NetIQ® Group Policy Administrator™ 6.8.2 Security Target

Initial Draft Date:	November 10th 2015
Last Updated:	November 22, 2016
Version:	0.7
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® Group Policy Administrator ™ 6.8.2[1] Security Target
ST Version:	0.7
ST Date:	November 22, 2016
ST Author:	Michael F. Angelo 713-418-5396 angelom@netiq.com

1.2. Target of Evaluation Reference:

TOE Reference:	NetIQ® Group Policy Administrator™ 6.8.2.31
TOE Version #:	6.8.2.31[2]
TOE Developer:	NetIQ Corporation
Evaluation Assurance Level (EAL):	EAL2+
TOE Components:	Console Subsystem NetIQ Group Policy Administrator Server Subsystem

1.3. Target of Evaluation (TOE) Overview:

[1] Note: The official name of the product is: NetIQ® Group Policy Administrator™ 6.8 SP2 (Group Policy Administrator™ 6.8 SP2). The release product can be uniquely identified as Group Policy Administrator™ 6.8.2.31. or Group Policy Administrator™ 6.8.2. The product name may also be abbreviated as GPA 6.8.2 or *GPA 6.8 SP2* or simply *GPA* or the *TOE*. For the purpose of this certification and the associated documentation, all of the above references are equivalent.

[2] Note: Some components, which are not touched by the SP code changes, may reflect the version number as 6.8.0.213.

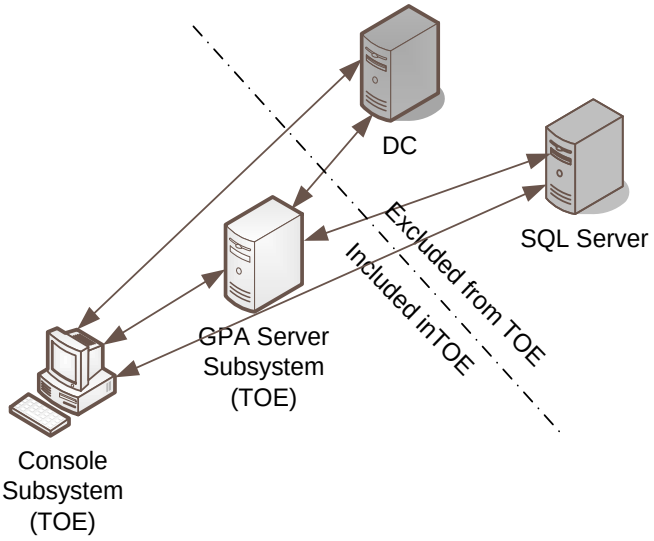

Figure 1: GPA Configuration

The NetIQ GPA 6.8.2 (Figure 1[3] above) consists of the following components:

- Console Subsystem (aka NetIQ Group Policy Administrator Console Subsystem)
- NetIQ Group Policy Administrator Server Subsystem
- Domain Controller (DC) (excluded from evaluation)
- Microsoft SQL Server 2014 Standard or Enterprise Edition (excluded from evaluation)

1.3.1. Product Overview:

NetIQ® Group Policy Administrator™ 6.8.2 (also referred to as GPA) provides the ability to securely model and predict the impact of Group Policy changes in an environment (both offline and online). Whether you are tasked with planning, executing, controlling, troubleshooting or reporting on Group Policies, GPA provides you the controls necessary to help identify and prevent unplanned, unmanaged, or malicious change—improving the security and overall availability of your IT environment.

GPA provides the following capabilities:

A secure offline repository for modeling and testing Group Policy Object (GPO) changes
A robust workflow and delegation model to safely allow for stakeholders to approve change
Built-in tools that help you analyze, compare, troubleshoot, and test GPOs

In addition GPA reduces down time and operational risks to Group Policies that may be caused by malicious or accidental changes.
Key benefits of GPA include:

- **Offers secure offline repository**
  Reduces the number of privileged accounts, by offering secure offline Group Policy management without having to provide permissions within Active Directory.
- **Provides robust workflow and delegation model –**
  Allows administrators to push the administration of Active Directory lower in the organization to safely involve all Group Policy stakeholders.
- **Reduces error risk when configuring GPOs –**

[3] Components that are not part of the TOE are in grey boxes.

Enables you to configure settings once, and then replicate and apply those settings to GPOs in other domains and even other forests. This feature guarantees that your settings are configured correctly and reduces the risk of accidentally mis-configuring or losing a setting.

- **Provides advanced analysis –**
  Simulate the effect of modifying the Group Policy environment without having to first deploy the modified GPO using online Resultant Set of Policy (RSoP) functionality. In addition, health checking, event logging, and the ability to compare GPOs help to quickly troubleshoot errors and take corrective action.
- **Live and offline RSoP analysis –**
  Determines the set of effective policies that apply to a user when logged on to a specific machine in the live environment; simulates the impact of making changes without affecting production; and even allows customers to troubleshoot issues by directly comparing two RSoP reports.
- **Centralized GPO control and synchronization across trust boundaries –**
  Enables GPOs to be centrally controlled and synchronized from domain to domain, both trusted and untrusted, and across forests—even disconnected forests.
- **After-hours GPO deployment –**
  Uses Windows Task Scheduler to schedule unattended GPO roll-outs from the NetIQ® Group Policy Administrator™ repository to AD.
- **Check-out, check-in and approval –**
  Allows GPOs to be checked out before editing and allows only the person checking them out to edit them. The objects can be checked back in after modification. Once complete, approval must be granted for the modification to be transferred to the live Active Directory environment.
- **Tight integration with NetIQ® Change Guardian for Group Policy™ –**
  Allows you to view NetIQ Change Guardian for Group Policy change activity from within GPA for a more complete GPO management experience.
- **Point-in-time analysis reports –**
  Captures what the Group Policy environment looked like at a particular point in time and reports on how many changes have been made and who made them.
- **Rollback features –**
  Provides administrators with a one button rollback capacity to allow a prior version of a GPO to be returned to production.
- **Offline mirror –**
  Provides a utility to automatically mirror production Active Directory Organizational Units and GPOs in an offline repository, making the offline environment look just like the online environment.
- **Enterprise GPO consistency enforcement and comparison** –
  Provides the ability to automatically synchronize GPO changes enterprise-wide with just one click; also provides a GPO comparison report to ensure master GPOs are consistent across domains.
- **Administration delegation –**
  Allows you to strategically limit the authority to create and change GPOs so that Group Policy administration can be delegated without any permissions being granted within Active Directory.
- **Support for Group Policy Preferences –**
  Allows the administrator to manage and assess Group Policy Preferences within GPA

