NetIQ® Secure Configuration Manager™ 6.2 Security Target

Date:	November 17th, 2016
Version:	0.1
Prepared By:	NetIQ Corporation
Prepared For:	
	NetIQ Corporation Suite 1200 515 South Post Oak Blvd Houston, TX 77027

Table of Contents

Figures:

Tables:

1. Security Target Introduction (ASE_INT)

This section presents the following information:

- Security Target Reference
- Target of Evaluation Reference
- TOE Overview
- CC Conformance Claims
- Specifies the Security Target conventions,
- Describes the Security Target Organization

1.1 Security Target Reference:

ST Title:	NetIQ® Secure Configuration Manager™ 6.2.0 Security Target
ST Version:	0.1
ST Date:	November 17th, 2016
ST Author:	Michael F. Angelo 713-418-5396 angelom@netiq.com

1.2 Target of Evaluation Reference:

TOE Reference:	NetIQ® Secure Configuration Manager ™ 6.2	
TOE Version #:	6.2.0	
TOE Components:	Component	Version
	SCM Console	6.2.52.0
	Core Services	6.2.52.0
	Unix agent(s)	7.3, 7.4, 7.5
	Windows agent	6.2.52.0
TOE Developer:	NetIQ Corporation	
Evaluation Assurance Level (EAL):	EAL 2+	
Keywords:	Secure Configuration Manager, sensitive data protection device, ST, EAL 2, NetIQ Secure Configuration Manager.	

1.3 Target of Evaluation Overview (TOE):

Note: The official name of the product is: NetIQ® Secure Configuration Manager™ 6.2.52.0 (Secure Configuration Manager™ 6.2.52.0). The released product can be uniquely identified as: Secure Configuration Manager™ 6.2 or SCM 6.2 . For the purpose of this certification all products were tested with SCM 6.2 . The product name may also be abbreviated as *Secure Configuration Manager*™ 6.2 or simply *Secure Configuration Manager, or SCM* or the *TOE*. For the purpose of this certification, and the associated documentation, all of the above references are equivalent.

Note: The Core Services may also be referred to as SCM Core Services.

1.3.1 Product Overview:

The NetIQ Secure Configuration Manager (SCM) Version 6.2 is a software application that enables organizations to determine organizational security policy compliance, to identify security vulnerabilities and potential threats, and to assist in correcting exposures in a timely manner to reduce the risk of security breaches, failed compliance audits or downtime. NetIQ SCM also provides reporting capabilities, risk scoring to assist with prioritizing the discovered potential threats and vulnerabilities, and an update

service that integrates new expertise and security knowledge[1] by providing new security checks for the latest vulnerabilities, updated policy templates, and current manufacturer-recommended patches.

The NetIQ SCM can assess and report on multiple systems, however only Windows and Sun Solaris 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 installed on the systems or "audit by proxy" which does not require an agent.

The typical configuration can have the SCM console separate from the core services, however to simplify testing, we tested using configuration as described in Section 1.3.2 entitled TOE Components. Given the number of agents and complexity of the certification we will be certifying the configuration as depicted in Figure 1.

The product is supported on multiple operating systems at the time of this certification; however it is not being certified on all of them. For the purpose of this certification we will limit the agents to Sun Solaris and Windows Server 2012. Virtual machines have been shown to be analogous in form and function to physical machines, and thus may be used to house the components for testing in this certification.

1.3.2 TOE Components:

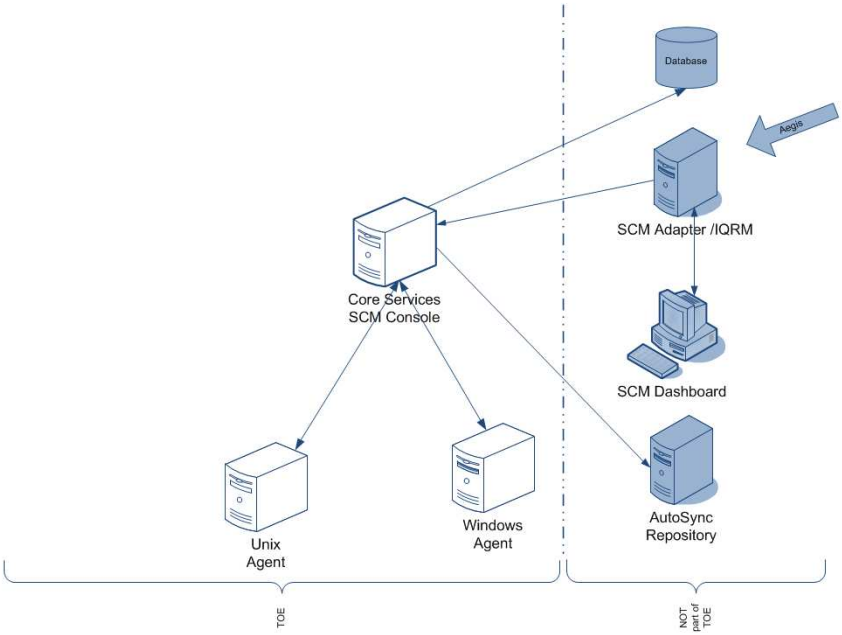

Figure 1: Secure Configuration Manager Evaluated Configuration

[1] The term "security knowledge" refers to IT data used to categorize and detect potential vulnerabilities and threats (e.g., object ownership, configuration settings, and object permission).

1.3.3 SCM Architecture

The TOE is broken into three functional areas. They are:

- User Interfaces
- SCM Core Services
- Agents (Sun Solaris) and Windows)

The TOE also depends on the SCM database and Internet which are in the IT environment.

1.3.3.1 User Interface

The SCM console is collocated with the Core Services and communicates directly with the Core Services. It is important to note that the SCM Dashboard depicted above is really to control communications between IQRM and SCM. This functionality is excluded from the certification.

The regular SCM console interface to the TOE is a Win32 application and is a required component. In the evaluated configuration, the user console will be installed on the middleware host. The middleware component (also known as SCM Core Services or core services) can 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.

1.3.3.2 SCM Core Services

The SCM Core Services 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[2], including Windows and Sun Solaris from SCM Core Services.

An *AutoSync* client resides on the SCM Core Services system[3] and provides a mechanism for NetIQ Corporation to update SCM Core Services with current security knowledge. The *AutoSync* client provides a common mechanism 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 will be installed on the same machine as the SCM Core Services.

1.3.3.3 SCM Agents

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

- Windows Agent [4] or Endpoints (i.e. Active Directory, Domain Infrastructures, IIS, and SQL server)
- Unix/Linux Agent
- iSeries Agent (not included in the evaluation)

[2] An endpoint is an entity that an agent manages and audits. An endpoint could be a computer, database, or application.
[3] The *auto-sync* client can also be deployed on another computer. In this case, SCM Core Services communicates with the *auto-sync* client to obtain the updates. This feature is not included in the evaluated configuration.
[4] While Windows Agents run on Windows 7, Windows 8, Windows 2008, Windows 2008 R2, Windows 2003, and Windows 2012, we are only certifying with Windows 2012.

