common Criteria (CC) for Information Technology Security Evaluation – January 2004, Version 2.2.

[2] 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).

are tested in this evaluation.

NetIQ SCM uses both host-based and network-based vulnerability assessment techniques. The NetIQ SCM can leverage NetIQ Security Agents[3] installed on the systems or "audit by proxy" which does not require an agent.

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.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1 – ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP Interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

[3] The term "Agent" refers to the software used to evaluate or assess a system.

Refinement: ***additions are indicated with bold text and italics***

deletions are indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

2 TOE Description

2.1 Overview

The product type of the TOE is a vulnerability manager and security assessment software application 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.

2.2 Architecture Description

The TOE is broken into three components: user interfaces, middleware, and NetIQ security agents (also known as Agents). The TOE also relies upon SCM database and Internet which are in the IT environment.

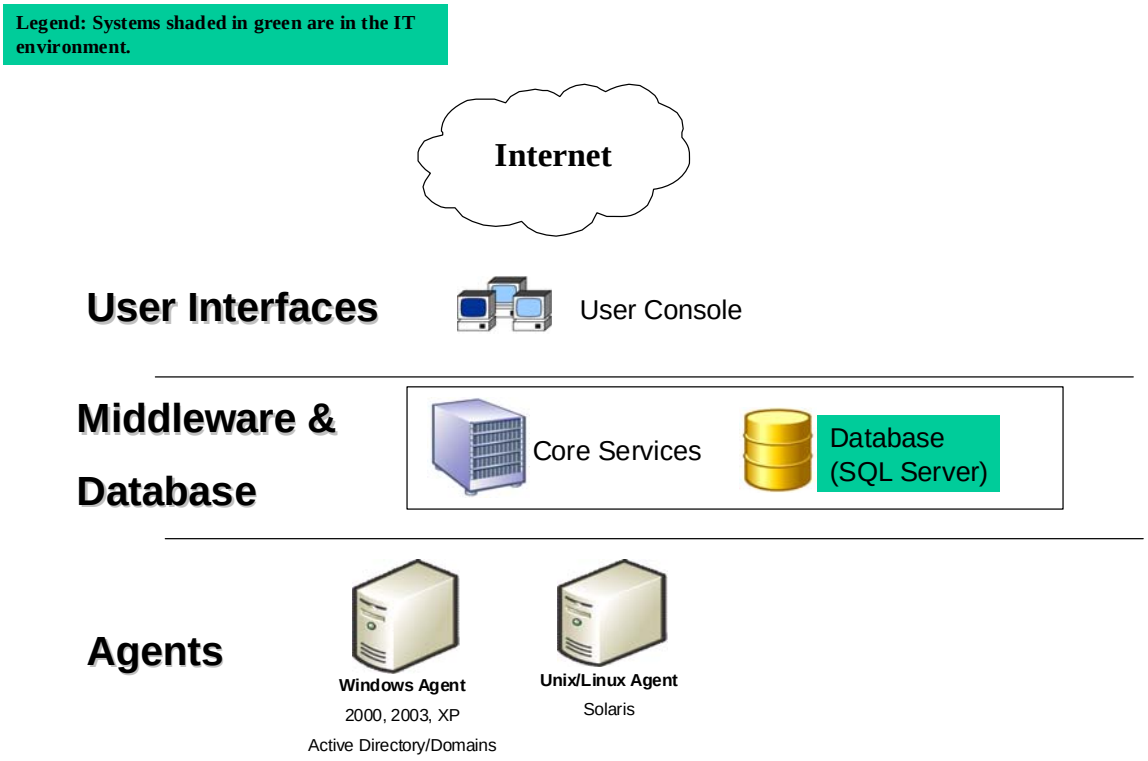

Figure 1: NetIQ SCM Network Environment

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 which 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[4], including Windows and Solaris from SCM Core Services.

An AutoSync client resides on the SCM Core Services system[5] 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.

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.

As depicted in the figure 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.

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

[5] 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.

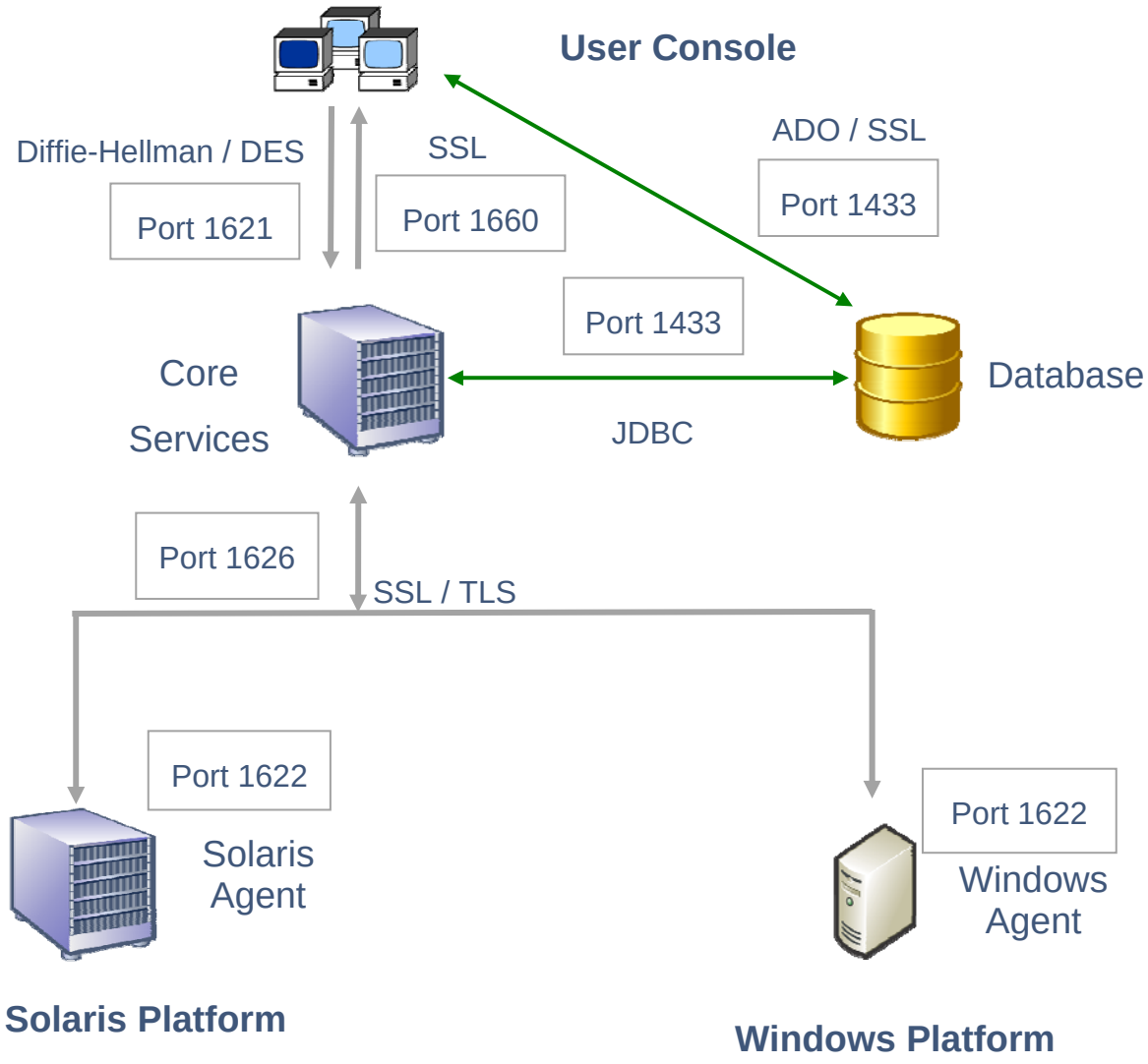

Figure 2: SCM Architecture and Data Flow

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 which is a member of the Administrators group or a member of the Domain Administrators group in the domain of the managed computer. In the proxy configuration (the second case), the Windows agent service must run under an account that is a member of the Domain Admins 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.

2.2.1 SCM Agents

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

- Windows Agent (Windows 2000, 2003, XP[6], 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[7] 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 on 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.

2.3 Physical Boundaries

This section lists the hardware and software components and denotes which are in the TOE and which are in the environment. The NetIQ SCM is a software-only TOE.

2.3.1 Hardware/Software Components

The following table identifies hardware and/or software components of the deployed system and indicates whether each component is in the TOE or the Environment.

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.

[6] NetIQ SCM does not operate with the 64 bit version of Windows XP.

[7] These agent protocols are NetIQ proprietary protocols.

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 on 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 that the User Console runs on.
Environment	SCM Core Services (Middleware) hardware and Windows 2000 Server or 2003 Server Operating System	This includes the hardware and the operating system that the SCM Core Services runs on.
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).

TOE or Environment	Component	Description
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.

Table 2 – Physical Boundary

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.