1.3.2. TOE Components:

For the purpose of this certification includes the:

The **NetIQ Group Policy Administrator Console Subsystem** includes the following functionality:

- Enables / disables group policies
- Allows you to edit Group Policy Objects(GPO) Offline

- Enables access to versions
- Provides notification of changes
- Enables workflows

The **NetIQ Group Policy Administrator Server Subsystem** enables the extension and management of Microsoft Group Policies. GPA extends GPA management capability to individuals while:

- protecting Group Policy Objects (GPO) consistency
- providing improved audit capability
-

1.3.3. Major Security Features of the TOE:

The TOE provides the ability to:

- protect GPO consistency [4]
- improve audit capability
- improve the integrity by validating all administrative changes
- enables the ability to automate administrative functions

The TSF provides the following security functions:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Windows Management Policy Proxy

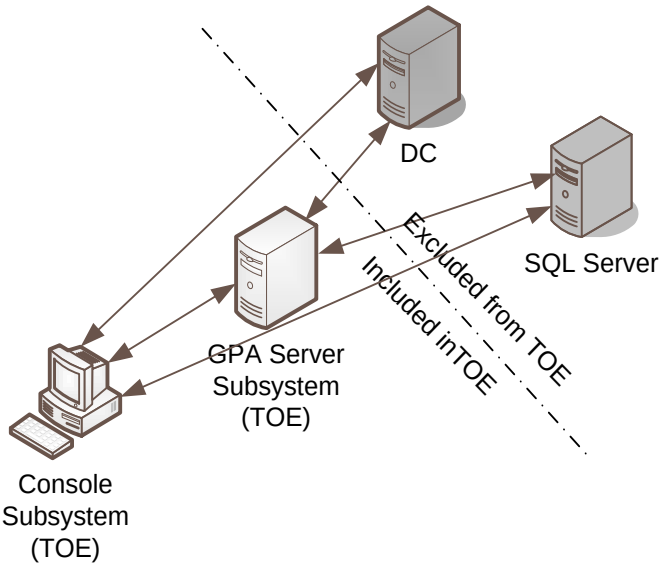

Figure 2: GPA Functional Architecture[5]

1.3.3.1. Security Audit

The TOE can be set up to produce detailed audit reports for events and to aid in their analysis via the use of the Console Subsystem. The TOE reporting capabilities are completely configurable.

1.3.3.2. User Data Protection

[4] Consistency includes rollback
[5] Objects that are in grey boxes are not part of the TOE.

The TOE implements multiple levels of access as well as functions to enforce them. In addition the transactions are authenticated, and exportable. Data can be imported and exported from the TOE as well as moved across different components in the TOE. In addition residual data created by the TOE is cleaned up. Inter-TSF data confidentiality transfers are protected by use of the Operating Environments native communications process.

1.3.3.3. Identification and Authentication

Users of the TOE depend on the IT Environment to handle initial access authentication, however errors and transactions are logged by the TOE. While the TOE depends on the IT Environment for protection of passwords and service credentials (via file protections and access controls), the subject binding[6] is enabled at the SQL Server and the GPA Server.

The subject binding allows the TOE to provide privileges (or groups of privileges) for individuals or groups of individuals.

1.3.3.4. Security Management

Security functions and attributes in the TOE are controlled / managed and specified at different levels or roles by the TSF and the IT Environment . The TOE and IT Environment can also be used to revoke indivual access.

1.3.3.5. Windows Management Policy Proxy

The TOE manages all GPA activities and events. It has features for enabling analysis of potential changes as well as rollback and replay.

1.3.4. TOE Type:

For the purpose of this security target the TOE Type is a **W**indows **M**anagement **Policy Proxy** (WMP).

1.3.5. Non-TOE hardware/software/firmware required by the TOE:

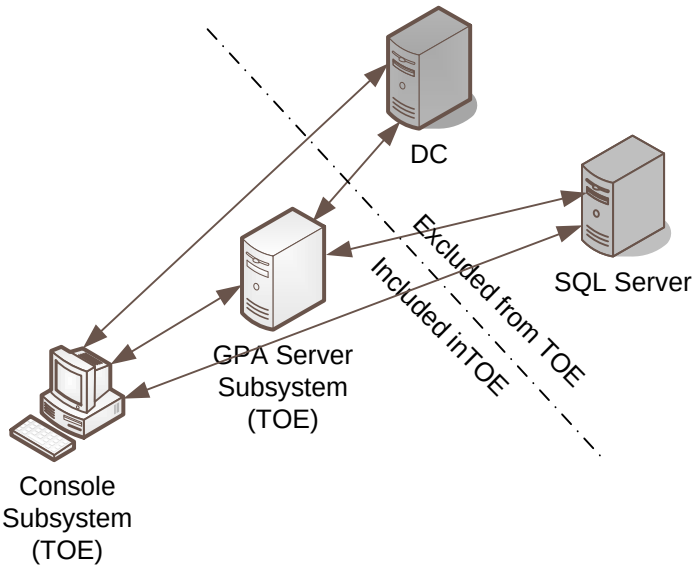

Figure 3: GPA

Note: For the purpose of this evaluation all operating system and the hardware (or emulations in a virtual machine) are excluded.

The Console Subsystem will be evaluated on the following operating systems:

- Windows Server 2012 R2

[6] Subject binding is defined as identifing actions users can take.

- The Console Subsystem requires the following minimum hardware:

  CPU 1 Pentium III, 800MHz
  RAM 1 GB
  Disk space 100 MB

  Note: Or equivalent emulated in a virtual machine.

The GPA Server Subsystem will be evaluated on the following operating systems:

- Windows Server 2012 R2
- The GPA server requires the following minimum hardware:

  CPU 1 GHz (x86 processor) or 1.4 GHz (x64 processor)
  RAM 1 GB
  Disk space 100 MB

  Note: Or equivalent emulated in a virtual machine.