- Database Endpoints (not included in the evaluation)

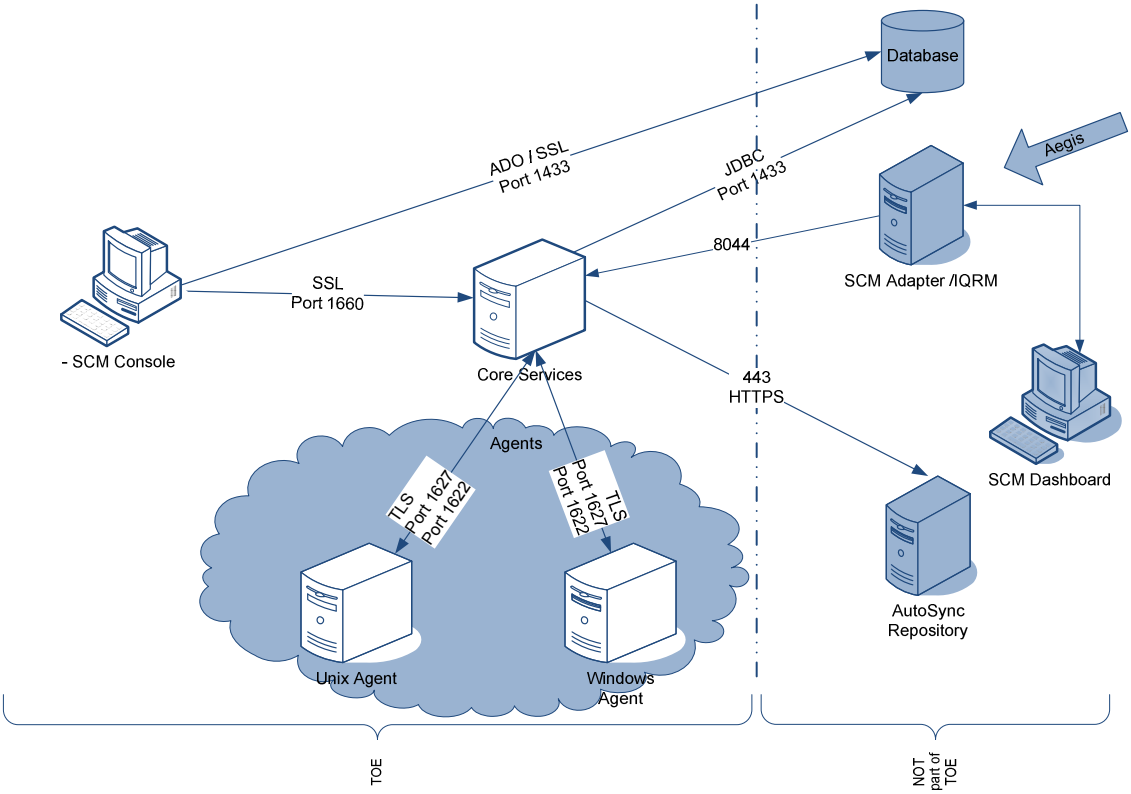

Figure 2: Communication Ports

1.3.3.4 Communications:

SCM supports both Series 4 and Series 3 agent protocols[5] for transmissions between the SCM Core Services and SCM Agents. However, the evaluated configuration only includes the Series 4 Agents for Sun Solaris and Windows. The Series 4 agents are issued an authentication key at registration. The Series 4 agent protocol can communicate using 128-bit AES and 1024-bit RSA.

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 a Windows machine other than itself, it is called proxy auditing.

As depicted in figure 3, the 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 TLS connections into consideration when configuring the boundary protection mechanisms.

1.3.3.5 SCM Installation:

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

[5] These agent protocols are NetIQ proprietary protocols.

endpoints in its domain. NetIQ security agents for Unix can only be deployed by installing an agent on each computer being managed.

1.3.4 Major Security Features of the TOE:

The TOE provides:

- Audit capabilities.
- Security Assessments

The TSF includes the following security functions:

- Security Audit
- Cryptographic Operations
- User Data Protection
- Identification and Authentication
- Protection of the TOE
- Security Management
- Secure Communications

1.3.4.1 Security 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.

1.3.4.2 Cryptographic Operations

The TOE can verify the consistency of files on Sun Solaris endpoints using message digests calculated for the files.

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

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

1.3.4.3 User Data Protection

SCM implements User Data Protection via the Console Administrator Role. A console administrator is a console user who has administrator permissions in SCM. For example, you can create a console administrator by assigning the Administrators role to a console user. A console administrator is not required to be an administrator or super user on a specific endpoint or platform. You do not need to grant escalated permissions on remote systems that Secure Configuration Manager is monitoring. Console administrators can perform the following console security activities:

- Implement and modify external authentication
- Implement and modify password policy
- Reset console user and console administrator account passwords
- Create console user accounts
- Create, copy, and modify roles
- Assign permissions to roles or console users

Console administrators can also perform actions and generate reports through Secure Configuration Manager.

1.3.4.4 Identification and Authentication

SCM requires each user to be identified and authenticated prior to performing any functions using the 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 Sun 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.

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.

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.

1.3.4.5 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 ensure the TOE security services are not bypassed or tampered with. 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 executable(s) from tampering. The hardware and operating system implement process separation.

1.3.4.6 Security Management

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

The TOE implements roles by assigning console permissions (also known as just permissions) directly to users or to define 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).

1.3.4.7 Secure Communications

The TOE provides for secure communications between the separate portions of the TOE.

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.)

1.3.5 TOE TYPE:

For the purpose of this security target the TOE Type is a **S**ecurity **D**ata **A**cquisition and **R**ules **A**ssessment tool (SDARA). This TOE is a Software Only TOE.

1.3.6 Non-TOE hardware/software/firmware required by the TOE.

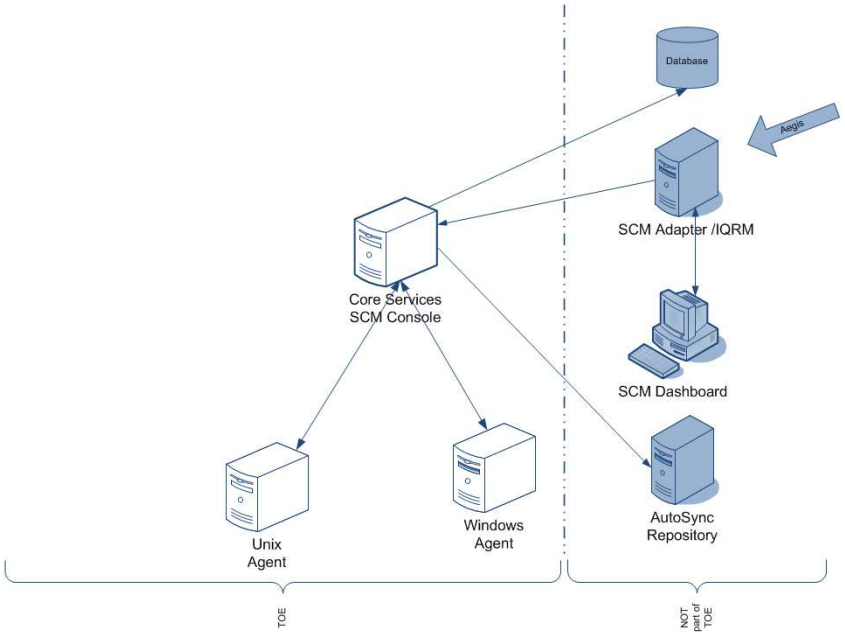

Figure 3: NetIQ Secure Configuration Manager Configuration

The system may employ SSL, MSMQ, DCOM, ADO, and .net Remoting for communications, which are provided by a third party and are not part of the TOE.

1.3.7 Excluded TOE Items:

The following elements are not included in the TOE. This list is broken into elements that are included in the product, but will not be evaluated at this time.