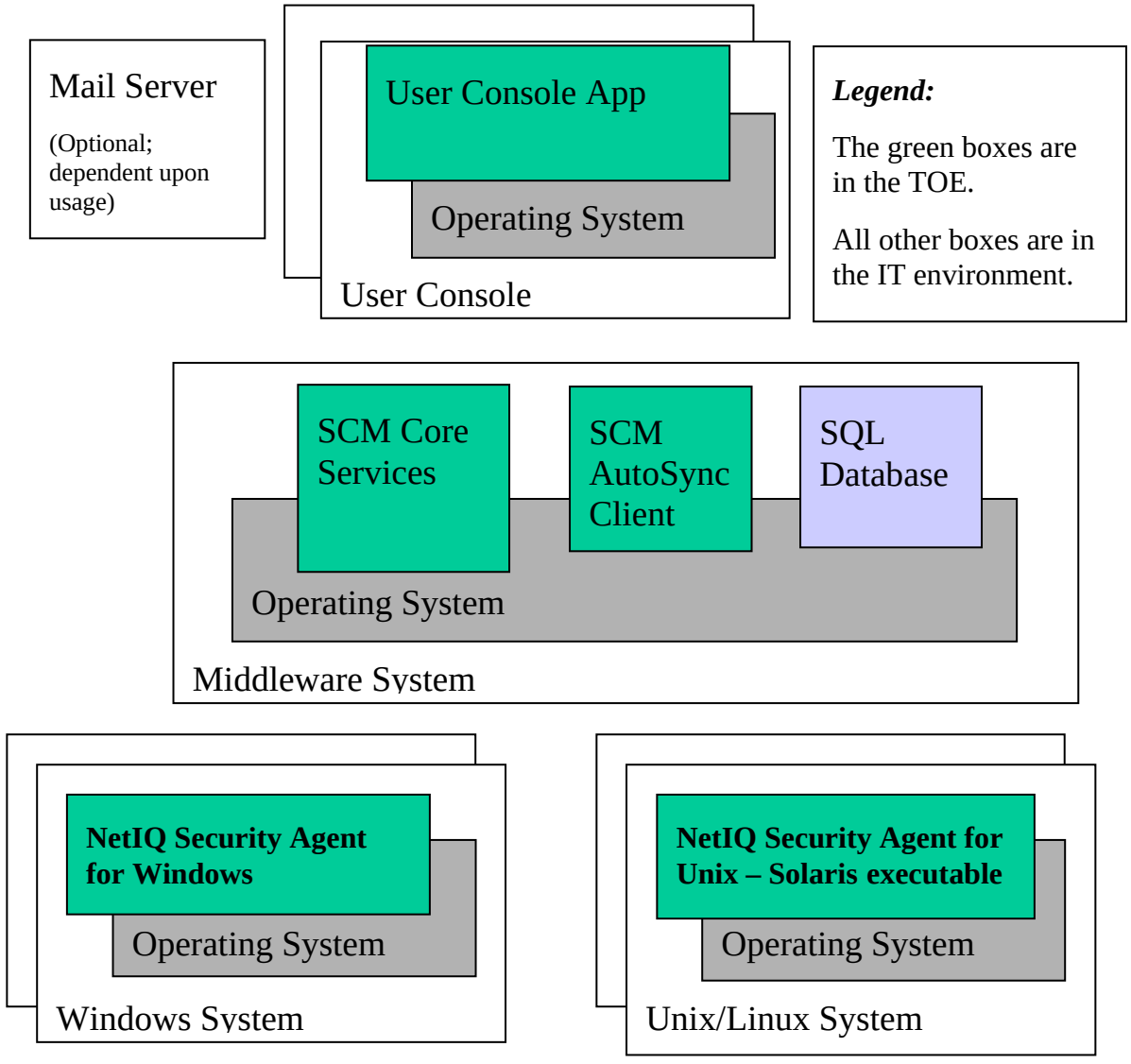

Figure 3: TOE Physical Boundary

2.4 Logical Boundaries

This section describes the product features and denotes which are in the TOE. Recall that the SCM database is in the IT environment.

2.4.1 Audit

The audit functionality 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 since these subjects are not authenticated.

Protection of the audit trail is provided by both the TOE and the database (DB). 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.

2.4.2 Cryptographic Operations

The TOE can verify 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[8] 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.

2.4.3 Identification and Authentication

NetIQ SCM requires each user to be identified and authenticated prior to performing any

[8] 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.

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 which 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 is protected by the IT environment.

2.4.4 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 work together 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.

2.4.5 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 which are then assigned to users. The console permissions determine access to specific management functions (or tasks).

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).

2.4.6 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.)

2.4.7 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[9]. NetIQ SCM provides the tools necessary to audit security controls across Windows and Solaris systems, 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. [10]

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.

---

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

[10] The templates and their ability to meet the regulations were not evaluated or tested.

Customers are provided with 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 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 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.

2.5 Items Excluded from the TOE

The items listed below 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.

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	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.

IRIX	
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 which 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.

Table 3 – Items Excluded from the TOE

3 TOE Security Environment

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

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

3.1 Assumptions

The assumptions are organized into four categories: connectivity assumptions, personnel assumptions, physical environment assumptions, and operational assumptions.

3.1.1 Connectivity Assumptions

A.INTERNET 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.

3.1.2 Personnel Assumptions

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

3.1.3 Physical Environment Assumptions

A.ITPHYS 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.

A.PHYS_SEC 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.

3.1.4 Operational Assumptions

A.CS_ACCTS 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.

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

3.2 Threats

The TOE or IT environment addresses the security threats identified below. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with low attack potential who posses an average expertise, few resources, and low to moderate motivation.

T.ACCOUN	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.
T.AUD_COMP	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.
T.BAD_UPDATE	An authorized user may install a content update that an attacker has intercepted and modified.
T.CNT_COMP	A user or process may gain unauthorized access to content files and delete or modify the information in the content files.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to TOE data or resources.
T.NO_POL_COMP	An attacker may be able to access protected data due to a policy compliance failure.
T.RESIDUAL	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.
T.TSF_COMP	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).

T.UNIDENT_ACTION	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.
T.VULN	An attacker may be able to access protected data due to an undiscovered system vulnerability.

3.3 Organisational Security Policies

There are no organizational security policies defined for this TOE.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

O.AUD_GEN	The TOE will provide the capability to detect and create records of security relevant events performed within the User Console.
O.AUD_PROT	The TOE will provide the capability to protect audit information through its own interfaces.
O.AUD_REVIEW	The TOE will provide the capability to selectively review audit information.
O.CNT_PROT	The TOE will provide the capability to protect the content files through its own interfaces.
O.CRYPTO	The TOE shall provide cryptographic services to verify the integrity and authenticity of data.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.
O.PART_SELF_PROT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosures through its own interfaces.
O.SECURE_COMM	The TOE will provide secure communications that prevent unauthorized disclosure and modification of transmissions between distributed portions of the TOE and between the user console and the DB.
O.SECURE_CHK	The TOE will detect policy compliance failures or vulnerabilities that were discovered on the system during execution of security checks.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the User Console.

4.2 Security Objectives For The Environment

The following IT security objectives for the environment are to be addressed by the IT environment by technical means.

OE.AUD_STORAGE	The IT environment will provide a means for secure storage of the TOE audit log files.
OE.DOMAIN_SEP	The IT environment will provide an isolated domain for the execution of the TOE.
OE.NO_BYPASS	The IT environment will ensure that the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.
OE.RESIDUAL	The IT environment will ensure that any information contained in a protected resource within the TOE scope of control is not released when the resource is reallocated.
OE.TIME_STAMPS	The IT environment will provide reliable time stamps.
OE.TSF_DATA_PROT	The IT environment will provide mechanisms to control access to the TSF data.

The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

OE.CS_ACCTS	Only SCM Core Services console administrators will be given user accounts on the underlying operating system of the SCM Core Services middleware system.
OE.DEDICATED	Administrators will ensure that the systems executing the SCM Core Services and SCM database systems are dedicated to those functions and do not provide any general-purpose or user data storage capabilities.
OE.INTERNET	The SCM Core Services middleware system will be connected to the Internet, behind appropriate boundary protection mechanisms, in order to receive updated content information from the NetIQ servers.
OE.NOEVIL	Sites using the TOE shall ensure that the authorized administrators are appropriately trained, not careless, not willfully negligent, non-hostile, and follow all administrative guidance.

OE.ITPHYS Physical security will be 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.

OE.PHYS_SEC The SCM Core Services middleware system will be located within a controlled access facility, which only allows SCM Core Services console administrators to have access to the SCM Core Services middleware system.

OE.SEC_UPDATES Enterprises using the TOE shall implement procedures to ensure that the table of contents for the updated content files (vulnerability alert information, patch databases, regulation templates, best practices templates, and administration reports) are reviewed prior to receipt of the updated content files from NetIQ Corporation, the updates are validated before being used, and the updates are distributed to systems within the enterprise via secure mechanisms.

4.3 Mapping of Threats and Assumptions to Objectives

The following table represents a mapping of the threats and assumptions to the objectives defined in this ST.

	A.INTERNET	A.NOEVIL	A.ITPHYS	A.PHYS_SEC	A.CS_ACCTS	A.DEDICATED	A.SEC_UPDATES	T.ACCOUN	T.AUD_COMP	T.BAD_UPDATE	T.CNT_COMP	T.MASQUERADE	T.NO_POL_COMP	T.RESIDUAL	T.TSF_COMP	T.UNIDENT_ACTION	T.VULN
O.AUD_GEN								X								X	
O.AUD_PROT									X								
O.AUD_REVIEW																X	
O.CNT_PROT											X						
O.CRYPTO										X							X
O.MANAGE															X		
O.PART_SELF_PROT									X		X				X		
O.SECURE_COMM									X						X		
O.SECURE_CHK													X				X
O.TOE_ACCESS								X				X					
OE.AUD_ STORAGE									X								
OE.DOMAIN_SEP									X		X				X		
OE.NO_BYPASS									X		X				X		
OE.RESIDUAL									X					X	X		
OE.TIME_STAMPS								X								X	
OE.TSF_DATA_PROT									X		X	X			X		

	A.INTERNET	A.NOEVIL	A.ITPHYS	A.PHYS_SEC	A.CS_ACCTS	A.DEDICATED	A.SEC_UPDATES	T.ACCOUN	T.AUD_COMP	T.BAD_UPDATE	T.CNT_COMP	T.MASQUERADE	T.NO_POL_COMP	T.RESIDUAL	T.TSF_COMP	T.UNIDENT_ACTION	T.VULN
OE.CS_ACCTS					X							X					
OE.DEDICATED						X											
OE.INTERNET	X																
OE.NOEVIL		X															
OE.ITPHYS			X														
OE.PHYS_SEC				X													
OE.SEC_UPDATES							X										

Table 4 – Assumptions, Threats & IT Security Objectives Mappings for the Environment

4.4 Rationale For Threat Coverage

T.ACCOUN — O.AUD_GEN helps to mitigate this threat by ensuring that security-relevant actions taken by authorized users within the User Console are detected and recorded for review. O.TOE_ACCESS supports this threat by requiring the TOE to identify and authenticate all authorized users prior to allowing access via the User Console. OE.TIME_STAMPS assists in mitigating this threat by requiring the IT environment to provide a reliable time stamp. The audit mechanism is required to include the current date and time in each audit record. Note: Auditing and accountability for actions taken using the Core Services Configuration Utility is excluded from this threat and any responsibility for auditing and accountability of this utility is on the IT environment.