The SQL Server will be installed on the following operating systems:

- Windows 2012 Server R2
- The SQL Server requires the following minimum hardware:

  CPU 1 GHz (x86 processor) or 1.4 GHz (x64 processor)
  RAM 1 GB
  Disk space 1 GB (able to expand to 5 GB)

  Note: Or equivalent emulated in a virtual machine.

1.3.6. Excluded TOE Items:

These environments (components) are not part of the TOE, but are required to demonstrate TOE functionality.

- DC: The DC can run on the following operating systems:
  - Windows 2012 Server R2

In addition the system requires 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.

For those components that are resident on a Microsoft Operating System, the encryption technology is provided natively by Microsoft as part of the operating environment. The encryption technology has been certified by NIST to be FIPS validated.

Finally the system employs SSL, MSMQ, DCOM, and .net Remoting for communications, which are provided by a third party and are not part of the TOE.

The operating system environment(s) are responsible for providing FIPS Certified encryption. Currently the following environments have FIPS certifications.

OS	Cert #	Description
Windows Server 2012 R2	2357	Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll)
	2356	Kernel Mode Cryptographic Primitives Library (cng.sys)
	2355	Code Integrity (ci.dll
	2354	BitLocker® Dump Filter (dumpfve.sys)
	2353	BitLocker® Windows Resume (winresume)

OS	Cert #	Description
	2352	BitLocker® Windows OS Loader (winload)
	2351	Boot Manager

Table 1: FIPS Certificate Numbers

1.3.7. Evaluated Configuration:

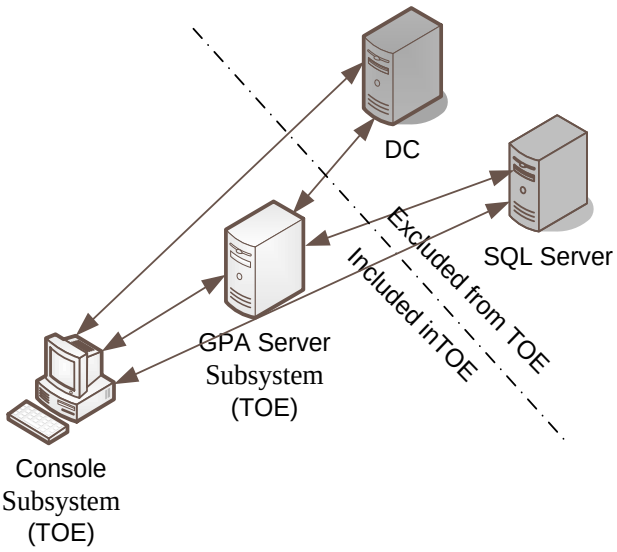

Figure 4: Evaluated Configuration

Those elements labeled TOE in Figure 4 are covered by this ST.

- Console Subsystem:
  - While the Console Subsystem can run on multiple operating systems, it will be evaluated on the following operating system:
    - Windows 2012 R2
- GPA Server Subsystem:
  - The GPA Server Subsystem will be evaluated on the following operating systems:
    - Windows 2012 R2

1.3.8. TOE Physical Scope:

The NetIQ Group Policy Administrator is a software only TOE; The TOE physical boundary consists of the Console Subsystem, the GPA Server Subsystem running on their supporting operating systems and hardware. User installation and guidance documentation is supplied with the TOE. For the purpose of this evaluation the Domain Controller (DC) is not included in the TOE.

The components that make up the evaluated configuration are:

- Console Subsystem
- GPA Server Subsystem

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**]).
  - 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*]).
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as acronyms, definitions, or captions.

1.5. Acronyms:

AD	Active Directory
API	Application programming interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
DC	Domain Controller
GPA	Group Policy Administrator
GPO	Group Policy Objects
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HLD	High-level Design
IA	Initial Assessment
IDS	Intrusion Detection Systems
NSS	Network Security System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NRC	NetIQ Reporting Center Console
NSA	National Security Agency
OS	Operating system
PP	Protection Profile
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
TSF	TOE Security Functionality
TSP	TOE Security Policy
UI	User Interface
WMP	Windows Management Policy Proxy

Table 2: Acronyms

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 (ASE_CCL)

This TOE and ST are 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
- The TOE is augmented with ALC_FLR.1 Basic Flaw remediation.
- The Evaluation Assurance Level (EAL) is 2+ (EAL2+)

2.1. PP Claim

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

2.2. 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.

2.3. Conformance Rationale:

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

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 (EAL2+) 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
- Subjects 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 on the GPA Server and the SQL Server.
- Configuration information stored on the GPA Server Subsystem, SQL Server, and Console Subsystem.
- Data in transit from / to the GPA Server Subsystem, SQL Server, and the Console Subsystem.

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
- Subjects

3.1.2. Subjects:

3.1.2.1. Administrators:

The Administrators can perform all tasks associated with Group Policy Objects (GPOs). These tasks are enumerated in Appendix A.

3.1.2.2. GPA Admin[7]:

The GPA Admin can perform all tasks associated with Group Policy Objects (GPOs). These tasks are enumerated in Appendix A.

3.1.2.3. GPA Users:

GPA Users are delegated one or more task functions from the enumerated list in Appendix A, based on their responsibilities in the GPA. For ease of use, roles have been grouped into the following:

- GPO Importer
- GPO Exporter
- GPR Security Manager
- GPO Approver
- GPO Synchronizer

These default roles may be customized to include other privileges.

3.1.3. Attacker:

[7] A GPA Admin is a user who is in the GPA_REPOSITORY_MANAGEMENT group. By default the user installing/configuring GPA is in this group, but others can be assigned to it as need be.

An Attacker is a person (or persons) who is not a user or administrator, and does not have 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 DC and subsequent Active Directory (AD) and create / modify / delete group policy objects (GPO)
- access the GPA repository and create / modify / delete group policy objects (GPO)
- delete all Group Policy entries in the AD
- view the contents of the AD and GPA repository

3.2. Assumptions

3.2.1. Intended Usage Assumptions

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
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.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.

3.2.2. Physical Assumptions

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

3.2.3. 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.