1.3.7.1 Elements:

These environments (components) are not part of the TOE.

- Microsoft SQL Server (Database)
- Microsoft .NET Framework 4.0.30319.1
- SCM Dashboard
- Aegis
- AutoSync Repository
- SCM Adapter / IQRM

In addition while the system may require a network which may consist of routers, switches, hubs, and other technology used in a TCP/IP based network, which are also not part of the TOE.

1.3.8 Evaluated Configuration

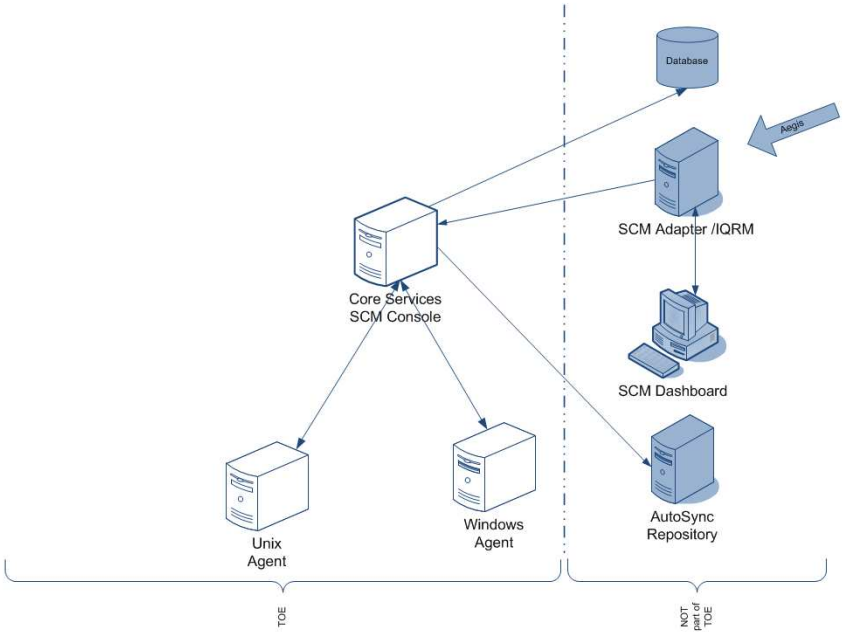

Figure 4: Evaluated Configuration

1.3.8.1 Physical Scope of TOE

The NetIQ Secure Configuration Manager program is a software only TOE. The TOE consists of the elements in Figure 4 (above), labeled (TOE). The TOE explicitly includes at least one Console, the core services, one Unix Agent and one Windows Agent. The TOE explicitly excludes the Database, IQRM Adapters and SCM Dashboard.
User installation and guidance documents are supplied with the TOE.
The components that make up the evaluated configuration are:

- SCM Console 6.2
- Security Agent for Windows 6.2
- Security Agent for Unix 7.4
- SCM Core Services 6.2

The SCM User Console will be evaluated on the following operating systems:

- Microsoft Windows Server 2012

The Security Agent for Windows will be evaluated on the following operating systems:

- Microsoft Windows Server 2012

The Security Agent for UNIX will be evaluated on the following operating systems:

- Sun Solaris

The SCM Core Services will be evaluated on the following operating systems:

- Microsoft Windows Server 2012

The following packages are used to provide cryptographic functions and are included in the TOE boundary. They meet the cryptographic quality requirements as evidenced by the following certificates:

Component	Cert #
OpenSSL 1.0.1p (FIPS module 2.0.9)[7]	2473
NSS 3.12.4[8]	1279 1475

Table 1: FIPS Certificate Numbers

The product will be evaluated when it is in FIPS mode.

1.4 Security Target Conventions:

This section specifies the formatting information used in the ST. The notation, conventions, and formatting in this security target are consistent with Version 3.1 of the Common Criteria for Information Security Evaluation. Clarifying information conventions, as well as font styles were developed to aid the reader.

- Security Functional Requirements – Part 1, section C.2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, iteration, refinement, and selection,.
  - Assignment: allows the specification of an identified parameter or parameter(s).
  - Iteration: allows a component to be used more than once with varying operations.
  - Refinement: allows the addition of details.
  - Selection: allows the specification of one or more elements from a list.
- Within section 6 of this ST the following conventions are used to signify how the requirements have been modified from the CC text.
  - Assignments are indicated using bold and are surrounded by brackets (e.g., **[assignment**]).

[7] The OpenSSL FIPS Object Module was compiled a priori on a windows x86 system as per the OpenSSL FIPS 140-2 Security Policy. The result passed the OpenSSL FIPS Integrity Test. This module was then moved to Windows Server 2012 where it works without issue or change. As such it qualifies for the FIPS 140 Inside program under certificate 2473. OpenSSL is provided with the product and is part of the TOE.

[8] NSS was distributed in its entirety and was not modified to run with SCM. In addition NSS was merely copied onto the Windows 12 platform where it ran without re-compilation or changes. As such it qualifies for the FIPS 140 Inside program under either certificate 1279 or 1475. NSS is provided with the product and is part of the TOE.

  - Iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **every** object …" or "… ~~all~~ **things** …").
  - Selections are indicated using italics and are surrounded by brackets (e.g., [*selection*]).
  - Special comments or Application Notes are indicated using *Italics*.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as acronyms, definitions, or captions.
- Security Functional requirements labeled #<letter>-<letter> denotes an inclusive range. (e.g., FCS_COP.1a-e would denote FCS_COP.1 iteration a through e.).

1.5 Acronyms:

AD	Active Directory
ADO	ActiveX Data Object
AES	Advanced Encryption Standard – FIPS 197
API	Application programming interface
CC	Common Criteria
CCDB	Control Center Database
CCDS	Control Center Deployment Service
CCDWS	Control Center Deployment Web Server
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CQS	Command Queuing Services
DB	Database
DCOM	Distributed Component Object Model
EAL	Evaluation Assurance Level
FERC	Federal Energy Regulatory Commission
GLBA	Gramm–Leach–Bliley Act
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
HLD	High-level Design
HTTPS	Hypertext Transfer Protocol Secure
IA	Initial Assessment
IDS	Intrusion Detection Systems
IIS	Internet Information Server
IQRM	NetIQ Resource Manager
LDAP	Lightweight Directory Access Protocol
MS	Management Server
LDAP	Lightweight Directory Access Protocol
NSS	Network Security System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating system
PP	Protection Profile
PSSI	Professional Services Support Interface
SCM	Secure Configuration Manager
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Monitoring Protocol
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality
TSP	TOE Security Policy
UI	User Interface
YTBD	Yet To Be Determined

1.6 Security Target Organization

The Security Target (ST) contains the following sections:

Section 1	Security Target Introduction (ASE_INT)	The ST introduction describes the Target of Evaluation (TOE) in a narrative with three levels of abstraction: A TOE reference, TOE overview, a TOE description (in terms of physical and logical boundaries) and scoping for the TOE.
Section 2	CC Conformance Claims (ASE_CCL)	This section details any CC and PP conformance claims.
Section 3	Security Problem (ASE_SPD)	This section summarizes the threats addressed by the TOE and assumptions about the intended environment.
Section 4	Security Objectives (ASE_OBJ)	This section provides a concise statement in response to the security problem defined in definition.
Section 5	Extended Components Definition (ASE_ECD)	This section provides information about security requirements outside of components described in CC Part 2 or CC Part 3.
Section 6	IT Security Requirements (ASE_REQ)	This section provides a description of the expected security behavior of the TOE.
Section 7	TOE Summary Specification (ASE_TSS)	This section provides a general understanding of the TOE implementation.