T.AUD_COMP — O.AUD_PROT contributes to mitigating this threat by controlling access to the individual audit log records via the user console. No one is allowed to modify audit record. Only the Console Administrator is allowed to delete audit records. OE.AUD_STORAGE contributes to mitigating this threat by restricting the ability of users in the IT environment to access the audit log file. O.SECURE_COMM contributes to mitigating this threat by providing secure communications preventing unauthorized modification of audit records transmitted over the network. OE.RESIDUAL prevents a user from accessing audit information that might be persistent in a resource used by the TOE (e.g., memory). By preventing residual information in a resource, audit information will not become available to any user or

	process except those explicitly authorized for that data. O.PART_SELF_PROT contributes to countering this threat by ensuring that the TSF can protect itself from users via its own interfaces. This limits access to the audit information to the functions defined for the specified roles. OE.DOMAIN_SEP contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the operating system could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control access to the resources under its control, which includes the audit trail. OE.NO_BYPASS ensures audit compromise cannot occur simply by bypassing the TSF. OE.TSF_DATA_PROT is necessary to control who is able to view and modify TSF data stored in the IT environment using non-TSF interfaces (this includes attempting to access the TSF files directly via the OS). Note: Database administrators can access the audit log records stored in the DB.
T.BAD_UPDATE	O.CRYPTO counters this threat by providing cryptographic services, which can be used to verify the integrity and authenticity of data. The TOE can verify the integrity and authenticity of content updates prior to their use by an authorized user.
T.CNT_COMP	O.CNT_PROT contributes to mitigating this threat by controlling access to the content files via the TOE interfaces. Users are not allowed to modify or delete content files. O.PART_SELF_PROT contributes to countering this threat by ensuring that the TSF can protect itself from users via its own interfaces. This limits access to the content information to the functions defined for the specified roles. OE.DOMAIN_SEP contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the operating system could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control access to the resources under its control, which includes the audit trail. OE.NO_BYPASS ensures compromise cannot occur simply by bypassing the TSF. OE.TSF_DATA_PROT is necessary to control who is able to view and modify content files stored in the IT environment using non-TSF interfaces (this includes attempting to access the files directly via the OS). Note: Database administrators can access the content files stored in the DB.
T.MASQUERADE	O.TOE_ACCESS mitigates this threat by requiring administrative users to be identified and authenticated prior to using SCM user

	console, a necessary step in controlling the logical access to the TOE and its resources by constraining how and when users can access the SCM user console. OE.CS_ACCTS contributes to mitigating this threat by requiring that only SCM Core Services Console administrators have accounts on the SCM Core Services middleware system, so only console administrators can execute the SCM Core Services Configuration utility. OE.TSF_DATA_PROT controls who is able to view and modify TSF data and resources stored in the IT environment using non-TSF interfaces partially by requiring users to be identified and authenticated prior to using the underlying operating system.
T.NO_POL_COMP	O.SECURE_CHK mitigates this threat by providing methods to detect policy compliance failures and take remedial actions to correct the failure. The policy compliance failures are detected by executing security checks configured to detect violations of the organization's policy.
T.RESIDUAL	OE.RESIDUAL counters this threat by ensuring that memory contents are not persistent when resources are released by the TOE and allocated to another user/process.
T.TSF_COMP	OE.RESIDUAL is necessary in mitigating this threat because even if the security features do not allow a user to explicitly view TSF data, if the TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data. O.PART_SELF_PROT is necessary so that the TSF protects itself and its resources from inappropriate access through its own interfaces. OE.DOMAIN_SEP is necessary so that the TSF is protected from other processes executing on the workstation. O.MANAGE is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data via the TOE interfaces, as well as the behavior of TSF functions. OE.NO_BYPASS ensures TSF compromise cannot occur simply by bypassing the TSF. OE.TSF_DATA_PROT is necessary to control who is able to view and modify TSF data stored in the IT environment using non-TSF interfaces. O.SECURE_COMM counters this threat by providing secure communications preventing unauthorized disclosure for communications between distributed parts of the TOE and between the user console and the SCM DB.
T.UNIDENT_ACTION	O.AUD_REVIEW helps to mitigate this threat by providing a method for reviewing the recorded security actions that could indicate a

	potential security violation. O.AUD_GEN helps to mitigate this threat by recording actions performed within the SCM User Console for later review. OE.TIME_STAMPS assists in mitigating this threat by requiring the IT environment to provide a reliable time stamp.
T.VULN	O.SECURE_CHK mitigates this threat by providing methods to detect known vulnerabilities and take remedial actions to correct the vulnerability. The vulnerabilities are detected by executing security checks designed to detect potential vulnerabilities. O.CRYPTO assists in mitigating this threat by providing a method to check the integrity of files.

4.5 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

A.INTERNET	OE.INTERNET restates the assumption as an objective and therefore, addresses the assumption.
A.NOEVIL	OE.NOEVIL restates the assumption as an objective and therefore, addresses the assumption.
A.ITPHYS	OE.ITPHYS restates the assumption as an objective and therefore, addresses the assumption.
A.PHYS_SEC	OE.PHYS_SEC restates the assumption as an objective and therefore, addresses the assumption.
A.CS_ACCTS	OE.CS_ACCTS restates the assumption as an objective and therefore, addresses the assumption..
A.DEDICATED	OE.DEDICATED restates the assumption as an objective and therefore, addresses the assumption.
A.SEC_UPDATES	OE.SEC_UPDATES restates the assumptions as an objective therefore, and addresses the assumption. Administrators use secure methods to receive and validate the updates from the NetIQ Corporation, then use secure methods to distribute the updates.

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 - 5.4.

TOE Security Functional Requirements (from CC Part 2)	
FAU_GEN.2	User Identity Association
FAU_SAR.1a	Audit Review – Administrator
FAU_SAR.1b	Audit Review – User
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_COP.1a	Cryptographic Operation – Baseline
FCS_COP.1b	Cryptographic Operation - AutoSync
FCS_COP.1c	Cryptographic Operation – DES
FCS_COP.1d	Cryptographic Operation – IKE
FCS_COP.1e	Cryptographic Operation - MAC
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MSA.2	Secure security attributes
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_ITT.1	Basic internal TSF data transfer protection
Explicitly Stated TOE Security Functional Requirements	
FAU_GEN_EXP.1	Explicit audit data generation
FMT_MOF_EXP.1	Explicit Management of security function behaviour
FMT_MTD_EXP.1a	Explicit Management of TSF data – Query
FMT_MTD_EXP.1b	Explicit Management of TSF data – Create, initialize
FMT_MTD_EXP.1c	Explicit Management of TSF data – Modify
FMT_MTD_EXP.1d	Explicit Management of TSF data – Delete
FMT_MTD_EXP.1e	Explicit Management of TSF data – Export
FPT_SEP_EXP.1	Partial TSF domain separation
FSC_ASM_EXP.1	Security assessments
FSC_NAL_EXP.1	Network security check alerts for Solaris
FSC_RMT_EXP.1	Remediation Recommendations
FSC_RPT_EXP.1	Security Check Reports
FSC_REV_EXP.1	Security Check Report Review

FSC_SDI_EXP.1	Security attribute integrity
FSC_SDI_EXP.2	Stored Solaris content integrity
FSC_SDI_EXP.3	Solaris network security checks
IT Environment Security Functional Requirements (from CC Part 2)	
FAU_STG.1	Protected audit trail storage
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.1	Subset residual information protection
FIA_UAU.2a	User authentication before any action – SCM DB
FIA_UAU.2b	User authentication before any action – OS
FIA_UID.2a	User identification before any action – SCM DB
FIA_UID.2b	User identification before any action – OS
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps

Table 5 – Security Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 ***For audit events resulting from actions of identified users, the ~~The~~*** TSF shall be able to associate each auditable event with the identity of the user that caused the event. ***(NIAP Interpretation 0410)***

5.1.1.2 FAU_SAR.1a Audit Review - Administrator

FAU_SAR.1.1a The TSF shall provide **Console Administrators and console users with the View Task History for all Console Users permission** with the capability to read **all audit trail data** from the audit records.

FAU_SAR.1.2a The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 FAU_SAR.1b Audit Review - User

FAU_SAR.1.1b The TSF shall provide **Console Users** with the capability to read **audit trail data produced by their own activity** from the audit records.

FAU_SAR.1.2b The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 FAU_SAR.2 Restricted Audit Review

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

5.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on

a. **user identity;**

b. **date and time of the event;**

c. **endpoint;**

d. **type of event (e.g., Admin, Report, and Security Checkup).**

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **TLS v1 symmetric key & secret generation** and specified cryptographic key sizes **128 bits for symmetric keys and 1024 bits for asymmetric keys** that meet the following: **conformant to RFC 2246 (TLS v1) symmetric key and secret generation**.

5.1.2.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **IKEv1 or IKEv2** that meets the following: **RFC 2409 for IKEv1, RFC 4306 for IKEv2**.

5.1.2.3 FCS_COP.1a Cryptographic Operation – Baseline

FCS_COP.1.1a The TSF shall perform **message digest calculations** in accordance with a specified cryptographic algorithm **MD5** and cryptographic key sizes **not applicable**[11] that meet the following: **IETF RFC 1321**.

5.1.2.4 FCS_COP.1b Cryptographic Operation – AutoSync

FCS_COP.1.1b The TSF shall perform **decryption and signature verification of the AutoSync updates** in accordance with a specified cryptographic algorithm **Advanced Encryption Standard (AES) for decryption and RSA SHA-1 for signature verification** and cryptographic key sizes **128-bit for decryption and 1024-bit for signature verification** that meet the following: **FIPS-PUB 197 for AES and ANSI X9.31 for RSA SHA-1**.

---

[11] Message digests use hash functions, which do not have keys. Therefore the assignment related to the cryptographic key size has been set to “not applicable”.

5.1.2.5 FCS_COP.1c Cryptographic Operation – DES

FCS_COP.1.1c The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **DES** and cryptographic key sizes **56-bit** that meet the following: **FIPS 46-3 and RFC2406 "Encapsulating Security Payload (ESP)".**

5.1.2.6 FCS_COP.1d Cryptographic Operation – IKE

FCS_COP.1.1d The TSF shall perform **IKE (Internet key exchange)** in accordance with a specified cryptographic algorithm **Diffie-Hellman** and cryptographic key sizes **1024 bits** that meet the following: **RFC 2409 (IKEv1) & RFC 4306 (IKEv2).**

5.1.2.7 FCS_COP.1e Cryptographic Operation – MAC

FCS_COP.1.1e The TSF shall perform **production of message authentication codes (MAC)** in accordance with a specified cryptographic algorithm **RSA SHA-1** and cryptographic key sizes **128 bits** that meet the following: **FIPS 180-2.**

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within **the range of 3 to 10** unsuccessful authentication attempts occur related to **the unsuccessful authentication attempts occurring within an administrator configurable timeframe of at least 30 minutes**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **prevent the offending user from successfully authenticating until either an administrative configurable timeframe has passed or an authorized administrator takes some action to make authentication possible for the user in question**.

5.1.3.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) identity;

b) password;

c) role(s);

d) permission(s).

5.1.3.3 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **administrator configurable password complexity rules set as follows:**

- **password length: 8 characters**
- **password composition: at least 2 non-alphabetic characters & the non-**

alphabetic characters cannot be consecutive within the password

- **password age: 60 days**
- **password reuse: prohibit reuse of 8 previous passwords**.

