NetIQ® Directory and Resource Administrator 10.2.3

Security Target

Last Updated:	March 24, 2025
Version:	1.14
Prepared By:	OpenText
Prepared For:	OpenText 275 Frank Tompa Drive Waterloo ON N2L 0A1 Canada

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
- Security Target conventions
- Acronyms
- Security Target Organization

1.1. Security Target Reference:

ST Title:	NetIQ ®Directory Resource Administrator 10.2.3 Security Target
ST Version:	1.14
ST Date:	March 24, 2025
ST Author:	Michael F. Angelo Mangelo2@opentext.com

1.2. Target of Evaluation Reference:

TOE Reference:	NetIQ®Directory Resource Administrator10.2.3[1]
TOE Version #:	10.2.3.0.2175
TOE Developer:	OpenText
Evaluation Assurance Level (EAL):	EAL2+
TOE Components:	Console Subsystem DRA Server Subsystem

1.3. Target of Evaluation Overview (TOE):

1.3.1. Product Overview:

The NetIQ® Directory Resource Administrator™ 10.2.3 (DRA) product enables the extension and management of Microsoft Active Directory (AD). DRA extends AD management capability to individuals while:

- protecting AD consistency
- providing improved audit capability
- improving the integrity by validating all administrative changes
- enables the ability to automate administrative functions

DRA does this by providing:

- granular delegation of permissions

[1] Note: The official name of the product is: NetIQ® Directory Resource Administrator 10.2.3. The released product can be uniquely identified as Directory Resource Administrator 10.2.3.0 or Directory Resource Administrator 10.2.3. The product name may also be abbreviated as DRA 10.2.3 or simply DRA, or the TOE. For the purpose of this certification, and the associated documentation, all of the above references are equivalent.

- robust change management policies
- simplified workflow automation

In addition, DRA reduces down time and operational risks to Active Directory that may be caused by malicious or accidental changes.

Key benefits of DRA include:

- Policy and regulation compliance

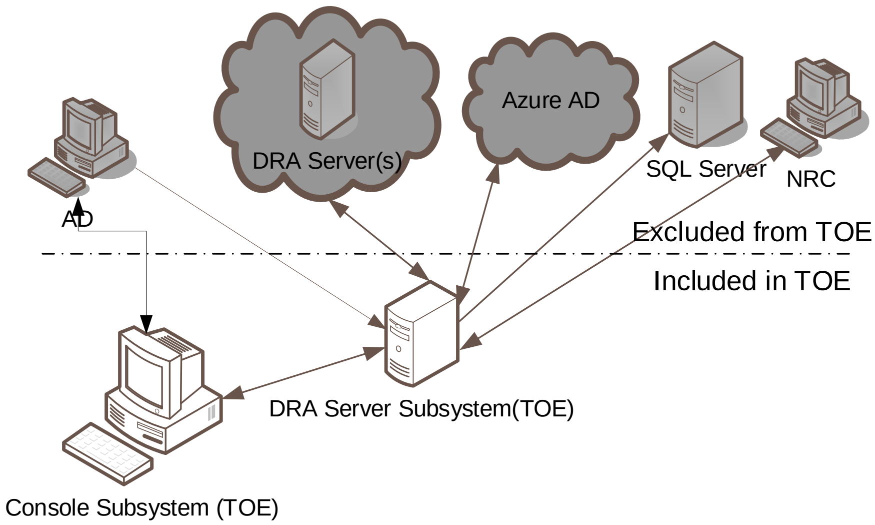
Provides for the assessment, operation, and control of systems and resources in accordance with security standards, best practices, and regulatory requirements and provides logging and auditing capabilities that help demonstrate compliance.

- Operational integrity

Prevents malicious or incorrect changes that affect the performance and availability of systems and services by providing granular access control for administrators and managing access to systems and resources.

- Process enforcement

Maintains the integrity of key change management processes that help you improve productivity, reduce errors, save time, and increase administration efficiency.



ARC document,

FTP_ITC.1 i

Figure 1: A Typical Directory Resource Administrator Deployment

The NetIQ® Directory Resource Administrator Security Target (Figure 1[2] above) consists of the following components:

- Console Subsystem (which provides an Interface GUI / UI and is included in TOE)

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

- DRA Server Subsystem (which provides a DRA Server Interface and is included in TOE)

The TOE also provides the following roles

- Administrator
- Assistant Administrator
- Administrators from Managed Domains

Additional roles / powers can be defined or added to extend the user roles. A list of these can be found in Appendix A.

1.3.2. TOE Components:

For the purpose of this certification, we will include:

The Console Subsystem which includes the following functionality:

- *Delegation and Configuration Console* – Provides a mechanism to securely delegate administrative tasks in the managed domain, set policies and automation triggers, and configure the Administration server.
- *Directory and Resource Reporting* **–** Provides a mechanism to view and print administration activity reports. This enables auditing of your enterprise security and track administration activities.
- *Web Console* – Part Provides a mechanism for Administrators to view configurations in the TOE.

The DRA Server Subsystem which provides audit, authentication, authorization, management and communications functionality.

1.3.3. Logical TOE Boundary (Major Security Features of the TOE):

The TSF provides the following security functions:

- Security Audit
- User Data Protection
- Cryptographic Support
- Identification and Authentication
- Security Management
- Windows Management Administrative Proxy Functions
- Trusted Channel/Path

The TOE can be set up to produce audit reports for events. The TOE reporting capabilities are completely configurable and can even define rules to take automatic responses.

1.3.3.1. Security Audit

The TOE provides a capability to audit changes to the Active Directory made through the NetIQ Directory Resource Administrator application. As well as generating audit logs for regular events, the TOE generates audit records for security relevant events. All audit logs are stored. The TOE allows authorized users (administrators) to view these logs.

If a security event occurs, the TOE blocks the source of the event but also logs it. Logs can be reviewed and analyzed. From this, the administrator can formulate a response for these events.

1.3.3.2. User Data Protection

The TOE implements multiple levels of access as well as functions to enforce them. In addition, the transactions are authenticated, and exportable. The TOE can also be configured to control where functionality can be accessed.

1.3.3.3. Cryptographic Support

The TOE leverages encryption as provided by the Operating Environment in the default communication products.

1.3.3.4. Identification and Authentication

Users of the TOE depend on the IT Environment to handle access authentication, however, all errors and transactions are logged by the TOE. In addition, the TOE has multiple privileges for individuals or groups of individuals. The TOE depends on the IT Environment for protection of passwords and service credentials, as well as for user authentication, identification, subject binding[3].

1.3.3.5. 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 individual access.

1.3.3.6. Windows Management Administrative Proxy Functions

The TOE also provides additional functions. The TOE will provide authorized users with the ability to collect data, and generate reports in a manner suitable for the user to interpret. The TOE will generate alarms using various notification mechanisms. The TOE will react if the storage capacity has been reached.

1.3.3.7. Trusted Channel/Path

The TOE establishes trusted channels for communications between itself and the LDAP server. There is also a trusted path between the Console and the DRA Server.

1.3.4. TOE Type:

For the purpose of this security target the TOE Type is a **W**indows **M**anagement **A**dministrative **P**roxy (WMAP). The WMAP consists of the following functions:

WMAP_ADM_EXT The TOE will provide authorized users with the ability to collect data, and generate reports in a manner suitable for the user to interpret. As part of this it provides the following management mechanisms:

- a mechanism whereby administrators can delegate to authorized users the capability to issue administrative commands and changes.

