NetNumen™ U31

Network Element Management

Security Target

Version: R13 V12.11.10 for Linux/HP

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: +86-755-26771900
Fax: +86-755-26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn

Revision History

Revision No.	Revision Date	Revision Reason
0.1	November 1, 2010	First version, suitable for application for certification
0.2	November 20, 2010	Added FPT_ITT.1, removed duplicate ToC, aligned with ZXSS10 ST, corrected SAR listing
0.3	December 3, 2010	Added clarifications resulting from first evaluator review.
0.4	December 10, 2010	Modified FTA_SSL.3, added placeholder to FDP_ACF.1
0.5	January 15, 2011	Corrected ZTE comments of 12/2010
0.6	January 21, 2011	Removed dual-server functionality, removed LDAP-server, added USB-tokens, submitted for evaluation
0.7	January 31, 2011	Corrected evaluator comments from ST evaluation
0.8	February 10, 2011	Corrected comments from: ● Evaluator on ST v0.7 ● Certifier on ST v0.7 ● Evaluator on ADVAGD document Replaced telnet client by CLI, as this was confusing people. Removed anti-virus from the TOE to the environment Removed the possibility of restricting login to either EMS-Client or CLI. Clarified that the TOE is configured to use passwords by itself or by RADIUS for all users Corrected that the TOE can use passwords or USB-token (and not both)
0.9	March 1, 2011	Removed USB tokens, removed FAU_ARP.1 and references to alarms, restricted scope of FAU_GEN.1.
0.91	March 16, 2011	Changed endpoints of trusted channels from workstation to clients. Changed definition of CLI. Removed RADIUS. Moved start/stop logging to system log instead of syslog and therefore also removed syslog.
1.0	April 5, 2011	,Final

Serial Number: SJ-20101109101114-019

Publishing Date: 2011-04-05(R1.0)

References

[CCp1] Common Criteria for IT Security Evaluation, Part 1, v3.1r3, July 2009

[CCp2] Common Criteria for IT Security Evaluation, Part 2, v3.1r3, July 2009

[CCp3] Common Criteria for IT Security Evaluation, Part 3, v3.1r3, July 2009

[CEMe] Common Methodology for IT Security Evaluation, v3.1r3, July 2009

Contents

Chapter 1
ST Introduction

Table of Contents

1.1 ST and TOE References

This is version 1.0 of the Security Target for the NetNumen U31 R13 v12.11.10 Element Management System (EMS) for Linux/HP .

1.2 TOE Overview and usage

The TOE is an EMS plus client. The TOE is used to manage a wireless telecommunications network.

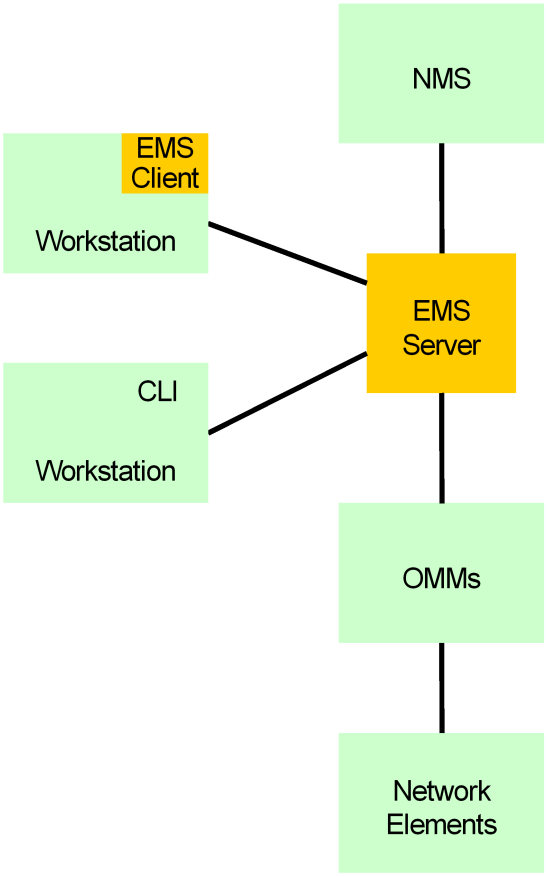
The TOE consists of two parts:

- An EMS Client, consisting of a Java application. This application is intended to run on a workstation. This client is a graphical user interface to the EMS Server.
- An EMS Server, consisting of a server plus software.

The EMS is intended to be the highest management workstation for a certain supplier in a telecommunication network. It manages one or more OMMs (see below) and provides information to the NMS (see below).

The TOE is depicted in Figure 1-1, together with relevant entities in its environment. The TOE communicates with these entities using the IP protocol.