5.1.3.4 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow **use of the Core Services Configuration Utility** on behalf of the user to be performed before the user is authenticated.

Application Note: The authentication of the Core Services Configuration Utility is performed by the IT environment.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The remaining TSF-mediated actions occurring on behalf of users are performed by the user console, which does require the TSF-performed authentication.

FIA_UID. 1 Timing of Identification

FIA_UID.1.1 The TSF shall allow **use of the Core Services Configuration Utility** on behalf of the user to be performed before the user is identified.

Application Note: The identification of the Core Services Configuration Utility is performed by the IT environment.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The remaining TSF-mediated actions occurring on behalf of users are performed by the user console, which does require the TSF-performed identification.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.4.2 FMT_SMF.1 Specification of Management Functions

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

a. **Enable audit functions**

b. **Review audit logs**

c. **Configure log file settings**

d. **User account and password management**

e. **Password policy management**

f. Role management

g. Update content information on the TOE

h. Security check management

i. Policy template management

j. Execute reports

k. AutoSync execution

l. Configuring database communications

m. Export the Results of Running a Security Check or Policy Template

5.1.4.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **console administrator, console user**.

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

Application Note: The TOE is delivered with more pre-defined roles than defined above. These roles (e.g., NetIQ Auditor, NetIQ Help Desk, etc.) are included in the console user role defined in FMT_SMR.1.1.

5.1.5 Protection of TSF (FPT)

5.1.5.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

5.1.5.2 FPT_ITI.1 Inter-TSF Detection of Modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **at least one MAC error in SSL transmissions.**

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **a re-send of network packet(s) that caused the error** if modifications are detected.

5.1.5.3 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN_EXP.1 Explicit Audit Data Generation

FAU_GEN_EXP.1.1 The TSF shall be able to generate an audit record of the auditable events identified in Table 6.

FAU_GEN_EXP.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, Endpoint.

Functional Component	**Auditable Event**
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and actions taken and the subsequent restoration to the normal state.
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.
FIA_UAU.1	Any use of the authentication mechanism.
FIA_UID.1	All use of the user identification mechanism, including the user identity provided
FMT_MOF_EXP.1	All modifications in the behavior of the functions in the TSF.
FMT_MTD_EXP.1b, c, d, e	All modifications to the values of the TSF data, except for: o the deletion of user accounts o the creation, deletion, or modification of security checks o the creation, deletion, or modification of security templates.
FMT_SMF.1	Use of the management functions within User Console.
FMT_SMR.1	Modifications to the group of users that are part of a role.
FSC	All attempts to perform security checks, to generate security check reports and to view security check reports.

Table 6 – FAU_GEN_EXP.1 Auditable Events

5.2.2 Security Management (FMT)

5.2.2.1 FMT_MOF_EXP.1 Explicit Management of Security Functions Behaviour

FMT_MOF_EXP.1.1 The ***User Console*** shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions **listed in Table 7** to **the identified roles listed in Table 7**.

Function	Role
Auditing (except disabling)[12]	**Console Administrator**
Authentication Mechanism	**Console Administrator**
Password Policy	**Console Administrator**
AutoSync Client Configuration	**Console Administrator**

Table 7 – Security Management Functions

5.2.2.2 FMT_MTD_EXP.1a Explicit Management of TSF data - Query

FMT_MTD_EXP.1.1a The ***User Console*** shall restrict the ability to query the **TSF data listed in Table 8** to **the associated role listed in Table 8**.

TSF Data	Role
Scheduled AutoSync Update Check frequency	**Console Administrator**
Password policy	**Console Administrator**
Content information	**Console Administrator**
Audit records	**Console Administrator** **Console users with the View Task History for all Console Users permission** **Console User who performed the action**
User accounts, associated roles and permissions	**Console Administrator**
Roles	**Console Administrator**
Security checks	**Console Administrator** **Console User who created the custom security check** **Console User with associated permission**
Templates	**Console Administrator** **Console User who created the custom template** **Console User with associated permission**

Table 8 – Query TSF data

5.2.2.3 FMT_MTD_EXP.1b Explicit Management of TSF data – Create, initialize

FMT_MTD_EXP.1.1b The ***User Console*** shall restrict the ability to create the **TSF data listed in Table 9** to **the associated role listed in Table 9**.

[12] The TOE does not allow the Administrator to disable the audit function.

TSF Data	Role
User accounts and associated password, roles, and permissions	**Console Administrator**
Roles	**Console Administrator**
Security checks	**Console Administrator** **Console User**
Templates	**Console Administrator** **Console User**

Table 9 – Create/initialize TSF data

5.2.2.4 FMT_MTD_EXP.1c Explicit Management of TSF data - Modify

FMT_MTD_EXP.1.1c The ***User Console*** shall restrict the ability to modify the **TSF data listed in Table 10** to **the associated role listed in Table 10**.

TSF Data	Role
Scheduled AutoSync Update Check frequency	**Console Administrator**
Password policy	**Console Administrator**
Content information	**Console Administrator**
Account passwords	**Console Administrator** **Console User owning the password**
User accounts and associated roles, and permissions	**Console Administrator**
Roles	**Console Administrator**
Security checks	**Console Administrator** **Console User who created the custom security check** **Console User with associated permission**
Templates	**Console Administrator** **Console User who created the custom template** **Console User with associated permission**

Table 10 – Modify TSF data

5.2.2.5 FMT_MTD_EXP.1d Explicit Management of TSF data - Delete

FMT_MTD_EXP.1.1d The ***User Console*** shall restrict the ability to delete the **TSF data listed in Table 11** to **the associated role listed in Table 11**.

TSF Data	Role
Audit records	**Console Administrator**
User accounts	**Console Administrator**
Roles	**Console Administrator**
Security checks	**Console Administrator** **Console User who created the custom security check** **Console User with associated permission**
Templates	**Console Administrator** **Console User who created the custom template** **Console User with associated permission**

Table 11 – Delete TSF data

5.2.2.6 FMT_MTD_EXP.1e Explicit Management of TSF data - Export

FMT_MTD_EXP.1.1e The ***User Console*** shall restrict the ability to ***export*** the **results of running the security check or policy template** to **the Console Administrator, Console User who created the corresponding custom security check or policy template, and Console User with associated permission**.

5.2.3 Protection of TSF (FPT)

5.2.3.1 FPT_SEP_EXP.1 Partial TSF Domain Separation

FPT_SEP_EXP.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2.4 Class FSC: Security Checkups

5.2.4.1 FSC_ASM_EXP.1 Security Assessments

FSC_ASM_EXP.1.1 The TSF Agents shall collect data on the objects and security attributes for the endpoints and store that data in the SCM database.

FSC_ASM_EXP.1.2 The TSF shall perform scheduled security checks against the data stored in the SCM database at the time and frequency configured by an authorized administrator.

FSC_ASM_EXP.1.3 The TSF shall perform manually invoked security checks against the data stored in the SCM database when directed by an authorized administrator.

5.2.4.2 FSC_NAL_EXP.1 Network Security Check Alerts for Solaris

FSC_NAL_EXP.1.1 Upon detection of changes in network service activity by the Solaris Agent of the TSF, the TSF shall audit these differences and, if configured, alert the user by email.

5.2.4.3 FSC_RMT_EXP.1 Remediation Recommendations

FSC_RMT_EXP.1.1 Upon detection of a security check failure, the TSF shall provide recommendations on how to correct detected failures.

5.2.4.4 FSC_RPT_EXP.1 Security Check Reports

FSC_RPT_EXP.1.1 The TSF shall generate a security check report based on the results of the security checks performed by the TOE.

FSC_RPT_EXP.1.2 The TSF shall generate a security check report in a manner suitable for the user to interpret the information.

5.2.4.5 FSC_REV_EXP.1 Security Check Report Review

FSC_REV_EXP.1.1 The TSF shall provide the Console Administrator and Console User who ran the security check report with the capability to read all information contained in the security check report.

5.2.4.6 FSC_SDI_EXP.1 Security attribute integrity

FSC_SDI_EXP.1.1 The TSF shall monitor files on the operating system for security attribute modifications, based on the following attributes: owner, group, permission or access control bits.

FSC_SDI_EXP.1.2 Upon detection of a security attribute integrity error, the TSF shall generate an audit record.

5.2.4.7 FSC_SDI_EXP.2 Stored Solaris content integrity

FSC_SDI_EXP.2.1 The Solaris Agent TSF shall monitor files on the Solaris operating system for content integrity errors, based on the file's hashed values stored within the systems most recently updated database.

FSC_SDI_EXP.2.2 Upon detection of a content integrity error, the Solaris Agent TSF shall generate an audit record.

5.2.4.8 FSC_SDI_EXP.3 Solaris Network Security Checks

FSC_SDI_EXP.3.1 The Solaris Agent of the TSF shall monitor the network ports to identify which are actively listening for a connection.

FSC_SDI_EXP.3.2 The Solaris Agent of the TSF shall provide the ability to detect changes in network service activity by comparing current activity with defined baseline activity.

5.3 IT Environment Security Requirements

The SFRs on the IT environment defined in this section are taken from Part 2 of the CC. Note: The SCM DB and the operating systems (OS) of Core Services and Agent systems are all in the IT environment. (Note: The OS of the Core Services is also the OS of the SCM DB since they are co-located on the same host.)

5.3.1 Security Audit (FAU)

5.3.1.1 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The ***IT Environment*** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The ***IT Environment*** shall be able to prevent unauthorised modifications to the audit records in the audit trail.

5.3.2 User Data Protection (FDP)

5.3.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The ***OS of the Core Services and Agent machines*** shall enforce the **Discretionary Access Control Policy** on **all processes, all named objects used by the TOE, and all read/view, write/update, and execute operations among subjects and objects covered by the SFP**.

5.3.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The ***OS of the Core Services and Agent machines*** shall enforce the **Discretionary Access Control Policy** to ***named*** objects ***used by the TOE*** based on the following ***types of subject and object security attributes***:

a) The authorized user identity and group membership associated with a subject and

b) The authorized user (or group) identity, access operations pairs associated with a named object.

FDP_ACF.1.2 The ***OS of the Core Services and Agent machines*** shall enforce the following rules to determine if an operation among controlled subjects and controlled ***named*** objects ***used by the TOE*** is allowed:

a) If the requested mode of access is denied to an authorized user identity or group membership associated with the subject, deny access

b) If the requested mode of access is granted to an authorized user identity or group membership associated with the subject, grant access

c) Else deny access.