2. CC Conformance Claims

2.1 CC Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Release 4, September 2012. Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 Release 4, September 2012. Part 3 Conformant
- Augmented with ALC_FLR.1

2.2 PP Claim

The TOE does not claim conformance to any Protection Profiles (PPs).

2.3 Package Claim

The TOE claims conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 4 (September 2012). The TOE does not claim conformance to any functional package.

3. Security Problem (ASE_SPD)

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 2) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Introduction:

In order to simplify the security problem, the TOE can be broken into 3 areas. These areas are the:

- Assets elements of the TOE that need protections
- Users persons with legitimate access to the TOE
- Attackers persons that are not a legitimate users

3.1.1 Assets:

The assets can be broken down into two classes – Primary and Secondary. The main aim of this TOE is to protect the primary assets against unauthorized access, manipulation, and disclosure. The primary assets are:

- Data stored in the Database
- Configuration information stored on the Core Services, Console, and Agent machines(s).
- Data in transit from / to the Agents, Core Services, Console, and the Database

The Secondary assets are themselves of minimal value, the possession of these assets enables or eases access to primary assets. Therefore these assets need to be protected as well.

- Credentials (i.e. account information and associated passwords) for access to the TOE
- Security attributes (i.e. File access permissions) on the TOE.
- Explicit Product privileges afforded to users of the TOE.

3.1.2 Subjects:

Subjects have privileges and associations depending on their roles in the Secure Configuration Manager infrastructure. In addition credentials and authorization associations can be stored in the Secure Configuration Manager database or in an External Authentication facility. For example, if a console user account belongs to a Windows Server 2012 or later domain, Secure Configuration Manager validates the account user name and password against the credentials stored in Active Directory on the domain controller for that domain. External authentication allows you to leverage your existing authentication settings.

3.1.2.1 Console Users:

A console user is any user who uses the Secure Configuration Manager console. Console users, including console administrators, need the appropriate roles or permissions to perform activities through Secure Configuration Manager.

3.1.2.2 Console Administrators:

A console administrator is a console user who has administrator permissions in Secure Configuration Manager. For example, you can create a console administrator by assigning the Administrators role to a console user. A console administrator is not required to be an administrator or super user on a specific endpoint or platform. You do not need to grant escalated permissions on remote systems that Secure Configuration Manager is monitoring. Console administrators can perform the following console security activities:

- Implement and modify external authentication

- Implement and modify password policy
- Reset console user and console administrator account passwords
- Create console user accounts
- Create, copy, and modify roles
- Assign permissions to roles or console users

Console administrators can also perform actions and generate reports through Secure Configuration Manager.

3.1.3 Attacker:

An Attacker is a person (or persons) who is not a user or administrator, and has not physical access to any device in the infrastructure. This means that their only mode of access would be from outside the corporate environment (i.e. a machine on the Internet).

A successful attacker would be able to gain access to TOE resources. Assuming successful access that attacker would then attempt to:

- access the console as an authorized user create / modify / delete jobs
- access the Secure Configuration Manager Repository and create / modify / delete jobs or data
- delete all data in the Secure Configuration Manager Repository
- access the Deployment Server and deploy packages
- access the agents and provide erroneous data to the Secure Configuration Manager Repository

3.2 Assumptions

3.2.1 Connectivity Assumptions:

A.AVAIL	The systems, networks and all components will be available for use.
A.CONFIG	The systems will be configured to allow for proper usage of the application.
A.NETCON	All networks will allow for communications between the components.

3.2.2 Intended Usage Assumptions

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.INTERNET	The TOE component for Core Services must be connected to the Internet, behind appropriate boundary protection mechanisms, in order to receive updated content information from the NetIQ servers.

3.2.3 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

3.2.4 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.2.5 Physical Assumptions

A.LOCATE	The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.AUTHCON	The TOE will be able to rely on the IT environment to determine the identity of users.
A.ENVFAC	The TOE will be able to rely on the IT environment to obtain a reliable time stamp.

3.3 Threats

3.3.1 Threats to the TOE

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.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
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.MAL_INTENT	An authorized user could initiate changes that grant themselves additional unauthorized privileges.
T.MIS_NORULE	Unauthorized accesses and activity, indicative of misuse, may occur on an IT System the TOE is installed on and the TOE response may not occur if no event rules are specified in the TOE.

T.NO_HALT	An unauthorized entity may attempt to compromise the continuity of the TOE by halting execution of the TOE or TOE Components.
T.PRIV	An unauthorized entity may gain access to the TOE and exploit functionality to gain access or privileges to TOE security functions and data.
T.SC_MISCFG	Improper security configuration settings may exist in the IT System the TOE is on and could make the TOE audit ineffective.
T.SC_MALRUN	Users could execute malicious code on an IT System that the TOE is installed on which causes modification of the TOE protected data or undermines the IT System security functions.
T.TSF_COMPROMISE	A malicious user may cause configuration data 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.

4. Security Objectives (ASE_OBJ)

4.1 Security Objectives for the TOE

O.ADMIN_ROLE	The TOE will define authorizations that determine the actions authorized administrator roles may perform.
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.CRYPTO	The TOE shall provide cryptographic services to verify the integrity and authenticity of data.
O.MANAGE	The TOE will allow administrators to effectively manage the TOE and its security functions,
O.RESPONSE	The TOE must respond appropriately to trigger events.
O.SECURE_COMM	The TOE will provide secure communications that prevent unauthorized disclosure and modification of transmissions between distributed portions of the TOE.
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 Non-IT Environment

OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
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.INTROP	The TOE is interoperable with the Environment it manages.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
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 Security Objectives for the IT Environment

OE.AUD_STORAGE	The IT environment will provide a means for secure storage of the TOE audit log files.
OE.OFLOWS	The TOE must appropriately handle potential System data storage overflows.
OE.USER_AUTHENTICATION	The IT environment will verify the claimed identity of users.
OE.USER_IDENTIFICATION	The IT environment will uniquely identify users.
OE.TIME	The IT environment will provide a time source that provides reliable time stamps.
OE.TOE_PROTECTION	The IT Environment will protect the TOE and its assets from external interference or tampering.

4.4 Non Security Objectives for the IT Environment

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.

4.5 Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;

- Security Assurance Requirements;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims

4.6 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

4.6.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats by the security objectives.

		O.CRYPTO	O.ADMIN_ROLE	O.AUD_GEN	O.AUD_PROT	O.AUD_REVIEW	O.MANAGE	OE.OFLOWS	O.RESPONSE	O.SECURE_COMM	O.SECURE_CHK	O.TOE_ACCESS	OE.AUD_STORAGE	OE.TOE_PROTECTION	OE.TIME
Threats to the TOE	T.ACCOUN			X								X			X
	T.AUD_COMP				X			X		X	X		X	X	
	T.ADMIN_ERROR						X								
	T.BAD_UPDATE	X													
	T.MAL_INTENT			X				X	X		X			X	
	T.MIS_NORULE			X							X				
	T.NO_HALT		X						X						
	T.PRIV		X	X											
	T.TSF_COMPROMISE	X												X	
	T.SC_MISCFG			X							X	X			
	T.SC_MALRUN		X									X			
	T.UNIDENT_ACTION			X		X									X

Table 2: Threat to Objective Correspondence

4.6.1.1 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	Supports in mitigating this threat by requiring the IT environment to provide a reliable time stamp.