[3] (tying users to actions)

- a mechanism whereby administrators can delegate to authorized users a group or set of abilities.

WMAP_ALR_EXT The TOE will generate an alarm for operations and events that are performed using one or more of the following notification mechanisms:

- Display alarm information to the administrator console
- Execute a command
- Execute a script

WMAP_STG_EXT The TOE will react if the storage capacity has been reached.

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

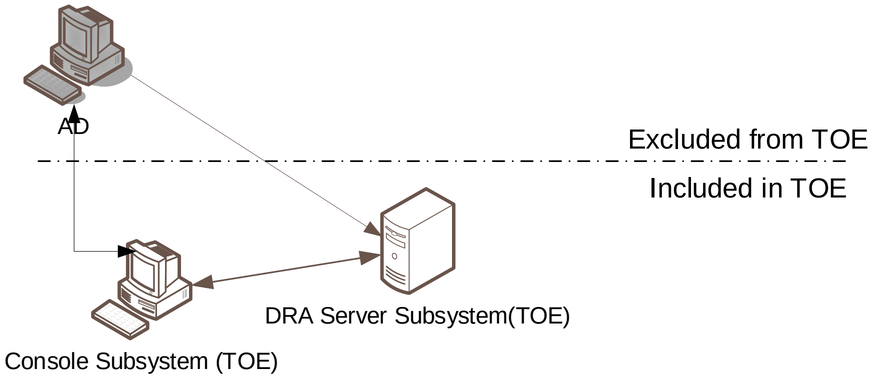


Figure 2: NetIQ Directory Resource Administrator

Note: For the purpose of this evaluation all operating systems and the hardware (or emulations in a virtual machine) are not evaluated but are required for testing DRA. They constitute the operational environment of DRA.

DRA requires the following system configurations for testing:

1.3.5.1. DRA Server Subsystem:

- Windows Server 2016
- The DRA server recommends the following hardware or equivalent emulated in a virtual machine.
- The minimum requirements are listed below.

Component	CPU	Memory	Storage
DRA Administration Server	8 CPU (x64)/cores 2.0 GHz	16 GB	120 GB
DRA Reporting	4 CPU (x64)/cores 2.0 GHz	16 GB	100 GB

DRA Workflow Server	4 CPU (x64)/cores 2.0 GHz	16 GB	100 GB

1.3.5.2. Console Subsystem:

- Windows Server 2016, Microsoft Edge with support for Google Chrome, Mozilla Firefox
- The Console Subsystem requires the following configuration:

Component	**CPU**	**Memory**	**Storage**
Console	2 CPU (x64)/cores 2.0 GHz	8 GB	100 GB

Note: While the physical environment is specified it can be an equivalent environment emulated in a virtual machine.

1.3.6. Excluded Items:

This environment component is not part of the TOE; but is required to demonstrate TOE functionality.

Component	**Operating Systems**
Active Directory	Microsoft Server 2016 or later

1.3.6.1. Web Browser Requirements

The Web Browser is not included in the TOE. The browser used with the Console Subsystem will be evaluated with Microsoft Edge 95.0.1020.44 or later. The following browsers are also supported but are not tested in this evaluation:

Supported Browsers
Microsoft Internet Explorer
Google Chrome
Mozilla Firefox

1.3.7. Evaluated Configuration:

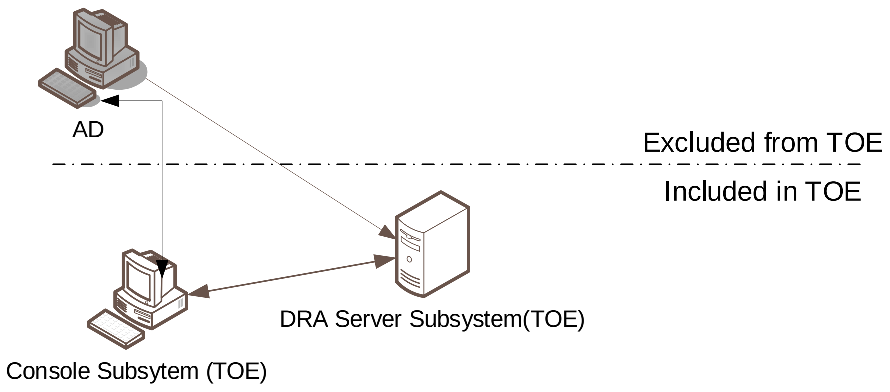


Figure 3: NetIQ Directory Resource Administrator Evaluated Configuration

1.3.8. Physical Scope of TOE

The NetIQ Directory Resource Administrator is a software only TOE. The TOE physical boundary consists of the Console Subsystem and the DRA 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 DC server is not included in the TOE.

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

- Windows Server 2016
- The Console Subsystem will be evaluated with Microsoft Edge 95.0.1020.44 or later.

The DRA Server Subsystem will be evaluated in the consolidated configuration with the following operating systems:

- Windows Server 2016

Further details for installation, administrative, and user guidance can be found in the following documentation:

NetIQ Directory and Resource Administrator Installation Guide November 2023

- NetIQ Directory and Resource Administrator
  - User Guide
  - November 2023

- NetIQ Directory and Resource Administrator
  - Administrator Guide

  - November 2023

- NetIQ® DRA ™ 10.2.3 AGD
  - Operation User Guidance and Preparative Procedures, v2.6, March 27, 2024

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. Excluded Features

The following features are excluded from the evaluation:

CLI
REST API
Email alarm
Power shell
ADSI Provider
DRA Reporting Center Setup (NRC)
SSH

1.6. Acronyms:

AD	Active Directory
CC	Common Criteria
D&C	DRA Delegation and Configuration
DCOM	Distributed Component Object Model
AES	Advanced Encryption Standard
DRA	Directory Resource Administrator
DRA AG	DRA Administrator Guide
DRA IG	DRA Installation Guide
DRA UG	DRA User Guide
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
NetIQ DRA	NetIQ Directory Resource Administrator
NIST	National Institute of Standards and Technology
NRC	NetIQ Reporting Center
OS	Operating system
PP	Protection Profile
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TRACE	Security Manager Log Archive Hook
TSF	TOE Security Functions
TSS	TOE Summary Specification
WMAP	**W**indows **M**anagement **A**dminstrative **P**roxy

1.7. 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)

The TOE is conformant to Common Criteria Version 3.1 Revision 5, April 2017 CC Part 2 extended and CC Part 3 conformant.

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 5 (April 2017). The ST does not claim conformance to any functional package. The TOE EAL2 assurance package is augmented with ALC_FLR.3.

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 who are not 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 DRA Server Subsystem in the local Trace Datastore.
- Configuration information stored on the DRA Server Subsystem and Console Subsystem.
- Data in transit from / to the DRA Server Subsystem, 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.

3.1.2. Subjects:

3.1.2.1. Administrator:

Members of this group manage all objects, define the security model policy, as well as configure and start the Administration server.

3.1.2.2. Assistant Administrators:

Assistant Administrators are users that are afforded a subset of privileges via the DRA Admin.

3.1.2.3. Administrators from Managed Domains:

Members of this group manage accounts, groups, contacts, and resources in a domain where the Member is an Administrator.

3.1.3. Attacker:

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 Active Directory (AD) and create / modify / delete accounts
- delete the entire Data in the Primary Server's Trace Datastore
- view the contents of the AD

3.2. Organisational Security Polices

There are no OSPs for this ST.

3.3. Assumptions

3.3.1. 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.

A.CRYPTO The operational environment provides cryptography for the protection of communications.