FDP_ACF.1.3 The ***OS of the Core Services and Agent machines*** shall explicitly authorize access of subjects to ***named*** objects ***used by the TOE*** based on the following additional rules: **superusers (e.g., root) or users with privilege to override the DAC policy are always granted access.**

FDP_ACF.1.4 The ***OS of the Core Services and Agent machines*** shall explicitly deny access of subjects to ***named*** objects ***used by the TOE*** based on the **no explicit deny rules.**

5.3.2.3 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The ***IT Environment*** shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to the following objects: **all objects used by the TOE**.

5.3.3 Identification and Authentication (FIA)

5.3.3.1 FIA_UAU.2a User Authentication before any action – SCM DB

FIA_UAU.2.1a The ***SCM DB*** shall require each user to be successfully authenticated before allowing any other ***database-mediated*** actions on behalf of that user.

5.3.3.2 FIA_UAU.2b User Authentication before any action – OS

FIA_UAU.2.1b The ***OS of the Core Services and Agent machines*** shall require each user to be successfully authenticated before allowing any other ***TOE-related*** actions on behalf of that user.

5.3.3.3 FIA_UID.2a User Identification before any action – SCM DB

FIA_UID.2.1a The ***SCM DB*** shall require each user to identify itself before allowing any other ***database-mediated*** actions on behalf of that user.

5.3.3.4 FIA_UID.2b User Identification before any action – OS

FIA_UID.2.1b The ***OS of the Core Services and Agent machines*** shall require each user to identify itself before allowing any other ***TOE-related*** actions on behalf of that user.

5.3.4 Protection of TSF (FPT)

5.3.4.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The ***IT Environment*** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.3.4.2 FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The ***IT Environment*** shall maintain a security domain for ***the TOE's*** execution that protects ***the TOE*** from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ***IT Environment*** shall enforce separation between the security domains of subjects in the TSC.

5.3.4.3 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The ***IT Environment*** shall be able to provide reliable time stamps for ***the TOE's*** use.

5.4 Explicitly Stated IT Environment Security Functional Requirements

This ST does not define any explicitly stated IT environment SFRs.

5.5 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms. Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The claimed minimum strength of function is SOF-basic. FIA_SOS.1 and FIA_UAU.1 are the only non-cryptographic TOE security functional requirements that contain a permutational function.

5.6 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) as defined by the CC. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 12 – Assurance Requirements: EAL2

5.6.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.2 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

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

5.6.3 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

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

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.6.4 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

5.6.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or

software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

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

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.6.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

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

5.6.7 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

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

5.6.8 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

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

5.6.9 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

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

5.6.10 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

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

5.6.11 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.6.12 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

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

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.6.13 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

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

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.7 Rationale For TOE Security Requirements

5.7.1 TOE Security Functional Requirements

	O.AUD_GEN	O.AUD_PROT	O.AUD_REVIEW	O.CNT_PROT	O.CRYPTO	O.MANAGE	O.PART_SELF_PROT	O.SECURE_COMM	O.SECURE_CHK	O.TOE_ACCESS
FAU_GEN_EXP.1	X									
FAU_GEN.2	X									
FAU_SAR.1a, b			X							
FAU_SAR.2		X								
FAU_SAR.3			X							
FCS_CKM.1								X		
FCS_CKM.2								X		
FCS_COP.1a, b					X				X	
FCS_COP.1c, d, e								X		
FIA_AFL.1										X
FIA_ATD.1										X
FIA_SOS.1										X
FIA_UAU.1										X
FIA_UID.1										X
FMT_MOF_EXP.1				X		X				
FMT_MSA.2								X		
FMT_MTD_EXP.1a, b, c				X		X				
FMT_MTD_EXP.1d		X		X		X				
FMT_MTD_EXP.1e						X				
FMT_SMF.1						X				
FMT_SMR.1						X				
FPT_ITC.1								X		
FPT_ITI.1								X		
FPT_ITT.1								X		
FPT_SEP_EXP.1							X			

	O.AUD_GEN	O.AUD_PROT	O.AUD_REVIEW	O.CNT_PROT	O.CRYPTO	O.MANAGE	O.PART_SELF_PROT	O.SECURE_COMM	O.SECURE_CHK	O.TOE_ACCESS
FSC_ASM_EXP.1									X	
FSC_NAL_EXP.1									X	
FSC_REV_EXP.1									X	
FSC_RMT_EXP.1									X	
FSC_RPT_EXP.1									X	
FSC_SDI_EXP.1									X	
FSC_SDI_EXP.2									X	
FSC_SDI_EXP.3									X	

Table 13 – TOE SFR and Security Objectives Mapping

O.AUD_GEN — FAU_GEN_EXP.1 defines the set of security-relevant events that the TOE must be capable of recording (all such events are performed from the User Console). This requirement also defines the information that must be contained in the audit record for each auditable event. FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, this association is accomplished with the user identifier. In all other cases, this association is based on the endpoint identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.

O.AUD_PROT — FAU_SAR.2 restricts the ability to read the audit trail to the Console Administrator, console users with the View Task History for all Console Users permission and the console user who performed the activity audited, thus preventing the disclosure of the audit data to any other users. The TOE does not prevent the disclosure of audit data that has been archived, copied, or moved. FMT_MTD_EXP.1d limits the ability to delete audit records to the Console Administrator.

O.AUD_REVIEW — FAU_SAR.1a, FAU_SAR.1b and FAU_SAR.3 provide the ability to review the audit records in a user-friendly manner. The console administrators and console users with the View Task History for all Console Users permission can review all audit records. Other console users can read the audit records produced by their own actions.

O.CNT_PROT	FMT_MOF_EXP.1 defines particular management capabilities provided by the User Console that can be used only by select users. FMT_MTD_EXP.1a, FMT_MTD_EXP.1b, FMT_MTD_EXP.1c, and FMT_MTD_EXP.1d define particular TOE data that using the User Console may be queried, created, and altered only by users with select roles.
O.CRYPTO	FCS_COP.1a requires that the TOE be able to calculate message digests to verify the integrity of files. FCS_COP.1b requires that the TOE provide the ability to decrypt and verify digital signatures to verify the integrity of content updates.
O.MANAGE	FMT_MOF_EXP.1 defines particular TOE management capabilities provided by the User Console that can be used only by select users. FMT_MTD_EXP.1a, FMT_MTD_EXP.1b, FMT_MTD_EXP.1c, and FMT_MTD_EXP.1d define particular TOE data that using the User Console may be queried, created, and altered only by users with select roles. FMT_MTD_EXP.1e defines who can export the results of running security checks and policy templates. FMT_SMF.1 defines the administrative functions provided by the TOE. FMT_SMR.1 defines the roles provided by the TOE.
O.PART_SELF_PROT	FPT_SEP_EXP.1 was chosen to ensure the TSF provides a domain that protects itself from untrusted users. The explicitly stated version was used to distinguish the aspects of FPT_SEP provided by the TOE from the aspects provided by the IT environment.
O.SECURE_COMM	FPT_ITT.1 ensures that the TOE provides secure communication between the distributed portions of the TOE. FPT_ITC.1 ensures that the user console protects communications from unauthorized disclosure when data is transmitted to the SCM database (remote trusted IT product). FPT_ITI.1 ensures that the user console protects communications from modification and ensures its integrity when the data is transmitted to the SCM database (remote trusted IT product). (Note: Since Core Services and the SCM DB are co-located on the same host machine, the SCM DB is not considered a remote trusted IT product for Core Services so the communications between Core Services and the SCM DB are not secured by IT mechanisms.) FCS_CKM.1 requires that the TOE generates cryptographic keys. FCS_CKM.2 and FCS_COP.1d requires that the TOE distribute cryptographic keys via Diffie-Hellman. FCS_COP.1c requires that the TOE provide the ability to encrypt and decrypt sessions. FCS_COP.1e requires that the TOE provide the ability to produce message

	authentication codes. FMT_MSA.2 requires that the TOE provide secure cryptographic keys for use during cryptographic operations.
O.SECURE_CHK	FSC_SDI_EXP.1 ensures that the TOE provides the ability to detect security attribute modifications on select files and generate an audit record when a modification is detected. FSC_SDI_EXP.2 also ensures that the Solaris Agent of the TSF can monitor select files for content modifications and generate an audit record when a content integrity error is detected. FCS_COP.1a requires that the TOE be able to calculate message digests to verify the integrity of files on the Solaris endpoints. FSC_ASM_EXP.1 ensures that the TOE provides the ability to perform security checks that are used to identify vulnerabilities and assess policy conformance. FSC_NAL_EXP.1 ensures that the TOE will generate audit records and alerts for network security checks on Solaris systems. FSC_SDI_EXP.3 ensures that the TOE can detect network security issues on Solaris systems. FSC_RMT_EXP.1 ensures that the TOE provides the ability to run tasks on the operating system to correct a failure discovered during a security check. FSC_RPT_EXP.1 ensures that the TOE generates reports summarizing the results of the security check. Console administrators and console users with the View Task History for all Console Users permission are allowed to generate all reports. Other console users are able to generate reports for the actions they have performed. FSC_REV_EXP.1 ensures that the TOE provides the ability for users to review the reports that they have generated.
O.TOE_ACCESS	FIA_AFL.1 provides a detection mechanism for unsuccessful authentication attempts by all users. The requirement enables a configurable threshold that prevents unauthorized users from gaining access to authorized user's account by guessing authentication data by locking the targeted account after an administrator configured number of consecutive unsuccessful attempts. FIA_ATD.1 ensures that for each user the TOE maintains a set of security attributes, which are used to make logical TOE access decisions. FIA_SOS.1 ensures that the strength of the user password meets a set of requirements configured by the administrator to meet the requirements of the evaluated configuration. FIA_UID.1 requires that a user be identified to the TOE in order to access the TOE, except when using the Core Services Configuration Utility. FIA_UAU.1 requires that a user be authenticated to the TOE before accessing the TOE, except when using the Core Services Configuration utility.

5.7.2 TOE Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

5.8 Rationale For IT Environment Security Requirements

	OE.AUD_STORAGE	OE.DOMAIN_SEP	OE.NO_BYPASS	OE.RESIDUAL	OE.TIME_STAMPS	OE.TSF_DATA_PROT
FAU_STG.1	X					
FDP_ACC.1	X					X
FDP_ACF.1	X					X
FDP_RIP.1				X		
FIA_UAU.2a	X					X
FIA_UAU.2b	X					X
FIA_UID.2a	X					X
FIA_UID.2b	X					X
FPT_RVM.1			X			
FPT_SEP.1		X				
FPT_STM.1					X	

Table 14 – IT Environment SFR and Security Objectives Mapping

OE.AUD_STORAGE FAU_STG.1 requires the operating system and database to protect the audit logs from unauthorized deletion. FIA_UID.2a and FIA_UAU.2a require the SCM database of the IT environment to require all users to identify and authenticate themselves before performing any database actions. (Note: The audit logs are stored in the database.) FIA_UID.2b and FIA_UAU.2b require the OS of the machine on which the SCM DB (and Core Services) resides to enforce identification and authentication of all users before performing any actions which could affect the DB. FDP_ACC.1 and FDP_ACF.1 require that the OS of the DB enforces discretionary access controls to ensure that the DB files stored in the file system are protected from unauthorized access. (Note: The DB and Core Services reside on the same host machine.)