4.6.1.2 T.AUD_COMP

O.AUD_PROT	The TOE 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.OFLOWS	The TOE counters this by preventing transactions from occurring when the system runs out of storage space.
O.SECURE_COMM	The objective mitigates this threat by providing secure communications preventing unauthorized modification of audit records transmitted over the network.
O.SECURE_CHK	The TOE protects against this threat by providing access policies that control who can do what to the audit logs and data streams.
OE.AUD_STORAGE	The IT environment will provide a means for secure storage of the TOE audit log files.
OE.TOE_PROTECTION	The IT Environment counters this threat by protecting the TOE and its assets from external interference or tampering.

4.6.1.3 T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is countered by ensuring that:

O.MANAGE:	The TOE counters this threat by providing a user interface that allows Administrators to effectively manage the TOE and its security functions. In addition the TOE ensures that only authorized entities are able to access such functionality.

4.6.1.4 T.BAD_UPDATE

O.CRYPTO:	The TOE 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.

4.6.1.5 T.MAL_INTENT:

An authorized user could initiate changes that grant themselves additional unauthorized privileges.

This Threat is countered by ensuring that:

O.AUD_GEN:	The TOE counters this event by collecting and storing transactional information that can be used to audit changes to the AD.
OE.OFLOWS:	The TOE counters this by preventing transactions from occurring when the system runs out of storage space.
O.RESPONSE:	The TOE counters this event by responding appropriately to trigger events.
O.SECURE_CHK:	The TOE counters this threat by providing an access policy.
OE.TOE_PROTECTION:	The IT Environment counters this threat by protecting the TOE and its assets from external interference or tampering.

4.6.1.6 T. MIS_NORULE

Unauthorized accesses and activity, indicative of misuse, may occur on an IT System the TOE is installed on and the TOE response may not occur if no rules are specified in the TOE.

This Threat is countered by ensuring that:

O.AUD_GEN:	The TOE collects and stores transactional information that can be used to audit changes to the AD.
O.SECURE_CHK:	The TOE protects against this threat by providing access policies.

4.6.1.7 T.NO_HALT

An unauthorized entity may attempt to compromise the continuity of the TOE by halting execution of the TOE or TOE Components.

This Threat is countered by ensuring that:

O.ADMIN_ROLE:	The TOE counters this threat by defining authorizations that determine the actions authorized entities may perform.
O.RESPONSE:	The TOE defines triggers that can be used to notify of events. This threat can be mitigated by configuring a trigger when a shutdown is attempted.

4.6.1.8 T.PRIV

An unauthorized entity may gain access to the TOE and exploit functionality to gain access or privileges to TOE security functions and data.

This Threat is countered by ensuring that:

O.ADMIN_ROLE:	The TOE counters this threat by providing strict access controls which determine the actions / roles authorized assistant administrators may perform.
O.AUD_GEN:	The TOE counters this threat by providing transactional based audit capabilities.

4.6.1.9 T.TSF_COMPROMISE

A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

This Threat is countered by ensuring that:

O.CRYPTO[9]:	The TOE will provide encryption to enable secure and private communications.
OE.TOE_PROTECTION:	The IT environment will protect the TOE and its assets from external interference or tampering.

4.6.1.10 T.SC_MISCFG

Improper security configuration settings may exist in the IT System the TOE is on and could make the TOE audit ineffective.

This Threat is countered by ensuring that:

O.AUD_GEN:	The TOE counters this threat by providing transactional based audit capabilities.
O.SECURE_CHK:	The TOE counters this threat by providing an access policy.
O.TOE_ACCESS:	The TOE protects against this threat by ensuring that only authorized administrators are able to access functionality.

4.6.1.11 T.SC_MALRUN

[9] Refers to crypto that is provided by NSS and OpenSSL, as provided by the product.

Users could execute malicious code on an IT System that the TOE is installed on which causes modification of the TOE protected data or undermines the IT System security functions.

This Threat is countered by ensuring that:

O.ADMIN_ROLE: The TOE counters this threat by defining authorizations that determine the actions / roles that authorized entities may perform.

O.TOE_ACCESS: The TOE protects against this threat by ensuring that only authorized administrators are able to access functionality.

4.6.1.12 T.UNIDENT_ACTION

O.AUD_GEN helps to mitigate this threat by recording actions performed within the SCM User Console for later review.

O.AUD_REVIEW: The TOE helps to mitigate this threat by providing a method for reviewing the recorded security actions that could indicate a potential security violation.

OE.TIME assists in mitigating this threat by requiring the IT environment to provide a reliable time stamp.

4.7 Security Objectives Rationale for Environment Assumptions

This section provides evidence demonstrating coverage of the Non-IT security objectives by the environmental assumptions. The following table shows this assumption to objective mapping.

		OE.INSTAL	OE.CREDEN	OE.CS_ACCTS	OE.DEDICATED	OE.PERSON	OE.PHYCAL	OE.INTROP	OE.INTERNET	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.SEC_UPDATES	OE.TIME
Intended usage assumptions	A.ACCESS							X					
	A.ASCOPE							X					
	A.DEDICATED				X								
	A.DYNMIC					X		X					
	A.SEC_UPDATES											X	
Physical assumptions	A.LOCATE						X						
	A.AUTHCON									X	X		
	A.ENVFAC												X
Personnel assumptions	A.CS_ACCTS			X									
	A.MANAGE					X							
	A.NOEVIL	X	X										
Connectivity assumptions	A.AVAIL						X	X					
	A.CONFIG						X	X					
	A.NETCON						X	X					
	A.INTERNET								X				

Table 3: Complete coverage – environmental assumptions

4.7.1 A.ACCESS

The TOE has access to all the IT System data it needs to perform its functions.

This Assumption is satisfied by ensuring that:

OE.INTROP:	The OE.INTROP objective ensures the TOE has the needed access.

4.7.2 A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

This Assumption is satisfied by ensuring that:

OE.INTROP:	The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

4.7.3 A.CS_ACCTS

OE.CS_ACCTS:	The OE.CS_ACCTS restates the assumption as an objective and therefore, addresses the assumption.

4.7.4 A.DEDICATED

OE.DEDICATED:	OE. DEDICATED restates the assumption as an objective and therefore, addresses the assumption.

4.7.5 A.DYNIMC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

This Assumption is satisfied by ensuring that:

OE.PERSON:	The OE.PERSON objective ensures that the TOE will be managed appropriately.
OE.INTROP:	The OE.INTROP objective ensures the TOE has the proper access to the IT System.

4.7.6 A.AUTHCON

The TOE will be able to rely on the IT environment to determine the identity of users.

This Assumption is satisfied by ensuring that:

OE.USER_AUTHENTICATION	The OE.USER_AUTHENTICATION ensures that the IT environment can verify the claimed identity of users.
OE.USER_IDENTIFICATION	The OE.USER_IDENTICATION ensures that the IT environment can uniquely identify users.

4.7.7 A.ENVFAC

The TOE will be able to rely on the IT environment to obtain a reliable time stamp.

This Assumption is satisfied by ensuing that:

OE.TIME	The OE.TIME ensures that the IT environment will provide a time source to be used for reliable time stamps.

4.7.8 A.INTERNET

OE.INTERNET	OE.INTERNET restates the assumption as an objective and therefore, addresses the assumption.

4.7.9 A.LOCATE

The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

This Assumption is satisfied by ensuring that:

OE.PHYCAL:	The OE.PHYCAL provides for the physical protection of the TOE.