3.3.2. Physical Assumptions

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

3.3.3. 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.

3.3.4. 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.

3.4. Threats

T.ADMIN_ERROR An authorized administrator may incorrectly install or configure the TOE resulting in the exposure of data, applications, or capabilities. Improper installation can also affect the security mechanisms in the product for example access control and audit functions.

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 integrity of the TOE or assets the TOE controls through denying services provided by the TOE by halting the execution of the entire TOE or one of its 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 via the TOE that enable additional privileges as specified in Appendix A. These privileges may not have been authorized via appropriate channels.

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

T.MAL_ACT A vulnerability in the IT system, on which the TOE is present, may allow for malicious activity, such as the introduction of malware (i.e. Trojan horses and viruses) by either an authorized entity or a vulnerability in the IT system. This may in turn lead to the compromise of the TOE.

T.MIS_NORULE An unauthorized user, performing an unauthorized activity, indicative of misuse, may occur on an IT System the TOE is installed on. If no event rules are specified in the TOE to cover the action, then the TOE may not issue an alert or log entry.

T.SC_MISCFG An administrator may improperly define the security configuration settings in the IT System the TOE is operating within. The lack of proper IT system configuration could make the TOE security features, such as access control or audit features, 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.SENSDATA	An unauthorized user can observe or modify data in transit between TOE components which causes a security exposure.

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.TOE_PROTECTION The TOE must protect itself and its assets from external interference or tampering.

O.DRA_AUTH The TOE must ensure that only authorized administrators are able to access functionality.

O.DRA_AUDIT The TOE must collect and store transactional information that can be used to audit changes to the Active Directory.

O.DRA_TDS The TOE must protect entries in the Log Archive Trace Datastore.

O.DRA_REP The TOE must provide identification for source and target objects.

O.DRA_ACPOL The TOE must provide an access policy.

O.DRA_DATVAL The TOE must provide audit data that is tamper evident.

4.2. Security Objectives for the Non-IT Environment

OE.ADMIN Those responsible for the TOE must ensure that the TOE is administered in a manner consistent with IT security administration.

OE.CONFIG Those responsible for the TOE must ensure that the TOE is configured in a manner consistent with IT security and according to the MS Configuration Guidance Documentation.

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.AVAILABILITY The IT environment is responsible for providing protection against loss of systems or services.

OE.CONNECT The IT environment will provide network connectivity between components.

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, disclosure, or tampering.

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; and,
- PP Claims.

4.4.1. 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.

4.4.2. Security Objectives Rationale for the TOE and Environment

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

		O.ADMIN_ROLE	O.MANAGE	O.OFLOWS	O.RESPONSE	O.DRA_AUTH	O.DRA_AUDIT	O.DRA_TDS	O.DRA_REP	O.DRA_ACPOL	O.DRA_DATVAL	O.TOE_PROTECTION	OE.ADMIN_ROLE	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TIME	OE.TOE_PROTECTION
Threats	T.ADMIN_ERROR		X														
	T.MASQERADE	X				X	X	X	X	X	X		X	X	X		
	T.NO_HALT	X			X												
	T.PRIV	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				X							
	T.SC_MALRUN	X					X	X	X		X						
	T.SENSDATA																X

Table 1: Threats to Objectives correspondence

4.4.2.1. T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in the exposure of data, applications, or capabilities. Improper installation can also affect the security mechanisms in the product for example access control and audit functions.

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.

4.4.2.2. 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.DRA_AUTH: The TOE counters this threat by only allowing users to execute functions based on their credentials or group memberships.

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

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

O.DRA_TDS: The TOE protects entries in the log facility by using cascaded hashes and not enabling modification of existing records.

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

O.DRA_ACPOL: The TOE counters this threat by use of an access policy that restricts authorized entities to specific activities.

O.DRA_DATVAL: The TOE counters this threat by providing audit data that is tamper evident by applying cascaded hashes.

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.

4.4.2.3. T.NO_HALT:

An unauthorized entity may attempt to compromise the integrity of the TOE or assets the TOE controls through denying services provided by the TOE by halting the execution of the entire TOE or one of its 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.

4.4.2.4. 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.

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

4.4.2.5. T.MAL_INTENT:

An authorized user could initiate changes via the TOE that enable additional privileges as specified in Appendix A. These privileges may not have been authorized via appropriate channels.

This Threat is countered by ensuring that:

OE.TIME: The IT Environment counters this by providing timestamps that can be used in the audit.

OE.TOE_PROTECTION: The IT Environment counters this threat by protecting assets from external interference, disclosure, or tampering.

O.RESPONSE: The TOE counters this event by responding appropriately to trigger events.

O.DRA_AUDIT: The TOE counters this event by collecting and storing transactional information that can be used to audit changes to the AD.

O.DRA_TDS: The TOE protects entries in the log facility by using cascaded hashes.

O.DRA_ACPOL: The TOE counters this threat by providing an access policy.

4.4.2.6. 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:

O.TOE_PROTECTION: The TOE counters this threat by using event triggers to protect itself and its assets from external interference or tampering.

OE.TOE_PROTECTION: The IT environment will protect the TOE and its assets from external interference, disclosure, or tampering.

4.4.2.7. T. MAL_ACT

A vulnerability in the IT system, on which the TOE is present, may allow malicious activity by either an authorized entity or unauthorized entity. This may in turn lead to the compromise of the TOE.

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.DRA_AUDIT: The TOE counters this threat by collecting and storing transactional information that can be used to audit changes to the AD.

O.DRA_DATVAL: The TOE counters this threat by providing audit data that is tamper evident.

OE.TIME: The IT environment counters this threat by providing a reliable timestamp.

OE.TOE_PROTECTION The IT Environment counters this threat by protecting assets from external interference, disclosure, or tampering.

4.4.2.8. T. MIS_NORULE

An unauthorized user, performing an unauthorized activity, indicative of misuse, may occur on an IT System the TOE is installed on. If no event rules are specified in the TOE to cover the action, then the TOE may not issue an alert or log entry.

This Threat is countered by ensuring that:

O.DRA_AUDIT: The TOE collects and stores transactional information that can be used to audit changes to the AD.

O.DRA_ACPOL: The TOE protects against this threat by providing access policies.

4.4.2.9. T. SC_MISCFG

An administrator may improperly define the security configuration settings in the IT System the TOE is operating within. The lack of proper IT system configuration could make the TOE security features, such as access control or audit features, ineffective.

This Threat is countered by ensuring that:

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

O.DRA_ACPOL: The TOE counters this threat by providing an access policy.

O.OFLOWS: The TOE counters this threat by requiring the TOE handle data storage overflows.

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

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

O.DRA_TDS: The TOE protect entries in the log facility by using cascaded hashes and not enabling modification of existing records.

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

O.DRA_DATVAL: The TOE counters this threat by providing audit data that is tamper evident by applying cascaded hashes.

4.4.2.11. T.SENSDATA

An entity could observe or modify data in transit between components of the TOE which causes a security exposure to the TOE.

This threat is countered by ensuring that:

OE.TOE_PROTECTION The IT Environment counters this threat by protecting assets from external disclosure or tampering.