Figure 1-1 The TOE in its environment



These entities are:

- A NMS: Network Management System[1]. This is a system that is used by a network operator to monitor its entire wireless telecommunications network. This network may contain several EMSs (usually from different suppliers). The TOE sends performance data, alarm data, configuration data and similar information to the NMS. The NMS is trusted by the TOE.
- One or more OMMs: (Operation Maintenance Module). An OMM manages a telecommunication network for a specific telecommunication technology (such as CDMA or WiMAX). The EMS can manage multiple OMMs at once. The OMMs are trusted by the TOE.
- Network Elements: These are the parts of the wireless telecommunications network that is managed by the OMMs and the TOE.
- One or more management workstations:
  - → Some with an EMS Client installed on them, which is used as a graphical user interface to the EMS Server.
  - → Some with no EMS Client installed on them. These use a command line interface running over a non-TOE ssh-client[2]) to access the EMS Server.

1. Some operators refer to an NMS as an OSS (Operations Support System).
2. This command line interface running on a non-TOE ssh-client is collectively referred to as CLI in this ST.

1.2.1 *Major security features*

The TOE:

- supports a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the wireless telecommunications network, and manage the TOE itself.
- supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.
- supports flexible logging and auditing of events.
- protects communication between EMS Server and the NMS, the OMMs the EMS Client and the CLI against masquerading, disclosure and modification.

1.2.2 *Non-TOE Hardware/Software/Firmware*

The EMS Client requires:

Type	**Name and version**
Workstation	A Workstation suitable to run the OS (see below)
OS	Windows, Linux or Solaris
Java	Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) Client VM (build 17.0-b16, mixed mode)

The command line interface requires:

Type	**Name and version**
Workstation	A Workstation suitable to run the OS (see below)
OS	Any OS suitable to run a ssh client (see below)
SSH client	Any software suitable to run ssh, such as putty.

The EMS Server does not require any non-TOE Hardware/Software/Firmware, but is always delivered with:

Type	**Name and version**
Anti Virus	A recent version of Trend Micro for CGS Linux (SPLX3.0 or higher with a recent virus library)

1.3 TOE Description

1.3.1 Physical scope

There are 4 hardware configurations[3] (called Modes) for the EMS Server. These are functionally identical, but differ in computing power.

	Mode 1	Mode 2	Mode 3	Mode 4
Platform	HP BL460cG6 2 E5504 CPUs 8GB Memory 2 300GB SAS Disks SAS adapter	HP BL680cG5 4 E7420 CPUs 8GB Memory 2 300GB SAS Disks SAS adapter	HP BL680cG5 4 E7420 CPUs 16GBMemory 2 300GB SAS Disks, SAS adapter	HP BL680cG5 4 E7450 CPUs 32GBMemory 2 300GB SAS Disks, SAS adapter
Disk Array	HP MSA2000sa G2 5 x HP 300GB SAS 15K 3.5"HDD	HP MSA2000sa G2 5 x HP 300GB SAS 15K 3.5"HDD	HP MSA2000sa G2 6 x HP 300GB SAS 15K 3.5"HDD	HP MSA2000sa G2 8 x HP 300GB SAS 15K 3.5"HDD

The TOE contains the following software:

EMS Client	Name and version
Application Software	EMS Client version NetNumen U31 R13 V12.11.10

EMS Server	Name and version
Application Software	EMS Server version NetNumen U31 R13 V12.11.10
Java	Java(TM) SE Runtime Environment (build 1.6.0_21-b06) Java HotSpot(TM) Client VM (build 17.0-b16, mixed mode)
OS	CGS Linux V3.02.00_P03/64bit
DB	Oracle 10.2.0.4 EE 64bit for Linux

The TOE is delivered with the following guidance:

3. There are also configurations available that provide the exact same functionality for Dell/Windows and Sun/Solaris, but these have not been evaluated. Similarly, there are also fault-tolerant dual server configurations available, but these also have not been evaluated.

Guidance (all prefixed with **NetNumenTM U31 (R13 V12.11.10))**
Standard Guidance: ● Network Element Management Technical Manual version 1.3 ● Network Element Management Security Management Manual version 1.2 ● Network Element Management Command Manual version 1.2
Maintenance: ● Network Element Management Routine Maintenance Manual version 1.2

1.3.2 Logical scope

The primary function of the TOE is to manage a telecommunications network by providing the following services:

- *Topology Management*: viewing, editing, and operating on the location, network structure, link connection and service distribution of the network resources in the network.
- *Fault Management*: monitor the running status of all devices in the network
- *Performance Management*: monitoring and analyzing the performance of the network
- *Configuration Management*: managing network elements and network services

To protect access to these services, the TOE provides four groups of security functionality:

Authentication: The TOE supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.

Whenever a user of the TOE wishes to use the TOE, the user needs to use either the graphical EMS-client or the CLI. The first action required by the user is then to log-in.

The TOE allows the Administrator[4] to configure (for each user), how that user must log-in:

- The user must always provide a username/password
- Whether the user can only login from a predefined IP-addresses and/or MAC-address
- Whether the user is only allowed to be logged in during a certain time (e.g. office hours)
- How the account is locked when the user repeatedly fails authentication (until unlocked by an Administrator[5] or until a predefined time elapses)

Authorization: The TOE supports a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the wireless telecommunications network, and manage the TOE itself.