3.2.4. 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.

3.3. Threats

3.3.1. Threats to the TOE

T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to TOE data or TOE resources.
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.MAL_INTENT	An authorized user could initiate changes that grant themselves additional unauthorized privileges.
T.TSF_COMPROMISE	A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.MAL_ACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
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.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.SC_NVUL	Vulnerabilities may exist in the IT System the TOE is installed on which causes the TOE to be compromised.

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.MANAGE	The TOE will allow administrators to effectively manage the TOE and its security functions,
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows.
O.RESPONSE	The TOE must respond appropriately to trigger events.
O.GPA_AUTH	The TOE must ensure that only authorized users are able to access functionality.
O.GPA_AUDIT	The TOE must collect and store transactional information that can be used to audit changes to the AD and group policy objects.
O.GPA_REP	The TOE must provide identification for source and target objects.
O.GPA_ACPOL	The TOE must provide an access policy.
O.TOE_PROTECTION	The TOE must enable the detection of external interference or tampering and allow for mitigation.

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.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.INTROP	The TOE is interoperable with the AD Environment it manages.

4.3. Security Objectives for the IT Environment

OE.ADMIN_ROLE	The IT Environment will provide authorized administrator roles to isolate administrative actions.
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.
OE.CRYPTO_PROT	The IT Environment will provide FIPS 140-2 Certified encryption and FIPS 180-3 compliant hashes.

4.4. 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

4.5. Security Objectives Rationale

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

4.5.1. Security Objectives Rationale for the TOE and Environment

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

		O.ADMIN_ROLE	O.MANAGE	O.OFLOWS	O.RESPONSE	O.GPA_AUTH	O.GPA_AUDIT	O.GPA_REP	O.GPA_ACPOL	O.TOE_PROTECTION	OE.ADMIN_ROLE	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TIME	OE.TOE_PROTECTION	OE.CRYPTO_PROT
Threats to the TOE	T.ADMIN_ERROR		x													
	T. MASQUERADE	x				x	x	x	x		x	x	x			x
	T.NO_HALT	x			x											
	T.PRIV	x				x	x									
	T.MAL_INTENT				x		x		x	x				x	x	
	T.TSF_COMPROMISE														x	x
	T.MAL_ACT				x		x			x				x	x	
	T.MIS_NORULE						x		x							
	T.SC_MISCFG					x			x							
	T.SC_MALRUN						x	x								
	T.SC_NVUL			x											x	

Table 3: Threats to Objective Correspondence

4.5.1.1. 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 assistant 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.

4.5.1.2. T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

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.GPA_AUTH: The TOE counters this threat by re-verifying the user credentials prior to execution of commands as well as mapping credentials to explicit sets of privileges.

O.GPA_AUDIT: The TOE counters this threat by providing transactional based audit capabilities.

O.GPA_REP: The TOE counters this threat by providing identification for all

	source and target objects transactions.
O.GPA_ACPOL:	The TOE counters this threat by use of an access policy that restricts authorized entities to specific activities.
OE.ADMIN_ROLE:	The IT Environment counters this threat by providing authorized roles to isolate actions.
OE.USER_AUTHENTICATION:	The IT Environment counters this threat by verifying the claimed identity of users.
OE.USER_IDENTIFICATION:	The IT Environment counters this threat by uniquely identify users.
OE.CRYPTO_PROT:	The IT Environment counters this threat by providing FIPS certified encryption for use in protecting the communications channel as well as authentication.

4.5.1.3. 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.

4.5.1.4. 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. Note: Authorized assistant administrators are users with privileges specified in Appendix A.
O.GPA_AUTH:	The TOE counters this threat by evaluating the request to defined sets of privileges.
O.GPA_AUDIT:	The TOE counters this threat by providing transactional based audit capabilities.

4.5.1.5. T.MAL_INTENT:

An authorized user could initiate changes that grant themselves additional unauthorized privileges.
This Threat is countered by ensuring that:

O.RESPONSE:	The TOE counters this event by responding appropriately to trigger events.
O.GPA_AUDIT:	The TOE counters this event by collecting and storing transactional information that can be used to audit changes to the AD.
O.GPA_ACPOL:	The TOE counters this threat by providing an access policy.
O.TOE_PROTECTION:	The TOE counters this by providing detailed audit logs as well as

	the ability to rollback changes.
OE.TIME:	The IT Environment counters this threat by providing a time source.
OE.TOE_PROTECTION:	The IT Environment counters this threat by protecting the TOE and its assets from external interference or tampering.

4.5.1.6. 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:

OE.TOE_PROTECTION:	The IT environment will protect the TOE and its assets from external interference or tampering.
OE.CRYPTO_PROT:	The IT Environment counters this threat by providing FIPS certified encryption for use in protecting the communications channel as well as authentication.

4.5.1.7. T. MAL_ACT

Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
This Threat is countered by ensuring that:

O.RESPONSE:	The TOE counters this threat by responding to events that may indicate attempts to perform unauthorized activities.
O.GPA_AUDIT:	The TOE counters this threat by collecting and storing transactional information that can be used to audit changes to the AD.
O.TOE_PROTECTION:	The TOE counters this by providing detailed audit logs as well as the ability to rollback changes.
OE.TIME:	The IT Environment counters this threat by providing a time source.
OE.TOE_PROTECTION:	The IT Environment counters this threat by protecting the TOE and its assets from external interference or tampering.

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

4.5.1.9. 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.GPA_AUTH:	The TOE protects against this threat by ensuring that only authorized administrators are able to access functionality.
O.GPA_ACPOL:	The TOE counters this threat by providing an access policy.

4.5.1.10. 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.
This Threat is countered by ensuring that:

O.GPA_AUDIT: The TOE counters this threat by providing transactional based audit capabilities.

O.GPA_REP: The TOE counters this threat by providing identification for all source and target bobjects transactions.

4.5.1.11. T. SC_NVUL

Vulnerabilities may exist in the IT System the TOE is installed on which causes the TOE to be compromised.
This Threat is countered by ensuring that:

O.OFLOWS: The TOE handles potential System data storage overflows.

OE.TOE_PROTECTION: The IT Environment protects the TOE and its assets from external interference or tampering.