OE.DOMAIN_SEP FPT_SEP.1 requires the operating system to provide an isolated domain for the TOE to execute within.

OE.NO_BYPASS FPT_RVM.1 requires the operating system to ensure that the TOE will not be bypassed.

OE.RESIDUAL FDP_RIP.1 requires the operating system to ensure that the contents of TOE resources are not available to subjects other than those explicitly granted access to the data.

OE.TIME_STAMPS FPT_STM.1 requires that the IT environment provide time stamps for the TOE's use.

OE.TSF_DATA_PROT FIA_UID.2a and FIA_UAU.2a require the SCM database of the IT environment to require all users to identify and authenticate themselves before performing any database actions. This protects the TSF data stored in the SCM database from disclosure and modification by unauthorized users by requiring all users to login prior to accessing the SCM database. The administrator guidance will instruct the administrator to ensure that logins are required for all DB access. FIA_UID.2b and FIA_UAU.2b require the OS of Core Services (and DB) and Agent machines enforce identification and authentication of all users before performing any actions which could affect the TSF or DB. FDP_ACC.1 and FDP_ACF.1 require that the OS of Core Services (and DB) and Agent machines enforce discretionary access controls to ensure that the TSF data stored in the file system (including executables, plain text files, and database files) are protected from unauthorized access.

5.9 Rationale for Explicitly Stated Security Requirements

Table 15 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FAU_GEN_EXP.1	Explicit audit data generation	The FAU_GEN.1 SFR from CC Part 2 requires that the TOE generate an audit record for the start-up and shutdown of the audit functions. The NetIQ SCM does not generate an audit record for the start-up and shutdown of the audit functions, so the audit data generation requirement was explicitly stated.
FMT_MOF_EXP.1	Explicit Management of Security Function Behaviour	The FMT_MOF SFR from CC Part 2 applies to all interfaces within the TSF which perform the defined functionality. However in the TOE, the ability to restrict what role can perform the defined functions is only provided by the User Console, not by the SCM Core Services Configuration Utility.

Explicit Requirement	Identifier	Rationale
FMT_MTD_EXP.1a, b, c, d, e	Explicit Management of TSF data	The FMT_MTD SFR from CC Part 2 applies to all interfaces within the TSF which control access to TSF data. However, the ability to restrict what role can operate on the TSF data is only provided by the User Console, not by the SCM Core Services Configuration Utility.
FPT_SEP_EXP.1	Partial TSF domain separation	The FPT_SEP SFR from CC Part 2 cannot be completely satisfied by an application TOE. This component defines the separation that may be performed by applications.
FSC_ASM_EXP.1	Security Assessments	This component defines the scanning features to be performed by the TOE to detect security-related issues. Existing SFRs in CC Part 2 are not suitable for the scanning features performed by vulnerability management products.
FSC_NAL_EXP.1	Network Security Check Alerts for Solaris	This component defines the alerting features to be used by the TOE to inform users when a Solaris network security check detects an issue. The SFRs provided in CC Part 2 (e.g., FAU_ARP.1) are not suitable for this feature since they do not provide a method for restricting the type of security violations that can cause an alert.
FSC_REV_EXP.1	Security Check Reports Review	This component defines the report review features to be provided by the TOE. Existing SFRs in CC Part 2 are not suitable for viewing security check reports. The FAU class of requirements provides for the review of audit records, not security checks.
FSC_RMT_EXP.1	Remediation Recommendations	This component provides recommendations to be taken by the TOE when a security check detects an issue. Existing SFRs in CC Part 2 are not suitable for the actions taken by vulnerability management products.
FSC_RPT_EXP.1	Security Check Reports	This component defines the report generation features to be provided by the TOE. Existing SFRs in CC Part 2 are not suitable for the generation of reports resulting from security checks. The FAU class of requirements operates on audit records, not security checks.
FSC_SDI_EXP.1	Security attribute integrity	This component defines the security attribute integrity protection capabilities performed by the TOE. This requirement is necessary because the existing CC data integrity SFRs (e.g., FDP_SDI.1 and FDP_SDI.2) focus on the integrity of user data stored in the TSC and are not suitable for monitoring data in the IT environment.

Explicit Requirement	Identifier	Rationale
FSC_SDI_EXP.2	Stored Solaris content integrity	This component defines the content integrity protection capabilities performed by the Solaris Agent of the TOE. This requirement is necessary because the existing CC data integrity SFRs (e.g., FDP_SDI.1 and FDP_SDI.2) focus on the integrity of user data stored in the TSC and are not suitable for monitoring data in the IT environment.
FSC_SDI_EXP.3	Network Security Checks for Solaris	This component defines the scanning features to be performed by the TOE to detect Solaris network security-related issues. Existing SFRs in CC Part 2 are not suitable for monitoring the integrity of network settings.

Table 15 – Explicitly Stated SFR Rationale

5.10 Rationale For IT Security Requirement Dependencies

This section includes a table of the requirements, their dependencies and a rationale for any dependencies that are not satisfied.

Functional Component	Dependency	Included / Rationale
FAU_GEN_EXP.1	FTP_STM.1	YES
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	YES, via FAU_GEN_EXP.1
FAU_SAR.1a, b	FAU_GEN.1	YES, via FAU_GEN_EXP.1
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	NO for FCS_CKM.4 (see below for rationale)
FCS_CKM.2	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	NO for FCS_CKM.4 (see below for rationale)

Functional Component	Dependency	Included / Rationale
FCS_COP.1a	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	NO These dependencies are for key management of the keys used by the cryptographic operation. This cryptographic function is a message digest, which does not use keys. So these dependencies do not apply since they provide for key management which is not required to provide message digest verification.
FCS_COP.1b	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	NO These dependencies are for key management of the keys used by the cryptographic operation. This cryptographic operation performed by the TOE does not perform or rely upon key management. A 1024-bit RSA public key is distributed with NetIQ SCM. The corresponding 1024-bit RSA private key is kept and protected by NetIQ Corporation.
FCS_COP.1c, d, e	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	NO for FCS_CKM.4 (see below for rationale)
FIA_AFL.1	FIA_UAU.1	YES
FIA_ATD.1	None	N/A
FIA_SOS.1	None	N/A
FIA_UAU.1	FIA_UID.1	YES
FIA_UID.1	None	N/A
FMT_MOF_EXP.1	FMT_SMF.1 FMT_SMR.1	YES

Functional Component	Dependency	Included / Rationale
FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	NO FMT_MSA.2 is for secure keys generated for use in FCS_COP.1c – e. Therefore, these dependencies are for key management of these keys. The keys used in these operations are generated by the TOE and cannot be modified or managed by users. In addition, these keys are temporary and are destroyed when the associated session is terminated.
FMT_MTD_EXP.1a, b, c, d, e	FMT_SMF.1 FMT_SMR.1	YES
FMT_SMF.1	None	N/A
FMR_SMR.1	FIA_UID.1	YES
FPT_ITC.1	None	N/A
FPT_ITI.1	None	N/A
FPT_ITT.1	None	N/A
FPT_SEP_EXP.1	None	N/A
FSC_ASM_EXP.1	None	N/A
FSC_NAL_EXP.1	FSC_SDI_EXP.3	YES
FSC_REV_EXP.1	FSC_RPT_EXP.1	YES
FSC_RMT_EXP.1	FSC_ASM_EXP.1 FSC_SDI_EXP.1 FSC_SDI_EXP.2 FSC_SDI_EXP.3	YES
FSC_RPT_EXP.1	FSC_ASM_EXP.1	YES
FSC_SDI_EXP.1	None	N/A
FSC_SDI_EXP.2	FCS_COP.1a	YES
FSC_SDI_EXP.3	None	N/A

Table 16 – SFR Dependencies

The dependencies of FCS_CKM.1, FCS_CKM.2, FCS_COP.1c, d, e on FCS_CKM.4 (cryptographic key destruction) are not explicitly met by the TOE. These cryptographic TOE

SFRs are realized in the TOE by a TLS/SSL implementation and the negotiation of TLS/SSL session keys. The TLS/SSL session keys are generated and valid only for the current session, so the use of key destruction to prevent key reuse is not necessary. The RSA private/public keys used to generate session keys are protected by environmental assumptions on the SCM Core Services middleware system (A.NOEVIL, A.PHYS_SEC, A.CS_ACCTS, and A.DEDICATED) and the Protection of the TOE security function (FPT_SEP_EXP.1).

5.11 Rationale For Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes SFRs to represent all security functionality provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying dependencies as demonstrated in Table 16 – SFR Dependencies
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.7.1
- including the SFRs FPT_SEP_EXP.1, FPT_RVM.1 and FPT_SEP.1 to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

5.12 Rationale For Strength of Function Claim

The rationale for choosing SOF-basic is based on the low to moderate attack potential of threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE, which include password composition rules.

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE is comprised of seven different security functions:

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

Note: The SCM database mentioned in the following sections is in the IT environment.

6.1.1 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 and console users with the View Task History for all Console Users permission can view the history of other users.

The user can view the following fields from the console history interface: Console User, Submitted Date & Time, Completed Date & Time, Endpoint, status, and task type.

The user can sort the audit records by any of the fields presented in the history interface. The user can also request to filter the audit records based on match criteria for one or more of the fields presented in the history interface.

Audit records are stored in the SCM database. The database administrator is responsible for developing database backup, archival and recovery plans.

Security audit generation: FAU_GEN_EXP.1, FAU_GEN.2

Audit data is generated by the NetIQ SCM Core Services and the NetIQ Security Agents. Audit data includes audit records for each of the auditable events specified in Table 6 – FAU_GEN_EXP.1 Auditable Events.

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. Examples of types of events are Admin, Report, and Security Checkup. 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 since these subjects are not authenticated.

Audit review: FAU_SAR.1a, FAU_SAR.1b, FAU_SAR.2, FAU_SAR.3

The TOE provides an interface which can be used by authorized users to view the audit records. The Console Administrators and console users with the View Task History for all Console Users permission have the ability to read all audit records. The console user who performed the action has the ability to read their corresponding audit records. The TOE restricts console users from reading audit records for actions they did not perform.