4.5. Security Objectives Rationale for Environment Assumptions and OSPs

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.ADMIN	OE.AVAILABILITY	OE.CONFIG	OE.CONNECT	OE.INSTAL	OE.CREDEN	OE.PERSON	OE.PHYCAL	OE.INTROP	OE.TOE_PROTECTION
Intended usage assumptions	A.ACCESS									x	
	A.ASCOPE									x	
	A.DYNMIC							x		x	
	A.CRYPTO										X
Physical assumptions	A.LOCATE								x		
Personnel assumptions	A.MANAGE							x			
	A.NOEVIL					x	x				
Connectivity Assumptions	A.AVAIL	x	x								
	A.CONFIG			x							
	A.NETCON				x						

Table 2: Complete coverage – environmental assumptions and organisational security policy

4.5.1. 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.

4.5.2. 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.

4.5.3. 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.

4.5.4. 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 objective provides for the physical protection of the TOE.

4.5.5. 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.

4.5.6. 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

4.5.7. A.AVAIL

The TOE will be installed in an IT environment that provides the systems, networks, and all components.

This Assumption is satisfied by ensuring that:

OE.ADMIN: The OE.ADMIN objective ensures that only Administrators can access the management functions for the TOE.

OE.AVAILABILITY: The OE.AVAILABILITY objective ensures that the system is fully available and fully redundant.

4.5.8. A.CONFIG

The TOE environment will be properly configured to allow for proper usage of the application.

This Assumption is satisfied by ensuring that:

OE.CONFIG: The OE.CONFIG objective ensures that the system is configured in a manner consistent with IT security and according to the MS Configuration Guidance Documentation.

.

4.5.9. A.CRYPTO

The environment provides crypto for use in protection of TOE communications.

This Assumption is satisfied by ensuring that:

OE.TOE_PROTECTION: The OE.TOE_PROTECTION objective meets the A.CRYPTO assumption.

4.5.10. A.NETCON

The TOE will be installed in an IT environment that allows for communications between the components.

This Assumption is satisfied by ensuring that:

OE.CONNECT: The OE.CONNECT objective addresses A.NETCON.

4.6. 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.DRA_ACPOL	O.DRA_AUDIT	O.DRA_AUTH	O.DRA_DATVAL	O.DRA_REP	O.DRA_TDS	O.MANAGE	O.OFLOWS	O.RESPONSE	OE.TOE_PRTOTECTION	O.TOE_PROTECTION
FAU_ARP.1										X		
FAU_GEN.1			X				X					X
FAU_SAA.1					X					X		
FAU_SAR.1			X									

	O.ADMIN_ROLE	O.DRA_ACPOL	O.DRA_AUDIT	O.DRA_AUTH	O.DRA_DATVAL	O.DRA_REP	O.DRA_TDS	O.MANAGE	O.OFLOWS	O.RESPONSE	OE.TOE_PRTOTECTION	O.TOE_PROTECTION
FAU_STG.1			X				X		X			X
FCS_CKM.1											X	
FCS_CKM.4											X	
FCS_COP.1											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				
FMT_MTD.1			X			X		X				
FMT_SMF.1								X				
FMT_SMR.1	X											
FPT_ITC.1												X
FPT_TRP.1												X
WMAP_ADM_EXT.1	X							X				
WMAP_ALR_EXT.1							X		X	X		
WMAP_STG_EXT.1							X		X			

Table 3: Objective to Requirement Correspondence

4.6.1. 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 as an “authorized administrator”.

WMAP_ADM_EXT.1: The TOE provides authorized administrators with the ability to delegate to assistants the ability to interactively modify resources using the UI.

4.6.2. O.DRA_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, Assistant Administrators or Administrators from Managed Domains.

FDP_ACF.1: The TOE can be configured to enforce access control to objects.

4.6.3. O.DRA_AUDIT

The TOE must collect and store 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 outside of the DRA system.

FMT_MOF.1: The TOE restricts the ability to enable and disable audit functions to Administrators, Assistant Administrators or Administrators from Managed Domains.

FMT_MTD.1: The TOE restricts the ability to *modify* the audit configuration to Administrators, Assistant Administrators or Administrators from Managed Domains.

4.6.4. O.DRA_AUTH

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

This TOE Security Objective is satisfied by ensuring that:

FDP_ACC.1: The TOE can be configured to limit access to Administrators and Assistant Administrators.

FMT_MSA.1: The TOE will enforce access controls that restrict the ability to alter security attributes powers or groups of powers to Administrators and Assistant Administrators.

4.6.5. O.DRA_DATVAL

This TOE Security Objective is satisfied by ensuring that:

FAU_SAA.1: The TOE can provide Analysis of the Audit data to determine if the data was modified.

4.6.6. O.DRA_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, Assistant Administrators or Administrators from Managed Domains.

FMT_MTD.1: The TOE can be configured to limit access to the audit configuration to Administrators, Assistant Administrators or Administrators from Managed Domains.

4.6.7. O.DRA_TDS

The TOE must protect entries in the Log Archive Trace Datastore.

This TOE Security Objective is satisfied by ensuring that:

FAU_GEN.1: The TOE provides the ability to generate an audit record.

FAU_STG.1: The TOE provides the ability to protect the audit record outside of the DRA system.

WMAP_STG_EXT.1: The TOE provides the ability to abort an attempted command and display a message if the storage capacity has been reached.

WMAP_ALR_EXT.1: The TOE provides the ability to define groups of rules as well as rules for the generation of events using one or more notification mechanisms.

4.6.8. 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 WMAP settings to authorized administrators.

FMT_MSA.1 The TOE enforces the access control policy and restricts the ability to modify, add, or delete the security roles to Administrators, Assistant Administrators or Administrators from Managed Domains.

FMT_MSA.3 The TOE enforces the access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

The TOE also allows Administrators, Assistant admin groups, and Administrators from Managed Domains to specify alternative initial values that override the default values when an object or information is created.

FMT_MTD.1: The TOE restricts the ability to query collected data and generated reports to authorized users.

FMT_SMF.1: The TOE provides authorized administrators with the ability to manage WMAP settings and review collected data.

WMAP_ADM_EXT.1: The TOE provides authorized administrators with the ability to delegate to assistants the ability to interactively modify resources using the UI.

4.6.9. 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 provides audit information for all transactions.

WMAP_ALR_EXT.1: The TOE generates an event failure alarm (message) when audit storage space is exceeded.

WMAP_STG_EXT.1: The TOE stops transactions from occurring when audit storage space is exceeded. Failed attempts due to storage generate messages.

4.6.10. O. RESPONSE

The TOE must respond appropriately to trigger events.

This TOE Security Objective is satisfied by ensuring that:

FAU_ARP.1: The TOE allows access to functions based on explicit privileges (powers) provided to an assistant admin. 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 Repository on the DRA Server.

FAU_SAA.1: The TOE can be configured to look at an events occurrence and generate an alarm.

WMAP_ALR_EXT.1: The TOE generates alarms that notify authorized administrators or assistants using the console, using email, using SMTP, and/or executing a command in a configured script. Note that alarms may be generated in response to administratively-configured processing rules.

4.6.11. O.TOE_PROTECTION

The TOE must protect itself and its assets from external interference or tampering. This TOE Security Objective is satisfied by ensuring that:

FAU_GEN.1: The TOE provides the ability to generate an audit record.

FAU_STG.1: The TOE provides the ability to protect the audit record outside of the DRA system.

FDP_ACC.1: The TOE provides the ability to limit access to only Administrative users with defined group associations.

FTP_ITC.1 The TOE makes use of LDAPS to protect the channel between parts of the TOE and trusted IT products.

FTP_TRP.1 The TOE makes use of TLS v1.2 to protect the paths from external entities into the TOE.

4.7. Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2. 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 product was augmented to comply with ALC_FLR.3 in order to document and address requirements for remediation and reporting of faults that may be discovered in the product after release.