4.6. 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.PERSON	OE.PHYCAL	OE.INTROP
Intended usage assumptions	A.ACCESS					x
	A.ASCOPE					x
	A.DYNMIC			x		x
Physical assumptions	A.LOCATE				x	
Personnel assumptions	A.MANAGE			x		
	A.NOEVIL	x	x			
Connectivity assumptions	A.AVAIL				x	x
	A.CONFIG				x	x
	A.NETCON				x	x

Table 4: Complete coverage – environmental assumptions

4.6.1. 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.

4.6.2. 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.

4.6.3. 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.

4.6.4. 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.

4.6.5. 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.

4.6.6. 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

4.6.7. 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.

4.6.8. 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.

4.6.9. A.NETCON

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

OE.PHYCAL:	The OE.PHYCAL objective ensures that the network interfaces are properly configured for use by the TOE.
OE.INTROP:	The OE.INTROP objective ensures that the network interface is configured to properly interoperate with the environment and the

TOE.

4.7. Security Requirements Rationale

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

	O.ADMIN_ROLE	O.MANAGE	O.OFLOWS	O.TOE_PROTECTION	O.RESPONSE	O.GPA_AUTH	O.GPA_AUDIT	O.GPA_REP	O.GPA_ACPOL
FAU_ARP.1					X				
FAU_GEN.1				X			X		
FAU_SAA.1					X				
FAU_SAR.1							X		
FAU_STG.1			X	X			X		
FDP_ACC.1				X		X		X	X
FDP_ACF.1									X
FIA_ATD.1	X								
FMT_MOF.1		X					X		
FMT_MSA.1		X				X			
FMT_MSA.3		X				X			
FMT_MTD.1		X					X		
FMT_SMF.1		X							
FMT_SMR.1	X								
WMP_ADM.1(EX)	X	X							
WMP_VLD.1(EX)	X	X				X			

Table 5: Objective to Requirement Correspondence

4.7.1. 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:	The TOE maintains authorization information that determines which TOE functions a role may perform.
FMT_SMR.1:	The TOE recognizes any user account that is assigned in the IT environment to one or more system-defined operating system user groups[8] as an "authorized administrator".
WMP_ADM.1(EX):	The TOE provides authorized administrators [9]with the ability to delegate to GPA Users the ability to interactively modify resources using the UI.
WMP_VLD.1(EX):	The TOE shall identify the association between the users and their privilege's prior to performing a task.

[8] In this case we are using the Domain Administrators, GPA Admins, and GPA Users groups.
[9] Administrators are defined as Domain Administrators or GPA Admins.

4.7.2. O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions.
This TOE Security Objective is satisfied by ensuring that:

FMT_MOF.1:	The TOE restricts the ability to manage WMP settings to authorized administrators.
FMT_MSA.1:	The TOE will enforce access controls that restrict the ability to alter security attributes to Administrators, GPA Admins[10].
FMT_MSA.3:	The TOE will enforce a default set of privileges as well as allowing the Administrators to change the default set of privileges.
FMT_MTD.1:	The TOE restricts the ability to modify the GPO privileges to Administrators and GPA Admins.
FMT_SMF.1:	The TOE provides authorized administrators with the ability to manage WMP settings and review collected data and correlation reports.
WMP_ADM.1(EX):	The TOE provides authorized administrators[11] with the ability to delegate to GPA Users the ability to interactively modify resources using the UI.
WMP_VLD.1(EX):	The TSF shall identify the association between the users and their privilege's prior to performing a task.

4.7.3. O. OFLOWS

The TOE must appropriately handle potential System data storage overflows
This TOE Security Objective is satisfied by ensuring that:

FAU_STG.1:	The TOE protects audit information for all transactions.

4.7.4. O.TOE_PROTECTION

The TOE must provide protection from, and detection of, external compromise.

FAU_GEN.1:	The TOE provides the ability to generate audit records.
FAU_STG.1:	The TOE protects audit information for all transactions.
FDP_ACC.1:	The TOE can be configured to limit access to Administrators, GPA Admins, or GPA Users.

4.7.5. 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.

4.7.6. O.GPA_AUTH

The TOE must ensure that only authorized users are able to access functionality.

[10] Note GPA Users are not included here as GPA Users can not alter security attributes (i.e. delegate or add privileges) to other users or themselves. This activity is reserved for Administrators and GPA Admins.
[11] Administrators are defined as Domain Administrators or GPA Admins.

This TOE Security Objective is satisfied by ensuring that:

FDP_ACC.1:	The TOE can be configured to limit access to Administrators, GPA Admins, or GPA Users.
FMT_MSA.1:	The TOE will enforce access controls that restrict the ability to alter security attributes to Administrators and GPA Admins.
FMT_MSA.3:	The TOE will enforce a default set of privileges as well as allowing the Administrators and GPA Admins to change the default set of privileges.
WMP_VLD.1(EX):	The TSF shall identify the association between the users and their privilege's prior to performing a task.

4.7.7. O.GPA_AUDIT

The TOE collects and stores transactional information that can be used to audit changes to the Active Directory.

This TOE Security Objective is satisfied by ensuring that:

FAU_GEN.1:	The TOE provides the ability to generate audit records.
FAU_SAR.1:	The TOE provides authorized users the capability to read all audit information.
FAU_STG.1:	The TOE provides the ability to protect the audit record.
FMT_MOF.1:	The TOE restricts the ability to enable and disable the functions that enable changes to the Group Policy Objects (GPOs) and audit capabilities to Administrators, GPA Admins, or GPA Users.
FMT_MTD.1:	The TOE restricts the ability to modify the GPO Privileges to Administrators and GPA Admins

4.7.8. O.GPA_REP

The TOE must provide identification for source and target objects.

This TOE Security Objective is satisfied by ensuring that:

FDP_ACC.1:	The TOE can be configured to limit access to Administrators, GPA Admins, or GPA Users.

4.7.9. O.GPA_ACPOL

The TOE must provide an access policy.

This TOE Security Objective is satisfied by ensuring that:

FDP_ACC.1:	The TOE can be configured to limit access to Administrators, GPA Admins, or GPA Users.
FDP_ACF.1:	The TOE can be configured to enforce access control to objects.