The audit review functionality also allows for audit records to be sorted and/or selected based on the user identity, date and time of the event, endpoint, and the type of the event (e.g., Admin, Report, and Security Checkup).

6.1.2 Cryptographic Operations

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.

Message Digest: FCS_COP.1a

The TSF provides the ability to calculate a message digest for data using the MD5 algorithm, which meets the ANSI RFC 1321 standard. The message digest operations are used to verify the content integrity of selected files on SOLARIS endpoints.

Decryption and Signature Verification: FCS_COP.1b

The TOE provides the ability to decrypt data using 128-bit and 256-bit AES, which meets the FIPS-PUB 197 standard. The decryption operation is used by the AutoSync client to protect the content updates from unauthorized disclosure. An AES key is generated for each package and scrambled by the packaging tool at NetIQ Corporation (which is not part of the TOE). The AES key and the encrypted content updates are transmitted to the AutoSync client on the SCM Core Services.

In addition, the TOE provides the ability to verify digital signatures using a 168-bit secure RSA SHA-1 hash with a 1024-bit RSA public key that meets the ANSI X9.31 Part 2 standard. The 1024-bit RSA public key is distributed with the TOE. The signature verification operation is used by the AutoSync client to verify the integrity of the content updates received from NetIQ Corporation.

6.1.3 Identification 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.

Identification and Authentication: FIA_UAU.1, FIA_UID.1

Users log into the SCM Core Services via the user console. User identification and authentication must take place before the user can perform any other actions. The only authentication method allowed in the evaluated configuration is the console authentication (username and password) performed by NetIQ SCM Core Services. The user enters their username and password to login to SCM Core Services. NetIQ SCM Core Services computes a hash of the password, retrieves the hashed password associated with the username from the SCM database and compares the two hashed values. If the values match, the user login succeeds.

The password authentication mechanism is realized by a probabilistic or permutational security mechanism.

Use of the Core Services Configuration utility to administer the TOE is protected via the physical security of the SCM Core Services system as well as the underlying operating system of the SCM Core Services.

User Attributes: FIA_ATD.1

The TOE manages user attributes that are stored in the SCM database in the IT environment. The user attributes maintained by the TOE are the user identity, authentication data (password), role(s) assigned, and permissions assigned. See Section 6.1.5 for a detailed description of roles and permissions.

Verification of Secrets: FIA_SOS.1

The password policy provides the ability to configure the password age and password strength. The password age parameter defines the maximum age for a password. The password strength parameters include defining the minimum length of a password, the number of previous passwords saved to prohibit reuse, and the number of non-alphabetic characters required.

In the CC-evaluated configuration, the administrator is instructed to define the password policy as follows:

- Enforce password discipline
- Password Age
  - Expires in 60 days
- Password Strength
  - Minimum length: 8 characters
  - Prohibit: 8 previous passwords
  - At least 2 non-alphabetic characters
  - Non-alphabetic characters cannot be consecutive within password

The verification of secrets is realized by a probabilistic or permutational security mechanism. The administrator guidance instructs the Console Administrator to set the password policy parameters to values that will be suitable to meet the claim of SOF-basic.

Authentication Failure Handling: FIA_AFL.1

The password policy provides the ability to configure the console account lockout parameters. The console account lockout parameters define the number of unsuccessful consecutive attempts allowed (the account lockout threshold) within a defined time interval (the reset duration) before the account is locked out. The console account lockout parameters also define the duration for which an account is locked out. The administrator guidance instructs the Console Administrator to set the account lockout threshold to a value between 3 and 10, the reset duration to at least 30 minutes and the account lockout duration for at least one day.

6.1.4 Secure Communications

The TOE uses TLS[13] 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.

The TOE uses a combination of 56-bit DES and Diffie-Hellman key exchange[14] to secure communication sessions between the SCM Core Services and a user console that are initiated by the user console. The Diffie-Hellman key exchange is used to generate a temporary shared key used to secure communications for each session. This shared key is used to encrypt the communication using 56-bit DES.

The TOE uses SSL (which is described above) to secure communications between the SCM Core Services and a user console that are initiated by the SCM Core Services. The SCM Core Services initiates communications for a few items such as notifications when reports are completed or new content is available from the AutoSync server. (Most of the communications between the SCM Core Services and a user console are initiated by the user console.)

The SCM User Console also uses SSL to secure communications with the SCM DB, which is hosted on the same machine as the SCM Core Services.

The standards met and key sizes used by the algorithms implementing the secure communications are defined in Section 5.1.2.

Key Management: FCS_CKM.1

The TOE provides the ability to generate temporary shared keys for use in TLS or SSL sessions.

Encryption and Decryption: FCS_COP.1c

The TOE provides the ability to encrypt/decrypt session data using 56-bit DES.

Internet Key Exchange: FCS_CKM.2, FCS_COP.1d

---

[13] The evaluation laboratory did not evaluate the cryptography related to these TLS or SSL sessions.

[14] The evaluation laboratory did not evaluate the cryptography related to these communications.

The TOE uses Diffie-Hellman key exchanges initiated by the console. The Diffie-Hellman key exchange is used to generate a temporary shared key used to secure communications for each session. This shared key is used to encrypt the rest of the session using 56-bit DES.

Message authentication codes: FCS_COP.1e

The MAC is generated for the transmitted data and is used in TLS/SSL.

Secure security attributes: FMT_MSA.2

The generation of secure cryptographic keys used in TLS/SSL is required. The keys are generated by the TOE to meet the RFC 2246 (TLS v1) symmetric key and secret generation standard.

Internal TSF Data Transfer Protection: FPT_ITT.1

Data is protected from disclosure and modification during transmission between the SCM Core Services and the SCM Agents by use of TLS version 1.0. The TOE is also capable of supporting SSL Versions 2 or 3 sessions for backwards compatibility.

Data is protected from disclosure and modification during transmission between the SCM Core Services and the user console that is initiated from the console using a combination of 56-bit DES and Diffie-Hellman key exchange.

Data is protected from disclosure and modification during transmission between the SCM Core Services and a remote console that is initiated from SCM Core Services by use of SSL Versions 2 or 3.

Inter-TSF Confidentiality and Integrity: FPT_ITC.1, FPT_ITI.1.

The TOE uses SSL over TCP/IP to provide a secure communication channel between the user console and the SCM database. 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 modifications to the transmitted data. Integrity violations are detected if at least one MAC error is found in an SSL transmission. If such integrity violations occur, the TOE will re-send network packet(s) that caused the error. The SCM DB is co-located with the SCM Core Services, so the SCM DB is not considered a *remote* IT product by the SCM Core Services.

6.1.5 Security Management

The TOE provides security management functions and tools to manage the security features it provides. In addition, the TOE provides permissions to determine what security management functions a particular user can perform.

Security Management: FMT_MOF_EXP.1, FMT_SMF.1

The TOE provides functions for the administrator to manage the TOE security features. It also restricts who can use these security functions from within the User Console. The ability to perform a specific job function within the User Console is determined by the user's permissions which may be provided by their assigned role(s). When a user logs into NetIQ User Console,

they assume the permissions and role that their account has been assigned. Refer to Table 7 – Security Management Functions for a list of the management functions and what roles can perform those functions.

The TOE management tools perform the following functions:

- view audit configuration
- enable and configure auditing
- review audit logs
- manage user accounts (including permissions) and passwords
- manage password policies
- manage roles
- manage security checks
- manage policy templates
- update content information on the TOE
- execute reports
- remediate actions
- execute AutoSync
- configuring database communications
- export the results of running a security check or policy template via sending an email or writing it onto a hard disk available on the Core Services system. (Note: This could be a network share.)

TSF Data Management: FMT_MTD_EXP.1a, FMT_MTD_EXP.1b, FMT_MTD_EXP.1c, FMT_MTD_EXP.1d., FMT_MTD_EXP.1e

The User Console provides functions for the administrator to manage the TSF data and restrict who can manage the TSF data. Refer to Table 8 – Query TSF data for the TSF data that can be queried from the User Console and what role is needed to perform the query. Refer to Table 9 – Create/initialize TSF data for the TSF data that can be created from the User Console and what role is needed create/initialize the data. Refer Table 10 – Modify TSF data to for the TSF data that can be modified from the User Console and what role is needed to modify the data. Refer to Table 11 – Delete TSF data for the TSF data that can be deleted from the User Console and what role is needed to delete the data.

The User Console provides the ability to export the results of running the security check or policy template to the Console Administrator, Console User who created the corresponding custom security check or policy template, and Console User with associated permission.

Security Roles: FMT_SMR.1

The TOE implements roles by assigning console permissions to user accounts or by assigning defined roles to user accounts. A role in NetIQ SCM is a set of permissions that controls access to specific functionality from within the User Console. Roles can be used to allow or deny a

console user the ability to perform certain actions or run certain reports. Permissions provide users with the ability to perform a specific job function, such as audit all Solaris servers or run particular reports. When a user logs into NetIQ SCM, they assume the roles and permissions that their account has been assigned.

This ST defines two logical roles: the Console administrator and the Console user. Note: The security management functions that the user is allowed to perform are defined via the console permissions assigned to the user or to the roles to which the user has been assigned. The TOE is delivered with more than 2 pre-defined roles. These additional roles (e.g., NetIQ Auditor, NetIQ Help Desk, etc.) are included in the console user role.

Both roles are administrative in nature. NetIQ SCM does not support any non-administrative users or functions. All TOE users perform some administrative function on the box whether it be running and reviewing reports on select systems or managing the security functionality of NetIQ SCM itself.

The Console Administrator role is defined as a user who has the permissions necessary to perform the following security functions:

- implement and modify external authentication (which must be disabled in the evaluated configuration)
- implement and modify password policy
- reset console user and console administrator account passwords
- create console user accounts
- create, copy, and modify roles
- assign permission to roles or console users
- perform SCM actions and generate reports
- enable and configure audit functions
- manage AutoSync Check Update frequency
- manage audit records
- manage content information
- manage security checks

Console users are administrative users that are not console administrators. They may be assigned a custom role or one of the default roles (e.g., NetIQ Auditor, NetIQ Help Desk, NetIQ iSeries Admin). Console users can obtain access to perform a specific job function by being assigned the necessary permission directly or by being assigned a role which contains the necessary permission.

The administrator guide describes all security-related console permissions and roles and provides guidance on how and when to assign them to user accounts.

6.1.6 Protection of TOE functions

Partial TSF Domain Separation: FPT_SEP_EXP.1

The User Console external interfaces to the TOE ensure that users must login prior to accessing other TOE resources. The TOE maintains a separate session for each interaction with the TOE.