4.7.1. 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_SAA.1	FAU_GEN.1	Included
FAU_GEN.1	FPT_STM.1	OE.TIME
FAU_SAR.1	FAU_GEN.1	Included
FAU_STG.1	FAU_GEN.1	Included
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	Included
FCS_CKM.4	FCS_CKM.1	Included
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	Included
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Included 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 Included
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	OE.USER_IDENTIFICATION
FTP_ITC.1	none	none

SFR	Dependencies	Met By
FTP_TRP.1	none	none
WMAP_ADM_EXT.1	None	None
WMAP_ALR_EXT.1	None	None
WMAP_STG_EXT.1	WMAP_ALR_EXT.1	Included

Table 4: Requirement Dependency

4.8. Explicitly Stated Requirements Rationale

A class of WMAP requirements was created to specifically address the administrative proxy capability of a WMAP. 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 WMAP's including capabilities for making, reviewing, and managing administrative changes.

4.9. 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 and assurance 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 5: Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

	Security Audit	User Data Protection	Identification and Authentication	Security Management	Windows Management Administrative Proxy Functions	Trusted Path/Channels	Cryptogrphic Suport
FIA_ATD.1			X				
FMT_MOF.1				X			
FMT_MTD.1				X			
FMT_SMF.1				X			
FMT_SMR.1			X	X			
FMT_MSA.1				X			
FMT_MSA.3				X			
FAU_ARP.1	X						
FAU_GEN.1	X						
FAU_SAA.1	X						
FAU_SAR.1	X						
FAU_STG.1	X						
FCS_CKM.1							X
FCS_CKM.4							X
FCS_COP.1							X
FDP_ACC.1		X					
FDP_ACF.1		X					
WMAP_ADM_EXT.1		X			X		
WMAP_ALR_EXT.1	X				X		
WMAP_STG_EXT.1	X				X		

FTP_ITC.1						X	
FTP_TRP.1						X	

Table 5: Security Functions vs. Requirements Mapping

5. Extended Components Definition (ASE_ECD)

This chapter defines a new class required by Windows Management Adminstrative Proxy Devices. The class consists of the following family members WMAP_ADM_EXT, WMAP_ALR_EXT, and WMAP_STG_EXT. This class is defined because the Common Criteria (Parts 2) 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.

Class	Component
WMAP: Windows Management Administrative Proxy	WMAP_ADM_EXT.1: Data Review
	WMAP_ALR_EXT.1: Data Alarms
	WMAP_STG_EXT.1: Data Loss Prevention

Table 6: Extended Functional Components

5.1. Definition for WMAP_ADM_EXT.1

For the TOE described in this ST it was necessary to provide authorized entities with a mechanism to read and perform administrative functions as specified in Appendix A or by being an Administrator, Administrative Assistant or User of the program. This mechanism is covered by the WMAP_ADM_EXT family and contains the components as shown in Figure 5 below.

Management: none

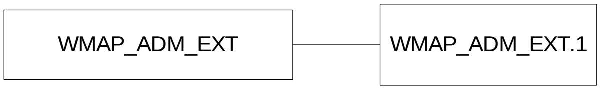


Figure 4: WMAP_ADM_EXT Component Leveling

5.1.1. Data Review (WMAP_ADM_EXT.1)

Hierarchical to: no other component
Dependencies: none

WMAP_ADM_EXT.1.1 The TSF shall provide authorized users with the capability to delegate to authorized users the capability to issue administrative commands and make changes to users.

WMAP_ADM_EXT.1.2 The TSF shall provide authorized users a group or set of abilities that can be delegated to users.

5.2. Definition for WMAP_ALR_EXT.1

For the TOE described in this ST it was necessary to define a new family (WMAP_ALR_EXT) that addresses what happens by enabling the creation of rules which define the generation of alerts, messages, and the disposition of events. This family contains the component as shown in the figure below.

Management: none

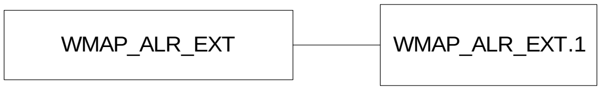


Figure 5: WMAP_ALR_EXT Component Leveling

5.2.1. Data Alarms (WMAP_ALR_EXT.1)

Hierarchical to: no other components
Dependencies: none

WMAP_ALR_EXT.1.1 The TSF shall provide rules, or groups of rules for events that [**selection, any of following:** display information on the administrator console, execute a command, execute a script] as (a/an) notification mechanism(s).

5.3. Definition WMAP_STG_EXT.1

For the TOE described in this ST it is necessary to define a new family (WMAP_STG_EXT) that address what happens when the system runs out of storage capacity. This family contains the components as shown in the figure below.

Management: none

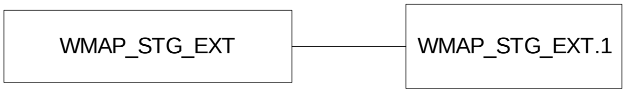


Figure 6: WMAP_STG_EXT Component Leveling

5.3.1. Data Loss Prevention (WMAP_STG_EXT.1)

Hierarchical to: no other components
Dependencies: WMAP_ALR_EXT.1

WMAP_STG_EXT.1.1 This TSF shall [selection, any of the following: block the collection of System data, block the execution of all TOE transactions, generate a message] if the storage capacity has been reached.

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
FCS: Cryptographic Support	**FCS_CKM.1: Cryptographic key generation**
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1: 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_ATD.1: User attribute definition**
FMT: Security Management	**FMT_MOF.1: Management of security functions behavior**
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.3: Static attribute initialization
FTP: Trusted Path/channels	**FTP_ITC.1: Inter-TSF trusted channel**
	FTP_TRP.1: Trusted path
WMAP: Windows Management Administrative Proxy	**WMAP_ADM_EXT.1: Data Review**
	WMAP_ALR_EXT.1: Data Alarms
	WMAP_STG_EXT.1: Data Loss Prevention

Table 7: TOE Security Functional Requirements

6.1.1. Security Audit (FAU)

6.1.1.1. Security alarms (FAU_ARP.1)

FAU_ARP.1.1 The TSF shall [**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) **[All auditable events listed in Table in FAU_GEN.1.2**].

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, [**All auditable events listed in Table below**].

FAU_ARP.1	The TOE allows access to functions based on explicit privileges (powers) provided to an assistant admin. 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 Repository on the DRA Server.
FAU_GEN.1	The TOE generates audit data for ALL transactions attempted and executed through the Console Subsystem. Audit data may include information about the operation that was performed including: ▪ the type of object ▪ who performed that operation (name, GUID, one point path of this account) ▪ the name of the target object, GUID of the target object, one point path of the target object ▪ Domain Controller used ▪ what properties were changed (before and after values), ▪ policy details & trigger details ▪ UTC date and time, transaction id, and return code.
FAU_SAA.1	The TOE provides functions to analyze audit events (all transactions attempted and executed) and trends as part of the Console Subsystem.
FAU_SAR.1	The TOE provides event audit review for all attempted and executed jobs as part of the Console Subsystem via the ability to read audit records from the audit log.