4.8. Security Assurance Requirements Rationale

EAL2+ 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 EAL2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.
The ALC_FLR.1 augmentation was claimed since fault level remediation is important to the customers of the product.

4.8.1. 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	FPT_STM.1	Environment Security Objective OE.TIME
FAU_SAA.1	FAU_GEN.1	Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_STG.1	FAU_GEN.1	Included
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Included
FIA_ATD.1	None	None
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	Included
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	Included Included Included
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Included Included
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	Included
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Met by OE.USER_IDENTIFICATION
WMP_ADM.1(EX)	FAU_GEN.1	Included
WMP_VLD.1(EX)	None	None

Table 6: Requirement Dependency

4.9. Explicitly Stated Requirements Rationale

A class of WMP requirements was created to specifically address the administrative proxy capability of a WMP. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique functionality of WMP's including capabilities for making, reviewing, and managing administrative changes. These requirements have no dependencies since the stated requirements embody all the necessary security functions, with the exception of time stamps provided by the IT environment to support event correlation.

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 work 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.
The table (below) describes the relationship between security requirements and security functions.

SFRs	TOE Security Functions				
	Security Audit	User Data Protection	Identification & Authentication	Security Management	Windows Management Policy Proxy
FAU_ARP.1	X				
FAU_GEN.1	X				
FAU_SAA.1	X				
FAU_SAR.1	X				
FAU_STG.1	X				
FDP_ACC.1		X			
FDP_ACF.1		X			
FIA_ATD.1		X	X	X	
FMT_MOF.1				X	
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
WMP_ADM.1(EX)	X	X			X
WMP_VLD.1(EX)			X		X

Table 7: Security Functions vs. Requirements Mapping

5. Extended Components Definition (ASE_ECD)

5.1. Class WMP: Windows Management Policy Proxy:

This chapter defines a new class required by GPA called a Windows Management Policy Proxy abbreviated WMP. The class consists of the following family members WMP_ADM and WMP_VLD. This class is defined because the Common Criteria (Part 2 and Part 3) does not contain any SFRs which cover these functions. The families in this class address requirements for data review, alarms, collection controls, correlation, and loss prevention.

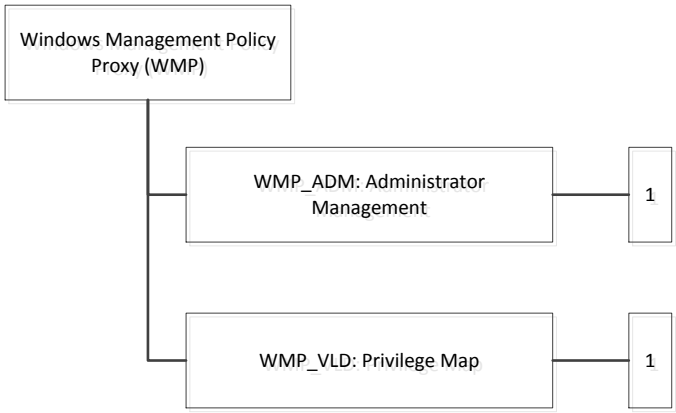

Figure 5: Class Decomposition

Class	Component
WMP: Windows Management Policy Proxy	WMP_ADM.1(EX): Administrator Management WMP_VLD.1(EX): Privilege Map

Extended Functional Components

5.2. Administrator Management (WMP_ADM)

5.2.1. Family Behavior

For the TOE described in this ST it was necessary to provide authorized entities with a mechanism to read and perform administrative functions as authorized.
This mechanism is covered by the WMP_ADM family and contains the components as shown in the figure below.

5.2.2. Component Leveling:

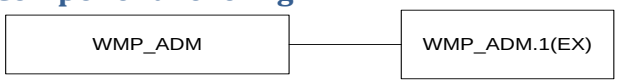

Figure 6: WMP_ADM Component Leveling

WMP_ADM.1(EX) Administrative management enables how administrators can delegate privileges or groups of privileges to users.

5.2.3. Management:

There are no management activities foreseen.

5.2.4. Audit: WMP_ADM.1 (EX)

The following actions should be auditable:

a) Start-up and shutdown of GPA.
b) Changes to configuration.
c) All delegations of administrative roles.

5.2.5. Administrator Management (WMP_ADM.1 (EX))

WMP_ADM.1.1(EX) The TSF shall provide administrators the ability to delegate to authorized users the capability to issue administrative commands and make system changes.

WMP_ADM.1.2(EX) The TSF shall provide administrators the ability to delegate to authorized users or groups of authorized users an ability or set of abilities.

5.2.5.1. Dependencies:

FAU_GEN.1

5.3. Privilege Map (WMP_VLD)

5.3.1. Family Behavior

For the TOE described in this ST it was necessary to provide the ability to map users to privileges and sets of privileges prior to performing a task.
This mechanism is covered by the WMP_VLD family and contains the components as shown in the figure below.

5.3.1.1. Component Leveling:

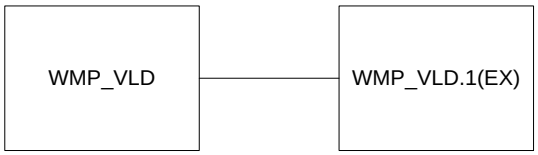

Figure 7: WMP_VLD Component Leveling

5.3.2. Privilege Map (WMP_VLD.1 (EX))

WMP_VLD.1.1(EX) The TSF shall identify the association between the users and their privilege's prior to performing a task.

5.3.3. Management:

There are no management activities foreseen.

5.3.4. Audit: WMP_VLD.1(EX)

There are no audit functions foreseen.

5.3.5. Dependencies:

There are no dependencies.

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_SAA.1: Potential violation analysis
	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FDP: User Data Protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and Authentication	FIA_ATD.1: User attribute definition
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.1: Management of 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
WMP: Windows Management Policy Proxy	WMP_ADM.1(EX): Administrator Management
	WMP_VLD.1(EX): Privilege Map

Table 8: TOE Security Functional Requirements

6.1.1. Security Audit (FAU)

6.1.1.1. Security alarms (FAU_ARP.1)

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

6.1.1.2. Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*detailed*] level of audit; and
c) [**transactional to trace log, server side auditing to event log**].