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 only provide user accounts to SCM Core Services administrative users.

6.1.7 Security Assessment

Security assessments check endpoint (operating system or software application) configurations and compare them against a set of expected values. Examples of configuration characteristics that can be checked are:

- File and directory security attributes (such as, owner identifier, group identifier, permissions or access control lists)
- Password Rules (such as password age, password length, etc.)
- Users with no password or expired password
- Disabled users
- Services executing
- Groups with no users
- Audit settings
- Network shares

Security assessments are performed by maintaining and checking against a set of templates. A template is a collection of security checks against a defined set of security controls and system configurations. Agents collect data from endpoints and store the collected data in the SCM database. A security check gathers the requested data, returns the data to Core Services, and places the data in the completed job queue. The results to the security check are then made available to the administrative user in the completed job queue. The requested data is either gathered by the Agents at the time of the request or from information previously gathered and stored in the DB. The customer can create their own custom security checks and scoring methods. Administrator guidance provides the users with a list of checks that can be performed by NetIQ SCM. NetIQ SCM provides a wizard to simplify the creation of custom security checks. Custom security checks are supported on NetIQ SCM Solaris and Windows agents.

Security assessments can be run as needed or scheduled to occur regularly to ensure on-going policy compliance. When a security assessment is performed, the TOE evaluates each endpoint against the expected security settings and generates a report which includes a security risk score.

The security risk score represents how well the endpoint matched the expected security settings. Risk-based reports highlight the most critical and most at-risk systems, provide executive-level summaries, and supply the information necessary for taking corrective actions.

The Agents execute on the host operating system in privileged mode in order to check the system configuration settings and services. On Solaris operating systems, the Agents run as root. On Windows operating systems, the Agents run as an account which is a member of the Domain Administrators group in the domain of the managed computer or when running locally as a member of the Administrators group.

Integrity Checking: FSC_SDI_EXP.1, FSC_SDI_EXP.2, FSC_SDI_EXP.3

The NetIQ Security Agents can detect object (e.g., file or directory) attribute values (owner identifier, group identifier, permission bits or access control lists, etc.) that are different than expected, as defined by the security check or template.

NetIQ Security Agents for Solaris can take a snapshot of the files, directories and network configuration for quick identification of changes later. This baseline can be used to detect changes by comparing the expected attribute values of files, directories and network ports to the current values. File and directory baselining covers not only file and directory settings but also MD5 hashes to ensure the detection of changes as small as a single bit. Network baselining detects changes to open ports and network services on a supported Solaris platform.

Security Checks: FSC_ASM_EXP.1

Agents collect data from endpoints and store the collected data in the SCM database. The data collected includes information on objects and security attributes. A security check gathers the requested data, returns the data to Core Services, and places the data in the completed job queue. The results to the security check are then made available to the administrative user in the completed job queue. The requested data is either gathered by the Agents at the time of the request or from information previously gathered and stored in the DB. Security assessments can be run as needed or scheduled to occur regularly to ensure on-going policy compliance.

A security check verifies that a system configuration is properly implemented based on a pre-defined, expected configuration. NetIQ SCM includes out-of-the-box, pre-defined security checks to evaluate the most common security controls. The pre-defined security checks include expected values of security controls, penalties, risk values, and remedies.

A policy compliance template is a collection of security checks against a defined set of security policies and best practices. Vulnerability scanning is also implemented by a collection of security checks against a set of security controls known to cause or represent vulnerabilities.

Security Check Reporting: FSC_RPT_EXP.1, FSC_REV_EXP.1

The TOE automatically generates a report after performing a security check. The resulting reports provide the information needed to assess the security of the assets, to show audit and policy compliance, to identify potential vulnerabilities, to identify high-risk systems, and to assess the risk. The report assists in assessing the risk by providing a security risk score based on the risk scoring parameters defined by the administrator. When available, the reports also provide suggested remediation checklists. Administrators are able to customize their reports to

easily evaluate systems against the company security policies.

The risk score is determined by importance levels assigned to IT assets. Administrators 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 importance level of medium. Each importance level is mapped to a percentage.

The TOE also provides a delta reporting capability which compares two existing reports to allow authorized administrators to easily identify and monitor system changes. This feature compares reports and should not be confused with baselining which compares the security attributes and configurations of endpoints. Baselines are not included in the CC evaluated configuration.

The TOE provides a report viewer that allows administrators to view reports during their generation and after the report completion. The TOE also provides an interface to print the security reports. The reports can be viewed by the console user who ran the security check, by console users with the View Task History for all Console Users permission and by the Console Administrator.

Remediation Recommendations: FSC_RMT_EXP.1

NetIQ SCM enables the remediation of exceptions from policies by providing detailed recommendations. Network Security Alerts for Solaris: FSC_NAL_EXP.1

The TOE can detect changes in network service capabilities by saving a baseline of appropriate network port and service settings and comparing it with against the information obtained from the current scan. When a change is detected in a scan, the differences can be logged and, if configured, an alert sent to the user via e-mail.

6.2 Security Assurance Measures

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Components
ACM_CAP.2	The description of the configuration items is provided in *EAL2 Configuration Management Documentation NetIQ Secure Configuration Manager 5.6*.
ADO_DEL.1	The description of the delivery procedures is provided in *NetIQ Product Delivery and Operations Process*.

Assurance Requirement	Assurance Components
ADO_IGS.1	The installation, generation, and start-up procedures are provided in the following documents: *Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6.* *NetIQ Secure Configuration Manager Installation Guide*, November 15, 2006. *NetIQ Secure Configuration Manager User Guide*, November 15, 2006. *NetIQ Secure Agent for Unix Installation and Configuration Guide, NetIQ Security Manager, NetIQ Secure Configuration Manager*, November 1, 2006. *Secure Configuration Manager Version 5.6 Release Notes*, November 20, 2006.
ADV_FSP.1	The informal functional specification is provided in *NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation*.
ADV_HLD.1	The descriptive high-level design is provided in *NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation*.
ADV_RCR.1	The informal correspondence demonstration is provided in *NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation*.
AGD_ADM.1	The administrator guidance is provided in the following documents: *Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6.* *NetIQ Secure Configuration Manager User Guide*, November 15, 2006. *Secure Configuration Manager Help* for NetIQ Secure Configuration Manager 5.6 (online help) *Secure Configuration Manager Version 5.6 Release Notes*, November 20, 2006.
AGD_USR.1	Not Applicable. All users of the TOE perform an administrative function.
ATE_COV.1	The evidence of coverage is provided in *EAL2 Test Activity ATE NetIQ Secure Configuration Manager 5.6*.
ATE_FUN.1	The functional testing description is provided in *EAL2 Test Activity ATE NetIQ Secure Configuration Manager 5.6*.
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	The strength of function analysis performed is provided in *NetIQ Secure Configuration Manager 5.6 Strength of Function Analysis*.
AVA_VLA.1	The vulnerability analysis performed is provided in *NetIQ Secure Configuration Manager 5.6 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2*.

Table 17 – Assurance Requirements: EAL2

6.3 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs). A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

	Identification & Authentication	Audit	Cryptographic Operations	Secure Communications	Security Management	Protection of TOE functions	Security Assessment
FAU_GEN_EXP.1		X					
FAU_GEN.2		X					
FAU_SAR.1a, b		X					
FAU_SAR.2		X					
FAU_SAR.3		X					
FCS_CKM.1				X			
FCS_CKM.2				X			
FCS_COP.1a			X				
FCS_COP.1b			X				
FCS_COP.1c				X			
FCS_COP.1d				X			
FCS_COP.1e				X			
FIA_AFL.1	X						
FIA_ATD.1	X						
FIA_SOS.1	X						
FIA_UAU.1	X						
FIA_UID.1	X						
FMT_MOF_EXP.1					X		
FCS_MSA.2				X			
FMT_MTD_EXP.1a, b, c, d, e					X		
FMT_SMF.1					X		
FMR_SMR.1					X		
FPT_ITC.1				X			
FPT_ITI.1				X			
FPT_ITT.1				X			
FPT_SEP_EXP.1						X	

	Identification & Authentication	Audit	Cryptographic Operations	Secure Communications	Security Management	Protection of TOE functions	Security Assessment
FSC_ASM_EXP.1							X
FSC_NAL_EXP.1							X
FSC_REV_EXP.1							X
FSC_RMT_EXP.1							X
FSC_RPT_EXP.1							X
FSC_SDI_EXP.1							X
FSC_SDI_EXP.2							X
FSC_SDI_EXP.3							X

Table 18 – TOE Security Function to SFR Mapping

6.4 Appropriate Strength of Function Claim

The claim of SOF-basic for the Identification and Authentication security function is consistent with the claim of SOF-basic for the FIA_UAU.1 and FIA_SOS.1 SFRs that map to that security function.

6.5 Rationale for Security Assurance Measures

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.2	*EAL2 Configuration Management Documentation NetIQ Secure Configuration Manager 5.6*	The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ADO_DEL.1	*NetIQ Product Delivery and Operations Process*	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADO_IGS.1	*Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6* *NetIQ Secure Configuration Manager Installation Guide*, November 15, 2006. *NetIQ Secure Configuration Manager User Guide*, November 15, 2006. *NetIQ Security Agent for Unix Installation and Configuration Guide, NetIQ Security Manager, NetIQ Secure Configuration Manager*, November 1, 2006. *Secure Configuration Manager Version 5.6 Release Notes*, November 20, 2006.	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	*NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation*	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_HLD.1	*NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation*	The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	*NetIQ Secure Configuration Manager 5.6 EAL 2 Design Documentation*	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.

Assurance Requirement	Assurance Measures	Assurance Rationale
AGD_ADM.1	*Common Criteria Supplement EAL2 NetIQ Secure Configuration Manager v5.6* *NetIQ Secure Configuration Manager User Guide*. November 15, 2006. *Secure Configuration Manager Help* for NetIQ Secure Configuration Manager 5.6 (online help) *Secure Configuration Manager Version 5.6 Release Notes*, November 20, 2006.	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	*N/A*	Not Applicable. All users of the TOE perform an administrative function.
ATE_COV.1	*EAL2 Test Activity ATE NetIQ Secure Configuration Manager 5.6*	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_FUN.1	*EAL2 Test Activity ATE NetIQ Secure Configuration Manager 5.6*	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	The TOE	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	*NetIQ Secure Configuration Manager 5.6 Strength of Function Analysis*	The strength of function analysis document provides the SOF argument for the password mechanism.
AVA_VLA.1	*NetIQ Secure Configuration Manager 5.6 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2*	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.3 - 4.5 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.7 - 5.12 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.4 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.