FAU_STG.1	The TOE stores audit event information for all attempted and executed changes in the DRA Server Subsystem.
FDP_ACC.1	The TOE generate audit information regarding changes to access control.
FDP_ACF.1	The TOE shall enforce access control to Audit records (containing all attempted and executed transactions) and prevent unauthorized deletion or modification of audit records. Audit data may include includes information about the operation that was performed including: ▪ the type of object ▪ who performed that operation (name, GUID, one point path of this account) ▪ the name of the target object, GUID of the target object, one point path of the target object ▪ Domain Controller used ▪ what properties were changed (before and after values), ▪ policy details & trigger details ▪ UTC date and time, transaction id, and return code. Details of privileges required for are defined in Appendix A
FMT_MOF.1	The TOE shall generate audit information regarding enabling / disabling /roles or the creation of groups of roles[4].
FMT_MSA.1	The TOE shall generate audit information regarding changes to privileges. The TOE shall also generate audit information regarding changes to default privileges.
FMT_MSA.3	The TOE shall provide audit records detailing changes from restrictive to permissive as well as changes from initial (default) values.to new values.
FMT_MTD.1	The TOE shall generate audit information for changes to configuration data and roles.

[4] For an explicit list of Roles please refer to Appendix A.

FMT_SMF.1	The TOE shall generate audit information for addition of users, changes to user, or addition of role groups. The TOE will also generate audit information for the use of management functions.
FMT_SMR.1	The TOE shall generate audit information for changes to the users associated with the roles (Administrator, Assistant administrators, or Users). The TOE will also generate audit information for actions performed by Administrators, Assistant administrators, and users.
WMAP_ADM_EXT.1	The TOE provides the ability to audit delegations to authorized users and groups of users.
WMAP_ALR_EXT.1	The TOE provides the ability to generate audit information for messages or alarms.
WMAP_STG_EXT.1	The TOE provides the ability to block transactions when audit storage capacity has been reached.

Table 8: Auditable Events

6.1.1.3. Security audit 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 [**authorized users**] 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 unauthorised deletion.

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

6.1.2. Cryptographic Support (FCS)

6.1.2.1. FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [See Table]

Algorithm	Key Mode and Size	Standard
RSA	2048 bits	FIPS 186-4
AES GCM	128, 256 bits	FIPS 197, SP 800-38D
AES CBC	128, 256 bits	FIPS 197, SP 800-38A
SHS	256, 384 bits	FIPS 198

6.1.2.2. FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [memory overwrite] that meets the following: [no standards].

6.1.2.3. FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [TLS 1.2, LDAPS] in accordance with a specified cryptographic algorithm [See table].

Algorithm	Key Mode and Size	Standard
RSA	2048 bits	FIPS 186-4
AES GCM	128, 256 bits	FIPS 197, SP 800-38D
AES CBC	128, 256 bits	FIPS 197, SP 800-38A
SHS	256, 384 bits	FIPS 198

6.1.3. User Data Protection (FDP)

6.1.3.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [**access control policy**] on [**all users with defined 'powers' as specified in Appendix A**]

6.1.3.2. Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**access control policy**] to objects based on the following: [**membership to Administrators, Assistant Administrators or Administrators from Managed Domains and functions as listed in Appendix A**].

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** e**xecution of functionality based on group membership and / or roles**[5]].

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 or member of groups with lack of explicitly granted powers as specified in Appendix A**].

6.1.4. Identification and Authentication (FIA)

6.1.4.1. User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~: **roles**: **[authorizations]**.

6.1.5. Security Management (FMT)

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

FMT_MOF.1.1 The TSF shall restrict the ability to [*enable and disable*] the functions [**Related to: Security Audit, User Data Protection, Identification and Authentication, Security Management, Windows Management Administrative Proxy**] to [**Administrators, Assistant Administrators or Administrators from Managed Domains**].

6.1.5.2. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**access control policy**] to restrict the ability to [*modify, **add**, or delete*] the security attributes [**powers and groups of powers**] to [**Administrators, Assistant Administrators or Administrators from Managed Domains**].

[5] As described in Appendix A

6.1.5.3. Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**access control policy**] 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,or administrator groups**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.4. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify*] the [**configuration data, report formats**] to [**Administrators, members of the Assistant administrators groups with the appropriate powers**[6]**, or Administrators from Managed Domains**].

6.1.5.5. 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 Assistant administrators by the addition of Roles in Appendix A, Modify the behavior of operational events**[7]**, and Query collected transaction log and generate associated report**].

6.1.5.6. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrators, Assistant Administrators or Administrators from Managed Domains**].

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

6.1.6. Windows Management Administrative Proxy (WMAP)

6.1.6.1. Data Review (WMAP_ADM_EXT.1)

WMAP_ADM_EXT.1.1 The TSF shall provide authorized users with the capability to delegate to authorized users the capability to issue administrative commands and make changes to users.

WMAP_ADM_EXT.1.2 The TSF shall provide authorized users a group or set of abilities that can be delegated to users.

[6] Powers are the list of privileges / group of privileges

[7] Operational events are included in Appendix A and include creation, modification, and deletion of accounts.

6.1.6.2. Data Alarms (WMAP_ALR_EXT.1)

WMAP_ALR_EXT.1.1 The TSF shall provide rules, or groups of rules for events that [*display information on the administrator console, execute a command, execute a script*] as (a/an) notification mechanism(s).

6.1.6.3. Data Loss Prevention (WMAP_STG_EXT.1)

WMAP _STG.1.1 This TSF shall [*block the collection of System data, block the execution of all TOE transactions, generate a message*] if the storage capacity has been reached.

6.1.7. Trusted channels

6.1.7.1. Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides. assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [authentication].

6.1.8. Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [local, remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [local users, remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication, [protected communications]].

6.2. Security Assurance Requirements

This section defines the assurance requirements for the TOE. The TOE assurance requirements are taken from the CC v3.1 Revision 5, Part 3. The TOE functional security requirements are verified by the specified security assurance requirements. 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
	ALC_FLR.3	Systematic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST 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.

7.1. Security Audit

The NetIQ Directory Resource Administrator provides the ability to audit changes to the Active Directory made through the NetIQ Directory Resource Administrator application. When the 'Assistant Admins' make a change using NetIQ DRA, all changes are logged. In addition the Assistant Admin can only execute commands they are authorized to execute.

The changes are logged in DRA's audit repository. This repository is a check in repository, that is you can write but not update or delete records. In addition, this information can be published to the Windows Event Log.

The TOE generates audit records for Security Relevant events and stores them. The table of the audit events generated by the TOE is provided in Table 8: Auditable Events.

The TOE provides functions to review and analyze audit events (all attempted and executed) and trends and generate reports on the same, as part of the Console Subsystem.

Access to the Audit log is restricted to a search UI, that has been explicitly been authorized for an assistant administrator to use. This privilege is provided by the DRA Administrator.

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

FAU_GEN.1

The TOE generates audit data for ALL transactions attempted and executed through Console Subsystem. Audit data may include:

- information about the operation that was performed including: the type of object
- who performed that operation (name, GUID, one point path of this account)
- the name of the target object, GUID of the target object, one point path of the target object
- Domain Controller used
- what properties were changed (before and after values),
- policy details & trigger details
- UTC date and time, transaction id, and return code.

FAU_SAA.1

The TOE provides functions to analyze audit events (all transactions attempted and executed) and trends as part of the Console Subsystem functionality.

FAU_SAR.1

The TOE provides event audit review for all attempted and executed jobs as part of the Console Subsystem via the ability to read audit records from the audit log.

FAU_STG.1. The TOE stores audit event information for all attempted and executed changes in the DRA Server Subsystem.

FAU.ARP.1 When a potential security violation occurs, the transaction is blocked and a message is posted. The violation is also logged.

7.2. Cryptographic Support

The TOE leverages environment crypto to provide encryption for the trusted channels to the LDAP server. LDAPS protocol is used to provide AES 128 and 256 encrypted links.