4.7.10 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This Assumption is satisfied by ensuring that:

OE.PERSON:	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

4.7.11 A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

This Assumption is satisfied by ensuring that:

OE.INSTAL:	The OE.INSTAL objective ensures that the TOE is properly installed and operated.
OE.CREDEN:	The OE.CREDEN objective supports this assumption by requiring protection of all authentication data

4.7.12 A.AVAIL

The IT environment will be available for use by the TOE.

OE.PHYCAL:	The OE.PHYCAL objective ensures that the TOE is in a protected environment.
OE. INTROP:	The OE.INTROP objective ensures that the TOE can interoperate with the environment it is deployed in.

4.7.13 A.CONFIG

The IT environment is properly configured for use by the TOE.

OE.PHYCAL:	The OE.PHYCAL objective ensures that the TOE configuration is properly protected.
OE. INTROP:	The OE.INTROP objective ensures that the TOE is configured to properly interoperate with the environment it is deployed in.

4.7.14 A.NETCON

The IT network environment is properly protected and can be used by the TOE.

OE.PHYCAL:	The OE.PHYCAL objective provides for the physical protection of the TOE Network and Network Elements. .
OE. INTROP:	The OE.INTROP objective ensures that the network interface is configured to properly interoperate with the environment and the TOE.

4.7.15 A.SEC_UPDATES

OE. 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.

4.8 Security Requirements Rationale

This section demonstrates how there is at least one functional component for each TOE security objective (and how all SFRs map to one or more TOE security objectives) by a discussion of the coverage for each TOE security objective.

	O.ADMIN_ROLE	O.AUD_GEN	O.AUD_PROT	O.AUD_REVIEW	O.CRYPTO	O.MANAGE	O.RESPONSE	O.PART_SELF_PROT	O.SECURE_COMM	O.SECURE_CHK	O.TOE_ACCESS
FAU_ARP.1							X			X	
FAU_GEN.1		X									
FAU_GEN.2		X									
FAU_SAA.1							X				
FAU_SAR.1a, b				X							
FAU_SAR.2			X								
FAU_SAR.3				X							
FAU_STG.1			X								
FCS_CKM.1									X		
FCS_CKM.2									X		
FCS_COP.1a, b					X					X	
FCS_COP.1c, d									X		
FDP_ACC.1											X
FDP_ACF.1											X
FIA_AFL.1											X
FIA_ATD.1	X										X
FIA_SOS.1											X
FIA_UAU.1											X
FIA_UID.1											X
FMT_MOF.1						X					
FMT_MSA.1	X										X
FMT_MSA.2											X
FMT_MSA.3						X					X
FMT_SMF.1						X					
FMT_SMR.1	X					X					
FMT_MTD.1a, b, c						X					
FMT_MTD.1d			X			X					
FMT_MTD.1e						X					
FPT_ITC.1									X		
FPT_ITI.1									X		
FPT_ITT.1									X		
FPT_SEP_EXT.1								X			

Table 4: Objective to Requirement Correspondence

4.8.1 O.ADMIN_ROLE

The TOE will define authorizations that determine the actions authorized administrator roles may perform.

This TOE Security Objective is satisfied by ensuring that:

FIA_ATD.1	maintains authorization information that determines which TOE functions a role may perform.
FMT_MSA.1	enforces access controls that restrict the ability to alter security attributes to Authorized Administrators.
FMT_SMR.1	recognizes any user account that is assigned in the IT environment to one or more system-defined operating system user groups “Authorized Administrator”.

4.8.2 O.AUD_GEN

The TOE must collect and store transactional information that can be used to audit jobs, data, or events.

FAU_GEN.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.

4.8.3 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.
FAU_STG.1	ensures that stored audit records, in the audit trail are protected from unauthorized deletion or modification.
FMT_MTD.1d	limits the ability to delete audit records to the Console Administrator.

4.8.4 O.AUD_REVIEW

FAU_SAR.1a FAU_SAR.1b	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.

FAU_SAR.3	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.

4.8.5 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.

4.8.6 O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

FMT_MOF.1:	defines particular TOE management capabilities provided by the User Console that can be used only by select users.
FMT_MSA.3	defines default restricted access control values that SCM Administrators and SCM Users with appropriate roles may modify.
FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c, FMT_MTD.1d, FMT_MTD.1e	define particular TOE data that using the User Console may be queried, created, and altered only by users with select roles.
FMT_SMF.1:	defines the administrative functions provided by the TOE.
FMT_SMR.1:	defines the roles provided by the TOE.

4.8.7 O. RESPONSE

The TOE must respond appropriately to event triggers

This TOE Security Objective is satisfied by ensuring that:

FAU_ARP.1:	The TOE can be configured to generate event triggers and be programmed to respond to those events.
FAU_SAA.1:	The TOE can be configured to look at an events occurrence and generate an alarm.

4.8.8 O.PART_SELF_PROT

FPT_SEP_EXT.1:	The TOE 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.

4.8.9 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).
FCS_CKM.1	requires that the TOE generates cryptographic keys.
FCS_CKM.2 FCS_COP.1c	requires that the TOE distribute cryptographic keys via Diffie-Hellman.
FCS_COP.1d	requires that the TOE provide the ability to produce message authentication codes.

4.8.10 O.SECURE_CHK

The TOE must provide an access policy.

FAU_ARP.1	The TSF shall generate audit records, block access, and generate a message upon detection of a security violation.
FCS_COP.1	requires that the TOE be able to calculate message digests to verify the integrity of files on the Sun Solaris endpoints.

4.8.11 O.TOE_ACCESS

The TOE must ensure that only authorized administrators, users, and agents are able to access the TOE functionality.

FDP_ACC.1	ensures that access controls (read write, modify, or execute) are provided for, and limited to SCM Administrators and SCM Users.
FDP_ACF.1	ensures that access controls are limited based on membership in SCM administrators or SCM Users roles.
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.
FMT_MSA.1	ensures that only authorized administrators can modify, add , or delete administrator privileges
FMT_MSA.3	ensures that default access control values are restricted, and that SCM Administrators and SCM Users can specify alternate default settings.

4.9 Security Assurance Requirements Rationale

EAL 2 was chosen to provide a low level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL 2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

4.9.1 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

SFR	Dependencies	Met By
FAU_ARP.1	FAU_SAA.1	Included
FAU_GEN.1	None	Included
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes, via FAU_GEN.1
FAU_SAA.1	FAU_GEN.1	Included
FAU_SAR.1a,b	FAU_GEN.1	Yes, via FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Included
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	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	NO for FCS_CKM.4 (see below for rationale)
FCS_COP.1a	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4	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	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.

SFR	Dependencies	Met By
FCS_COP.1c, d	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4	NO for FCS_CKM.4 [10]
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	YES
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.1	FMT_SMF.1 FMT_SMR.1	YES
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	FMT_MSA.2 is for secure values being entered.
FMT_MSA.3	None	N/A
FMT_MTD.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_SEP_EXT.1	None	YES
FPT_ITC.1	None	N/A
FPT_ITI.1	None	N/A

[10] 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).

SFR	Dependencies	Met By
FPT_ITT.1	None	N/A

Table 5: Requirement Dependency

4.10 TOE Summary Specification Rationale

Each subsection in the TSS describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions works together to satisfy all of the security functions requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 7, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 6 demonstrates the relationship between security requirements and security functions.