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, [**server side auditing**].

6.1.1.3. 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.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [**no such events specified**] known to

indicate a potential security violation;
b) [**all transactions performed by authorized TOE users**].

6.1.1.4. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**Administrators, GPA Admins**] with the capability to read [**all audit information**] from the audit records.

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

6.1.1.5. 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.

6.1.2. User Data Protection (FDP)

6.1.2.1. Subset access control (FDP_ACC.1)

FDP_ACC.1: The TSF shall enforce the [**access control**] on [**All GPA Components for read, write, modify, or execute access provided to authorized administrators.**]

6.1.2.2. 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:**
System Administrators group or
Membership in the GPA Administrators group, or
by membership in the GPA Users[12] groups
for Read, Write, Execute access to All GPA 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 of functionality based on membership in either the System Administrators group, or membership in the GPA Administrators group, or by membership in the GPA Users[13]] 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: [**users not in the System Administrators group, or the GPA Administrators group, or defined as GPA Users**[14]].

6.1.3. Identification and authentication (FIA)

6.1.3.1. User attribute definition (FIA_ATD.1)

FIA_ATD.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~: **roles**: [**authorizations**].

6.1.4. Security management (FMT)

6.1.4.1. Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [*enable and disable*] the functions

[12] GPA Users is a definition for users that have privileges granted from table 11.
[13] GPA Users is a definition for users that have privileges granted from table 11.
[14] GPA Users is a definition for users that have privileges granted from table 11.

[**that enable changes to the Group Policy Objects (GPOs) and audit capabilities**] to [**Administrators, members of the GPA Admin group**].

6.1.4.2. Management of Security Attributes (FMT_MSA.1)

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

6.1.4.3. 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 [**Administrators, GPA Admins**] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify*] the [**GPO privileges**][15] to [**Administrators, GPA Admins**].

6.1.4.5. Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**Modify the behavior of users**].

6.1.4.6. Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrators, GPA Admins, GPA Users**].

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

6.1.5. Windows Management Policy Proxy (WMP)

6.1.5.1. Administrator Management (WMP_ADM.1 (EX))

WMP_ADM.1.1(EX) The TSF shall provide administrators the ability to delegate to authorized users the capability to issue administrative commands and make system changes.

WMP_ADM.1.2(EX) The TSF shall provide administrators the ability to delegate to authorized users or groups of authorized users an ability or set of abilities.

6.1.5.2. Privilege Map (WMP_VLD.1 (EX))

WMP_VLD.1.1(EX) The TSF shall identify the association between the users and their privilege's prior to performing a task.

6.2. 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 TOE consists of the requirements specified for EAL2 of assurance augmented by Basic Flaw Remediation (ALC_FLR.1). The following table summarizes the requirements. The following table summarizes the requirements.

[15] GPO Privileges are defined in Appendix A.

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
	ALC_FLR.1	Flaw Remediation Procedures
ASE: Security Target evaluation	ASE_CCL.1	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

Table 9: Security Assurance Requirements

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 three different security functions:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Windows Management Policy Proxy

7.2. Security Audit

The NetIQ Group Policy Admnsitrator provides the ability to make changes to Group Policy Objects. When the Adminsitrators, GPA Admins, or GPA Users make a change using NetIQ GPA, changes are logged. In addition the GPA Users can not delegate or alter their privileges.

All commands and changes are logged and can be rolled back as well.

Access to the GPA audit is restricted to Administrators and GPA Admins.

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

FAU_ARP.1	The TOE allows access to functions based on explicit privileges (powers) provided to Administrators, GPA admins, or GPA Users. If a user attempts to 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	The TOE generates audit data for ALL transactions attempted and executed through GUI/UI (Console Subsystem).
FAU_SAA.1	The TOE provides functions to analyze audit events and trends as part of the GUI/UI (Console Subsystem) analysis reporting subsystem.
FAU_SAR.1	The TOE provides event audit review as part of the GUI / UI (Console Subsystem).
FAU_STG.1	The TOE stores audit event information in a protected area on the GPA Server Subsystem.
WMP_ADM.1(EX)	The TOE provides Administrators the ability to delegate the capability to issue administrative commands and changes.

7.3. User Data Protection

The GPA provides protection of the group policy objects by enforcing the privileges associated to individual users. These privileges are associated in the following ways:

- by virtue of being an Administrator (i.e. membership in the Administrators group),
- or being in the a GPA Administrators group,
- or by having privileges specified in the privilege table.

FDP_ACC.1	The TOE allows access to information by enforcing user privileges as defined by being a GPA Administrator, or by being a GPA User, or by being in the Systems Administrator group.
FDP_ACF.1	The TOE enforces access to functions based on the user privileges as defined by being a GPA Administrator, or by being a GPA Users, or by being in the Systems Administrator group.

FIA_ATD.1	The TOE will maintain a list of security attributes belonging to individual roles (authorizations) (i.e. for GPA Admins and GPA Users).
WMP_ADM.1.1(EX)	The TOE defines mechanisms for Administrators or GPA Admins to delegate privileges to individuals.
WMP_ADM.1.2(EX)	The TOE defines mechanisms for Administrators or GPA Admins to delegate privileges to users or groups of users an ability or set of abilities.

7.4. Identification and Authentication

GPA provides a user Console Interface GUI / UI that administrators may use to define GPA Admins as well as delegate responsibilities to Users (GPA Users). The GPA Console Interface GUI / UI application does not identify and authenticate individual administrators. When an Administrator, GPA Admin, or GPA User attempts to access the GPA Console Interface GUI / UI, the GPA Console Interface GUI / UI gets the users credentials from the operating system. These credentials are then forwarded to the IT environment. Note that, if the credentials are insufficient to perform any tasks, the Console Subsystem exits.

If the user has been successfully identified and authenticated by the environment, and if the user has been successfully identified and authenticated as an Administrator, GPA Admin, or GPA User, the GPA Console Interface GUI / UI provides access to the appropriate interfaces. Authorization data maintained by the TOE for each role that the TOE recognizes is used to determine the functions that a user possessing a given role may perform.

The TOE recognizes the following operating system groups and users which each correspond to TOE roles:

- Administrators
- GPA Admins
- GPA Users

Operating system groups and functions are described further in section 3.1.2.