The TOE uses cryptography from the bcrypt.dll in the environment (Windows 2016) to establish TLS 1.2 communications for both the Trusted Channel between the DRA Server and the LDAP Server and the Trusted Path between the Console and the DRA Server.

The following algorithms are used.

Algorithm
AES-CBC
AES-GCM
RSA
SHA256, SHA384

FCS_CKM.1 The TOE relies on the environment to generate keys.

FCS_CKM.4 The TOE relies on the environment to destroy keys.

FCS_COP.1 The TOE relies on the environment to produce keys required to protect communications.

7.3. User Data Protection

The NetIQ Directory Resource Administrator enables protection of data by enforcing the list of security attributes belonging to individual roles. These roles are defined in either the Assistant Administrators role or as explicit privileges provided by virtue of membership in the Administrators group.

FDP_ACC.1	The TOE allows access to information by enforcing user privileges as defined in the Assistant Administrator's explicit privileges, or in the Administrator groups.
FDP_ACF.1	The TOE enforces access to functions based on the user privileges as defined in the Assistant Administrator's explicit privileges or in the Administrator groups.
WMAP_ADM_EXT.1	The TOE defines mechanisms for administrators to delegate privileges to individuals and groups of individuals

7.4. Identification and Authentication

The NetIQ Directory Resource Administrator provides user interfaces that administrators may use to define assistants and delegate responsibilities. The DRA GUI application examines the identification and authentication information for individual administrators and assistant administrators. If the user has been successfully identified and authenticated by the IT Environment, and if the user has been successfully identified and authenticated as a member of an administrative system and/or administrative sub group that the TOE recognizes, the DRA GUI provides access to its interfaces according to authorization data. 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 (i.e. membership in an administrative system and/ or assistant administration group) may perform.

The TOE recognizes the following operating system and assistant administrator groups, which each correspond to TOE roles:

- Administrator,
- Assistant Administrator Groups,
- Administrators from Managed Domains

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.
FMT_SMR.1:	The TOE uses the operating system for the definition of different groups prior to allowing access.

7.5. Security Management

The NetIQ Directory Resource Administrator application includes the following components:

- DRA Primary Server
- Console Subsystem

To use the Console Subsystem the authorized administrator operating system account must be a member of one of the following groups:

- Administrators,

- Assistant Administrators Groups,
- Administrators from Managed Domains

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

FMT_MOF.1: The TOE restricts the ability to manage WMAP settings to authorized administrators and authorized assistant administrators.

FMT_MSA.1 The TOE provides the ability to enforce the access control policy to provide the ability to add / delete/ and modify security attributes to Administrators, Assistant administrator groups with the appropriate powers (listed in Appendix A) and Administrators from Managed Domains.

FMT_MSA.3 The TSF provides the ability to modify the initial restrictive access controls. It also enables Administrators, Assistant administrator groups and Administrators from Managed Domains to change default values.

FMT_MTD.1: The TOE restricts the ability to query and modify the collected data and generated reports to authorized users.

FMT_SMF.1: The TSF provides authorized administrators with the ability to manage assistant administrators by adding roles or privileges in Appendix A. In addition it allows for the modification of the behavior of operational events as well, the ability to modify the information that is collected and any associated reports.

FMT_SMR.1: The TSF maintains roles for Administrators, Assistant administrator groups, and Administrators from Managed Domains. It also allows authorized administrators the ability to associate users with roles.

7.6. Windows Management Administrative Proxy

NetIQ DRA is a Windows Management Administrative Proxy. By this we mean that it proxies all changes to the Windows Management. NetIQ DRA also provides a facility that can be used to review all changes. Logging is critical to the success of the product; hence all transactions will be logged. In the event of a log failure the user will be informed that the action did not take place.

The Window Management Administrative Proxy function is designed to satisfy the following security functional requirements:

WMAP_ADM_EXT.1 The TSF shall provide authorized users the capability to delegate to authorized users, or groups of users, the capability to issue administrative commands and changes.

WMAP_ALR_EXT.1 The TSF can generate an alarm using one or more of the following notification mechanisms:

	Display alarm information to the administrator console
	Execute a command
	Execute a script
	in response to one or more of the following rule types:
	Event rules
WMAP_STG_EXT.1	The TSF shall abort the attempted command and display a message if the storage capacity has been reached.

7.7. Trusted Channel

NetIQ DRA establishes trusted channels for communications between itself and other trusted IT products. This satisfies FTP_ITC.1.

There is also a trusted path between the Console and the DRA Server. The Trusted Path function is designed to satisfy the following security functional requirements:

The TOE OE provides the trusted path for TOE Users, using HTTPS/TLS.
The Management and user Interfaces use operating system or environmentally supplied encryption and their associated protocols (TLS 1.2). This satisfies FTP_TRP.1.

The TOE leverages encryption as provided by the Operating Environment for support of secure communications protocols using LDAPS for secure communications between the TOE and the AD. For the LDAPS support in DRA, Active directory LDAPS need to configured.
https://www.miniorange.com/guide-to-setup-ldaps-on-windows-server

Secure Active Directory is defined by a DRA environment that is configured to run using the LDAPS (LDAP over SSL) protocol to encrypt communications between DRA and Active Directory to provide a more secure environment.

DRA uses environment crypto. In Windows 2016, cryptsp.dll v10.0.14393.2457 calls bcrypt.dll v10.0.14393.4046 to provide the algorithms required.

Communications protected by TLS 1.2 use cipher suites which are also configured in the GPO, Manage Transport Layer Security (TLS) in Windows | Microsoft Learn

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Appendix A – DRA Privileges / Roles / Powers list

Power	Power	Power
Create Private Advanced Query	Create Public Advanced Query	Delete Public Advanced Query
Execute Advanced Query	Execute Saved Advanced Query	Modify Public Query
View Advanced Query	Export UI Reports	Generate UI Reports
Modify Clone Exceptions	View Clone Exceptions	Create Computer and Modify All Properties
Delete Computer Account	Delete Computer Account Permanently	Modify All Computer Properties
Modify Computer Dial-in Properties	Modify General Computer Properties	Reset Computer Account
Reset Password for Local Administrator	Start Computer Shutdown	Stop Computer Shutdown
Synchronize Domain Controllers	View All Computer Properties	View Name of Local Administrator
Clone Contact and Modify All Properties	Delete Contact Account	Delete Contact Account Permanently
Create Contact and Modify All Properties	Create Contact and Modify Limited Properties	Enable Email for New Contact
Delete Email for Contact	Enable Email for Cloned Contact	Enable Email for Contact
Modify Exchange Mailbox Email Addresses for Contact	Modify All Contact Properties	Modify Contact Address Properties
Modify Contact Extension Attributes	Modify Contact Name	Modify General Contact Properties
View All Contact Properties	Modify Advanced Exchange Mailbox Properties for Contact	Modify All Exchange Mailbox Properties for Contact
Modify Exchange Mailbox Custom Attributes for Contact	Modify Exchange Mailbox Delivery Restrictions for Contact	Modify Exchange Mailbox ILS Settings for Contact
Modify General Exchange Mailbox Properties for Contact	View All Exchange Mailbox Properties for Contact	Modify the VA1 property of User
Retrieves the VA1 property of User	Execute Custom Tools	Manage Custom Tools