	Security Audit	Cryptographic Operations	User Data Protection	Identification & Authentication	Protection of TOE functions	Security Management	Secure Communications
FAU_ARP.1	X						
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAA.1	X						
FAU_SAR.1a, b	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FAU_STG.1	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
FDP_ACC.1			X				
FDP_ACF.1			X				
FIA_AFL.1				X			
FIA_ATD.1			X	X			
FIA_SOS.1				X			

	Security Audit	Cryptographic Operations	User Data Protection	Identification & Authentication	Protection of TOE functions	Security Management	Secure Communications
FIA_UAU.1				X			
FIA_UID.1				X			
FMT_MOF.1						X	
FMT_MSA.1						X	
FMT_MSA.2						X	
FMT_MSA.3						X	
FMT_MTD.1a, b, c, d, e						X	
FMT_SMF.1						X	
FMR_SMR.1						X	
FPT_ITC.1							X
FPT_ITT.1							X
FPT_ITI.1							X
FPT_SEP_EXT.1					X		

Table 6: Security Functions vs. Requirements Mapping

5. Extended Components Definition (ASE_ECD)

This chapter defines extensions to existing classes of NetIQ Secure Configuration Manager (SCM) functionality. The class consists of the following family members FPT_SEP_EXT. This class is defined because the Common Criteria (Part 2 and Part 3) does not contain any SFRs which adequately cover these functions. The families in this class address requirements for ***audits, security management, and data management***.

Class	Component
SCM: Secure Configuration Manager	FPT_SEP_EXT.1

Table 7: Extended Functional Components

5.1 Protection of TSF (FPT)

5.1.1 FPT_SEP_EXT.1 Partial TSF Domain Separation

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

6. IT Security Requirements (ASE_REQ)

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been copied from version 3.1 of the applicable Common Criteria documents, with the exception of the explicitly stated Security Functional Requirements.

6.1 TOE Security Functional Requirements

Class	Component
FAU: Security Audit	FAU_ARP.1: Security Alarms
	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Identity Association
	FAU_SAA.1 - Potential violation analysis
	FAU_SAR.1a-b: Audit Review
	FAU_SAR.2: Restricted Audit Review
	FAU_SAR.3:Selectable Audit Review
	FAU_STG.1: Protected Audit Trail Storage
FCS: Cryptographic Operations	FCS_CKM.1: Cryptographic Key Generation FCS_CKM.2: Cryptographic Key Distribution FCS_COP.1a-d:Cryptographic Operation
FDP: User Data Protection	FDP_ACC.1: Subset Access Control
	FDP_ACF.1: Security Attribute Based Access Control
FIA: Identification and Authentication	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: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.2: Secure Security Attributes
	FMT_MSA.3: Static Attribute Initialization.
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Secure Communications	FPT_ITC.1: Inter-TSF Trusted Channel
	FPT_ITI.1: Integrity of Exported TSF Data
	FPT_ITT.1: Internal TOE TSF Data Transfer
EXT: Extended Components	FPT_SEP_EXT.1 Partial TSF Domain Separation

Table 8: TOE Security Functional Requirements

6.2 Security Audit (FAU)

6.2.1 Security Alarms (FAU_ARP.1)

FAU_ARP.1 The TSF shall take [**post a message, generate a log entry , and block the transaction**] upon detection of a potential security violation.

6.2.2 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the auditable events ~~of the following auditable events~~ **identified in** Table 9: FAU_GEN.1 Auditable Events.

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.1	All modifications in the behavior of the functions in the TSF.
FMT_MTD.1b,c,d,e	All modifications to the values of the TSF data, except for:
	• the deletion of user accounts
	• the creation, deletion, or modification of security checks
	• 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.

Table 9: FAU_GEN.1 Auditable Events

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

a) Date and time of the event, type of event, subject identity (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**].

6.2.3 User Identity Association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.4 Potential violation analysis (FAU_SAA.1)

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

6.2.5 Audit Review (FAU_SAR.1a) - 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 information**] 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.

6.2.5.1 Audit Review (FAU_SAR.1b) - User

FAU_SAR.1.1b The TSF shall provide [**Console Users**] with the capability to read [**all audit information 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.

6.2.5.2 Restricted Audit Review (FAU_SAR.2)

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.

6.2.5.3 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to ~~apply~~ [**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).

]

6.2.6 Protected Audit Trail Storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [**prevent**] unauthorized modifications to the stored audit records in the audit trail.

6.3 Cryptographic Support (FCS)

6.3.1 Cryptographic Key Generation (FCS_CKM.1)

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**] specified cryptographic key sizes [**128 bits for symmetric keys and 1024 bits for asymmetric keys**] that meet the following: [**RFC 4366 (TLS v1) symmetric key and secret generation**].

6.3.2 Cryptographic Key Generation (FCS_CKM.2)

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**].

6.3.3 Cryptographic Operation (FCS_COP.1a)– Baseline

FCS_COP.1.1a The TSF shall perform [**message digest calculations**] in accordance with a specified cryptographic algorithm [**SHA1**] and cryptographic key sizes [**not applicable[1]**] that meet the following: [**FIPS 180-4**].

6.3.3.1 Cryptographic Operation (FCS_COP.1b) – 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 for signature verification**] and cryptographic key sizes [**128-bit for decryption and 2048-bit**

[1] 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”.

for signature verification] that meet the following: [**FIPS-PUB 197 for AES and ANSI X9.31 for RSA**].

6.3.3.2 Cryptographic Operation (FCS_COP.1c) – IKE

FCS_COP.1.1c 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: [**FIPS 140-2**]**.**

6.3.3.3 Cryptographic Operation (FCS_COP.1d) – MAC

FCS_COP.1.1d 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 198**]**.**

6.4 User Data Protection (FDP)

6.4.1 Subset Access Control (FDP_ACC.1)

FDP_ACC.1: The TSF shall enforce the [**access control**] on [**All SCM Components for Read, write, modify, or execute access to SCM Administrators, SCM Users**]

6.4.2 Security Attribute Based Access Control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**access control]** to objects based on the following: [**Membership in the:**
SCM Administrators,
SCM Users roles
for Read, Write, Execute access to all SCM objects].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**user execution based on membership in the SCM Administrators group, SCM Users group**].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**as described in appendix A**].

6.5 Identification and Authentication (FIA)

6.5.1 Authentication Failure Handling (FIA_AFL.1)

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**], 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**].

6.5.2 User Attribute Definition (FIA_ATD.1)

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)
].

6.5.3 Verification of Secrets (FIA_SOS.1)

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

a) password length: 8 characters
b) password composition: at least 2 non-alphabetic characters
c) password age: 60 days
d) password reuse: prohibit reuse of 8 previous passwords
].

6.5.4 Timing of Authentication (FIA_UAU.1)

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.

6.5.5 Timing of Identification (FIA_UID.1)

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.

6.6 Security Management (FMT)

6.6.1 FMT_MOF.1 Explicit Management of Security Functions Behavior

FMT_MOF.1.1 The ~~TSF~~ **User Console** shall restrict the ability to [**determine the behavior of, disable, enable, modify the behavior of**] the functions [**listed in**] to [**the identified roles listed in** Table 10: Security Management Functions].

Function	Role
Auditing (except disabling)[11]	**Console Administrator**
Authentication Mechanism	**Console Administrator**
Password Policy	**Console Administrator**
AutoSync Client Configuration	**Console Administrator**

Table 10: Security Management Functions

6.6.2 Management of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Access Controls**] to restrict the ability to [*modify, **add,** or delete*] the security attributes [**privileges and groups of privileges**] to [**Administrators**].