The Identification and authentication function is designed to satisfy the following security functional requirements:

FIA_ATD.1	The TOE maintains authorization information that determines which TOE functions a role may perform.
WMP_VLD.1(EX)	The TOE shall determine a user's privilege, via a user privilege mapping, prior to performing a task.

7.5. Security Management

The GPA application includes the following components:

- Console Subsystem
- GPA Server Subsystem
- SQL Servers (not part of TOE)
- Domain Controller (not part of TOE)

To use the Console Subsystem, the authorized Administrator must be a member of one of the following groups:

- Administrators
- GPA Admins
- GPA Users

In order for the program to function, the System Administrator (as defined by the IT Environment) must access the AD and either assign users to the groups above or enable them with privileges as specified in Appendix A.

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

FIA_ATD.1	The TOE maintains authorization information that determines which TOE functions an Administrator, GPA Admin or GPA User may perform.
FMT_MOF.1	The TOE restricts the ability to manage WMP settings to authorized Administrators and authorized GPA Admins.
FMT_MSA.1	The TOE restricts access to modify, add, or delete the privileges to Administrators and GPA Admins.
FMT_MSA.3	The TOE provides a default set of privileges as well as the ability for Administrators and GPA Admins to modify the default.
FMT_MTD.1	The TOE restricts the ability to modify the GPO privileges[16] to Administrators and GPA Admins.
FMT_SMF.1	The TOE provides authorized Administrators and GPA Admins with the ability to manage GPA Admins and GPA Users.
FMT_SMR.1	The TOE maintains roles for Administrators, GPA Admins, and GPA Users.

7.6. Windows Management Policy Proxy

The NetIQ GPA Console Subsystem allows users access to its interfaces according to their membership in the Administrators Group, GPA Admins, or GPA Users. Membership, in each of these groups, enables roles that the NetIQ GPA Console Subsystem recognizes. The application-based Console Interface GUI / UI performs this check when they are invoked using operating system interfaces.

The TOE relies on the operating system in the environment to protect its application components and to provide a secure runtime environment. The TOE uses SSL, dotNET, DCOM, or SHTTP to protect communication between the components (Console Subsystem, GPA Server Subsystem).

The Protection of the TSF function is designed to satisfy the following security functional requirements:

WMP_ADM.1(EX)	The TOE provides the ability for Administrators and GPA Admins the ability to delegate to individuals or groups of individuals an ability or group of abilities.
WMP_VLD.1(EX)	The TOE will identify a user's privilege, prior to performing a task.

[16] GPO Privileges are defined in Appendix A

8. Appendix A - Privileges

#	Task	Notes
1	Full Control	Sets permissions for all tasks at all levels
2	Full GP Repository Server Control	Sets permissions for tasks 3-5
3	Add GP Repository User	This privilege allows the addition of a GP Repository User
4	Add Remote User	This privilege allows the addition of a Remote User
5	Customize Deployment Options	This privilege allows the Customization of Deployment Options
6	Full Domain Control	Sets all domain-level permissions for tasks 8, 9, 10, 12, and 14
7	Create New Domain	This privilege allows the Cteation of a New Domain
8	Delete Domain	This privilege allows the Deletion of a Domain
9	Migrate GPO	This privilege allows the Migration of a GPO
10	Import GPO from Active Directory	This privilege allows the Importation of a GPO from an Active Directory
11	Synchronize ADMX from the Central Store	This task is directly associated with the Import GPO from Active Directory task at the GP Repository and domain levels. You cannot set permissions for this task directly. When you enable the Import GPO from Active Directory task, you also set permissions for this task.
12	Export GPO to Active Directory	This privilege allows the Exportation of a GPO to an Active Directory
13	Export ADMX to the Central Store	This task is directly associated with the Export GPO to Active Directory and Modify Export Status tasks at the GP Repository and domain levels. You cannot set permissions for this task directly. When you enable the Export GPO to Active Directory and Modify Export Status tasks, you also set permissions for this task.
14	Edit Domain Maps	This privilege allows the Editting of Domain Maps
15	Full Category Control	Sets all category-level permissions for tasks 16-19
16	Create Category	This privilege allows the Creation of a Category
17	Delete Category	This privilege allows the Deletion of a Categoy
18	Paste GPO Category Link	This privilege allows the Pasting of a GPO Category Link
19	Rename Category	This privilege allows a Category to be Renamed
20	Full GPO Control	Sets all permissions below this level except Manage GPR Security
21	Create GPO	This privilege allows the Creation of a GPO
22	Add ADMX	This task is directly associated with the Create GPO task at the GP Repository and domain levels. You cannot set permissions for this task directly. When you enable the Create GPO task, you also set permissions for this task.
23	Modify GPO	Sets permissions for tasks 24-27
24	Modify GPO Settings	Allows the Modification of GPO Settings
25	Modify GPO Links	Allows the Modification of GPO Links
26	Modify GPO Security	Allows the Modification of GPO Security
27	Rename GPO	Allows a GPO to be Renamed
28	Delete GPO	Allows the Deletion of a GPO
29	Remove ADMX	This task is directly associated with the Delete GPO task at the GP Repository and domain levels. You cannot set permissions for this task directly. When you enable the Delete GPO task, you also set permissions for this task.

#	Task	Notes
30	Check Out GPO	Allows a GPO to be Checked Out.
31	Override Check Out	Allows the overriding of a Checked Out GPO
32	Rollback	Allows a GPO change to be Rolled Back
33	Approve/ Unapprove GPO	Allows a GPO to be Approved or Unapproved
34	Approve/ Unapprove ADMX Files	This task is directly associated with the Approve/ Unapprove GPO task at the GP Repository and domain levels. You cannot set permissions for this task directly. When you enable the Approve/ Unapprove GPO task, you also set permissions for this task.
35	Modify Export Status	Allows the Export Status of a GPO to be Modified
36	Modify GPO Security Filters	Allows GPO Security Filters to be Modified
37	Modify GPO Enterprise Sync	Enables user to designate master and controlled GPOs
38	GPO Synchronizer	Enables user to modify GPOs using Enterprise Synchronization
39	Manage GPR Security	Enables user to change all security settings

Table 10: Tasks