Power	Power	Power
View All Domain Properties	Provide .	Enable / Disable DRA Collectors and Management Reporting Collectors Information
Set Database Configuration Information	View Active Directory Collectors	View DRA Collectors and Management Reporting Collectors information
View Database Configuration Information	Delete Mailbox	Enable/Disable Exchange Mailbox Unified Messaging
Modify All Exchange Mailbox Features	Modify Exchange Mailbox Unified Messaging Properties	View All Exchange Mailbox Features
View Exchange Mailbox Unified Messaging Properties	Clone Exchange Mailbox and Modify All Properties	Clone Exchange Mailbox Only
Create Exchange Mailbox and Modify All Properties	Create Exchange Mailbox Only	Modify All Exchange Properties
Modify General Exchange Mailbox Properties	Move Exchange Mailbox	View All Exchange Mailbox Properties
Modify All Mailbox Rights	Modify Delete Mailbox Storage Rights	Modify Mailbox Associated External Account Rights
Modify Mailbox Change Permissions	Modify Mailbox Full Access Rights	Modify Mailbox Ownership Rights
Modify Mailbox Read Permissions	Modify Mailbox Receive As Rights	Modify Mailbox Send As Rights
View All Mailbox Rights	Modify Advanced Exchange Mailbox Properties	Modify Exchange Custom Attributes
Modify Exchange Mailbox Delivery Options	Modify Exchange Mailbox Delivery Restrictions	Modify Exchange Mailbox Email Addresses
Modify Exchange Mailbox ILS Settings	Modify Exchange Mailbox Storage Limits	Delete Group Account Permanently
Delete Group Account	Modify All Group Properties	Modify General Group Properties
View All Group Properties	Add Cloned Group to ActiveView	Clone Group and Modify All Properties
Add New Group to ActiveView	Create Group and Modify All Properties	Create Group and Modify Limited Properties

Power	Power	Power
Enable Email for New Group	Hide Group Membership in Distribution List	Modify Advanced Exchange Mailbox Properties for Group
Modify All Exchange Mailbox Properties for Group	Modify Exchange Mailbox Custom Attributes for Group	Modify Exchange Mailbox Delivery Restrictions for Group
Modify General Exchange Mailbox Properties for Group	Show Group Membership in Distribution List	View All Exchange Mailbox Group Properties
Delete Email for Group	Enable Email for Group	Modify Exchange Mailbox Email Addresses for Group
View Email Address for Group	Add Computer to Group	Add Contact to Group
Add Group to Group	Add Object to Group	Add User to Group
Modify Group Membership Security	Remove Computer from Group	Remove Contact from Group
Remove Group from Group	Remove Object from Group	Remove User from Group
Modify Group Description	Modify Group Name	Modify Group Type
Create Temporary Group Assignments	Delete Temporary Group Assignments	Modify Temporary Group Assignments
Reset Temporary Group Assignment State	View Temporary Group Assignments	Modify Properties of a Custom Power
View Power Properties	Clone OU and Modify All Properties	Create OU and Modify All Properties
Delete OU	Modify All OU Properties	Modify General OU Properties
Modify OU Name	Move Computer to OU	Move Contact to OU
Move Group to OU	Move Object to OU	Move Organizational Unit to OU
Move Printers to OU	Move User to OU	View All OU Properties
Delete Published Printer Print Job	Delete Published Printer Print Job Submitted by Managed User	Modify All Published Printer Print Job Properties
Modify All Published Printer Print Job Properties Submitted by Managed User	Modify Published Printer Print Job Priority	Pause Published Printer Print Job
Pause Published Printer Print Job Submitted by Managed User	Restart Published Printer Print Job	Restart Published Printer Print Job Submitted by Managed User

Power	Power	Power
Resume Published Printer Print Job	Resume Published Printer Print Job Submitted by Managed User	View All Published Printer Print Job Properties
Modify All Published Printer Properties	Pause Published Printer	Resume Published Printer
View All Published Printer Properties	Delete Computer from Recycle Bin	Delete Contact from Recycle Bin
Delete Group from Recycle Bin	Delete User from Recycle Bin	Restore Computer from Recycle Bin
Restore Contact from Recycle Bin	Restore Group from Recycle Bin	Restore User from Recycle Bin
View All Recycle Bin Objects	Delete Files from Server	Set File Information
Upload Files to Server	Disconnect Any User	Disconnect Managed User
View All Connected User Properties	Modify All Device Properties	Start Device
Stop Device	View All Device Properties	Clear Event Log
Modify All Event Log Properties	View Administration Server Events Only	View All Event Log Properties
Close Any Open File	Close Open File for Managed User	View All Open File Properties
Delete Print Job	Delete Print Job for Managed User	Modify All Print Job Properties
Modify All Properties of Print Job Submitted by Managed User	Modify Print Job Priority	Pause Print Job
Pause Print Job for Managed User	Restart Print Job	Restart Print Job For Managed User
Resume Print Job	Resume Print Job for Managed User	View All Print Job Properties
Modify All Printer Properties	Modify Printer Scheduling Properties	Pause Printer
Resume Printer	View All Printer Properties	Modify All Service Properties
Modify General Service Properties	Modify Service Logon Properties	Pause Service
Resume Service	Start Service	Stop Service

Power	Power	Power
View All Service Properties	Clone Share and Modify All Properties	Create Share and Modify All Properties
Delete Share	Modify All Share Properties	View All Share Properties
Manage My Account	Modify All User Properties	View All User Properties
Clone Exchange Mailbox during User Clone	Clone User and Modify All Properties	Clone User and Modify Limited Properties
Enable Email for Cloned User	Add New User to Group	Create User and Modify All Properties
Create User and Modify Limited Properties	Enable Email for New User	Copy User to Another ActiveView
Delete User Account	Delete User Account Permanently	Disable User Account
Enable and Provision Users	Enable User Account	Manage User Password and Unlock Account
Modify DES Encryption	Modify Kerberos Authentication Requirements	Modify Reversible Encryption for Password
Reset User Account Password	Specify When User Can Logon	Specify Whether Account Can Be Delegated
Specify Whether Account Is Trusted for Delegation	Specify Whether Password Expires	Specify Whether Password Is Required for Logon
Specify Whether SmartCard Is Required for Logon	Specify Whether User Can Modify Password	Specify Whether User Must Modify Password at Next Logon
Specify Which Computers User Can Logon	Unlock User Account	Delete Email for User
Enable Email for User	View Email Address for User	Modify User Account Expiration
Modify User Comment	Modify User Description	Modify User Employee ID
Modify User Fax Number	Modify User Home Phone	Modify User IP Phone
Modify User Mobile Phone	Modify User Name	Modify User Pager Number
Modify User Primary Group	Modify User Type	Modify User WTS Environment Properties
Modify User WTS Remote Control Properties	Modify User WTS Session Properties	Modify User WTS Terminal Properties

Power	Power	Power
View User Primary Group	Modify General User Properties	Modify User Account Properties
Modify User Address Properties	Modify User Dial-in Properties	Modify User Netware Properties
Modify User Organization Properties	Modify User Profile Properties	Modify User Telephone Properties
Modify User WTS Properties	Add a User to Groups Found in a Template	Modify Address Properties while Transforming a User Account
Modify All Properties while Transforming a User Account	Modify Description while Transforming a User Account	Modify General Properties while Transforming a User Account
Modify Office while Transforming a User Account	Modify Organization Properties while Transforming a User Account	Modify Telephone Properties while Transforming a User Account
Remove a User from Groups Found in a Template	Associate Virtual Attribute	Create Virtual Attribute
Disable Virtual Attribute	Disassociate Virtual Attribute	Enable Virtual Attribute