6.6.3 Secure Security Attributes (FMT_MSA.2)

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

6.6.3.1 Static Attribute Initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Access Control**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**SCM Administrators, SCM Users**] to specify alternative initial values to override the default values when an object or information is created.

6.6.4 FMT_MTD.1a Explicit Management of TSF data - Query

FMT_MTD.1.1a The ~~TSF~~ **User Console** shall restrict the ability to [*query*] the **TSF** to **the associated role listed in** .Table 11: Query TSF data

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**

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

TSF Data	Role
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: Query TSF data

6.6.5 FMT_MTD.1b Explicit Management of TSF data – Create, initialize

FMT_MTD.1.1b The ~~TSF~~ ***User Console*** shall restrict the ability to [*create*] the [**TSF]** to [**the associated role listed in** Table 12: Create/initialize TSF data**]**.

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 12: Create/initialize TSF data

6.6.6 FMT_MTD.1c Explicit Management of TSF data - Modify

FMT_MTD.1.1c The ~~TSF~~ **User Console** shall restrict the ability to [*modify*] the [**TSF**] to [**the associated role listed in** Table 13: Modify TSF data**]**.

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**

TSF Data	**Role**
Templates	**Console Administrator** **Console User who created the custom template** **Console User with associated permission**

Table 13: Modify TSF data

6.6.7 FMT_MTD.1d Explicit Management of TSF data - Delete

FMT_MTD.1.1d The ~~TSF~~ **User Console** shall restrict the ability to [*delete*] the [**TSF**] to [**the associated role listed in** Table 14: Delete TSF data].

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 14: Delete TSF data

6.6.8 FMT_MTD.1e Explicit Management of TSF data - Export

FMT_MTD.1.1e The ~~TSF~~ **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**].

6.6.9 Specification of Management Functions (FMT_SMF.1)

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) Export the Results of Running a Security Check or Policy Template**

]

6.6.10 Security Roles (FMT_SMR.1)

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

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.

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

6.7 Protection of TSF (FPT)

6.7.1 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 unauthorized disclosure during transmission.

6.7.2 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.

6.7.3 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.

6.8 Extended Components (_EXT):

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

6.9 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC v3.1 Release 3, Part 3. The following table summarizes the requirements.

Assurance Class	Assurance Components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security –enforcing functional specification
	ADV_TDS.1	Basic design
AGD Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures

Assurance Class	Assurance Components	
ASE: Security Target evaluation	ASE_CCL	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

7. TOE Summary Specification (ASE_TSS)

This chapter describes the security functions associated with the TOE.

7.1 TOE Security Functions.

The TOE is comprised of seven different security functions:

- Security Audit
- Cryptographic Operations
- User Data Protection
- Identification and Authentication
- Protection of the TOE
- Security Management
- Secure Communications

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

7.2 Security 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.

The Security Audit function is designed to satisfy the following security functional requirements:

Security Audit Generation:	FAU_ARP.1	The TOE allows access to functions based on privileges provided to Console Administrators, Console Users, or Agents. If a user attempts to access the system or make a change they are not authorized for, they receive a message, the transaction is blocked, and an entry is made into the Audit log.
	FAU_GEN.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 9: FAU_GEN.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 Alerts	**FAU_SAA.1**	The TOE can be configured to look at an events occurrence and generate an alarm.
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).

7.3 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 Sun Solaris endpoints is also provided by the TSF.

Secure Hash	FCS_COP.1a	The TSF provides the ability to calculate a secure hash for data using the SHA-1 algorithm, which meets the FIPS 180-3 standard. The secure hash algorithms are used to verify the content integrity of selected files on Sun 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.

7.4 User Data Protection

The NetIQ Secure Configuration Manager product provides the ability to make changes to security configurations, and generate events and alerts based on predefined parameters. The Secure Configuration Manager product is protected by enforcing the privileges associated to SCM Administrators or SCM Users. These privileges are associated in the following ways:

- by virtue of being an SCM Administrator (i.e. having roles assigned as an SCM Administrator),

- having roles assigned as an SCM User

The User Data Protection function is designed to satisfy the following security functional requirements:

Information Access	FDP_ACC.1	The TOE allows access to information by enforcing user privileges as defined by:

		- Assignments of SCM Administrator role - Assignment of SCM User roles
Function access	FDP_ACF.1	The TOE enforces access to functions based on the user privileges as defined by - Assignments of SCM Administrator role - Assignments of SCM User roles
	FIA_ATD.1	The TOE will maintain a list of security attributes belonging to SCM Administrators and SCM Users

7.5 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.

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 permutation 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.
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 Security Management (7.6) for a detailed description of roles and permissions.
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 o Expires in 60 days • Password Strength o Minimum length: 8 characters o Prohibit: 8 previous passwords o At least 2 non-alphabetic characters o Non-alphabetic characters cannot be consecutive within password The verification of secrets is realized by a probabilistic or permutation 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.

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.

7.6 Protection of the TOE

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.

FPT_SEP_EXT.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 10: 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.)

7.7 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.

FMT_MOF.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 10: 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.)

FMT_MSA.1, FMT_MSA.2, FMT_MSA.3

The User Console controls the ability to add, delete, or modify privileges to Authorized Administrators. Privileges are chosen from a pre-configured set, and can be extended via another process. In addition the console TOE provides a default set of privileges when accounts are authorized.

FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c, FMT_MTD.1d., FMT_MTD.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 11: 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 12: 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 13: 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 14: 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.

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 Sun 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.

7.8 Secure Communications

The TOE uses TLS[12] 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

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

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 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
The standards met and key sizes used by the algorithms implementing the secure communications are defined in Section 6.3.

FCS_CKM.1	The TOE provides the ability to generate temporary shared keys for use in TLS or SSL sessions.
FCS_CKM.2, FCS_COP.1c	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.
FCS_COP.1d	The MAC is generated for the transmitted data and is used in TLS/SSL.
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.
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.

8. Appendix A: Roles

8.1 Console Administrators

Provides administrative rights to any console user assigned this role. Assign this role to console users responsible for Secure Configuration Manager configuration and security activities, such as creating policy templates and setting console passwords.

8.2 NetIQ Auditor

Provides permissions to run all reports across all platforms, agents, and systems. Assign this role to console users responsible for network-wide reporting. This role lets you immediately begin identifying vulnerabilities.

8.3 NetIQ Database Legacy Admin

Provides permissions to run all reports and actions on the legacy database platforms. Assign this role to console users who are responsible for database security.

8.4 NetIQ Exception Approval Manager

Provides permissions to approve or disapprove security check exceptions created in Secure Configuration Manager. Assign this role to console users who are responsible for approving and disapproving exceptions.

8.5 NetIQ Exception Manager

Provides permissions to manage security check exceptions created in Secure Configuration Manager. Assign this role to console users who are responsible for maintaining exceptions.

8.6 NetIQ Help Desk

Provides permissions to run all reports and actions related to Help Desk activities. Assign this role to console users who are responsible for Help Desk activities.

8.7 NetIQ iSeries Admin

Provides permissions to run all reports and actions on an iSeries platform. Assign this role to console users who are responsible for iSeries security.

8.8 NetIQ UNIX Admin

Provides permissions to run all reports and actions on a UNIX platform. Assign this role to console users who are responsible for UNIX security.

8.9 NetIQ Windows Admin

Provides permissions to run all reports and actions on a Windows platform. Assign this role to console users who are Domain Admins or are responsible for Windows security.