4. Or a customisable role that has been assigned this right.
5. Or a customisable role that has been assigned this right.

The TOE allows management of the telecommunications network and itself by different users. The TOE can be configured to give each user precisely the access to the TOE and the resources of the telecommunication network that user needs to do his job. To assist in this, the role has a number of pre-defined roles:

- Administrator: a role with unrestricted access rights over all resources, including right to modify critical information of accounts.
- Maintenance: a role with high access rights, but only to resources assigned to him.
- Operator: a role with limited access rights, but only to resources assigned to him.
- Supervisor: a role with only viewing rights, but only to resources assigned to him

and can assign these roles to specific users. The last three roles can also be assigned per resource, that is: a user can have the Maintenance role for one resource, but Operator role for another, and no role at all for all other resources.

In addition, the TOE allows the Administrator[6] to define, modify and name customized roles and assign rights to these roles.

Note that none of the roles above has full “root” access to the TOE. This is reserved for ZTE maintenance staff that regularly service the TOE using the systems console, but this is out of scope for this ST.

Accounting: The TOE supports flexible logging and auditing of security, operation and system events.

The TOE maintains 3 separate logs:

- A security log for authentication events
- An operation log for operations performed by users
- A system log for server tasks that are not directly related to users performing operations

The logs are only accessible to the Administrator[7], who is only able to read the logs (not modify/delete them). Once logs become full, the oldest records are overwritten.

Secure communication: The TOE protects communication between the EMS Server and the NMS, the OMMs, the EMS Client and the CLI against masquerading, disclosure and modification

As shown in Figure 1-1, the TOE maintains communication between the EMS Server and the:

- EMS Client
- CLI
- NMS
- OMMs

All of this communication is performedusing standard protocols (such as SSH, SNMPv3 and SFTP) that protect against disclosure, modification and masquerading.

6. Or a customisable role that has been assigned this right.
7. Or a customisable role that has been assigned this right.

1.4 Excluded from the evaluation

The TOE is always delivered with anti-virus software installed on the EMS Server. As anti-virus software is updated almost daily, this software was not included in the evaluation.

In addition, the TOE can be used in conjunction with a NetBackup server to support backup and disaster recovery. This option was not assessed at all during the evaluation.

This page intentionally left blank.

Chapter 2
Conformance Claims

This ST conforms to:

- CC, version 3.1R3, as defined by [CCp1], [CCp2], [CCp3] and [CEMe].
- CC Part 2 as CC Part 2 conformant
- CC Part 3 as CC Part 3 conformant

This ST conforms to no Protection Profile.

This ST conforms to EAL 2+ALC_FLR.2, and to no other packages.

This page intentionally left blank.

Chapter 3
Security Problem Definition

Table of Contents

3.1 Organisational Security Policies

The TOE is intended to be used by many different telecom operators. Each operator will have a different wireless telecommunication network structure, different network technologies (such as CDMA, WiMAX), and a different organizational structure with different roles. The TOE must be able to support all of these operators. This leads to the following organizational security policy:

OSP.FLEXIBLE_MANAGEMENT

The TOE must be able to support:

- a flexible role-based authorization framework with predefined and customizable roles, both to manage the wireless telecommunications network, and manage the TOE itself.
- a flexible authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of IP/MAC-address and time of login.
- flexible logging and auditing of events.

3.2 Threats

3.2.1 Assets and threat agents

The purpose of the TOE is to allow various roles to manage the TOE and use the TOE to manage other equipment connected to the TOE (OMMs and equipment further downstream).

The relevant asset of the TOE is the ability of the organization owning the TOE to do the above properly.

This asset is threatened by the following threat agents:

1. TA.ROGUE_USER A TOE user seeking to act outside his/her authorization
2. TA.NETWORK An attacker with IP-access to the network that the TOE is part of
3. TA.PHYSICAL An attacker with physical access to the TOE

3.2.2 Threats

The combination of assets and threats gives rise to the following threats:

T.UNAUTHORISED

TA.ROGUE_USER performs actions on the TOE that he is not authorized to do.

T.AUTHORISED

TA.ROGUE_USER performs actions on the TOE that he is authorized to do, but these are undesirable[8] and it cannot be shown that this user was responsible.

T.UNKNOWN_USER

TA.NETWORK gains unauthorized access to the TOE and is able to use its functionality.

T. NETWORK

- Modify network traffic originating from / destined for the TOE or
- Impersonate the TOE

and thereby perform management actions on other entities on the network that the TOE manages or provide false information to the NMS.

T.PHYSICAL_ATTACK

TA.PHYSICAL gains physical access to the TOE (either client or server) and is able to use its functionality.

3.3 Assumptions

This Security Target uses a single assumption:

A.TRUSTED_NMS_AND_OMMs

It is assumed that the NMS and OMMs are trusted, and will not be used to attack the TOE.

8. For example, the user is allowed to modify data all over the telecommunications network to ensure that the network keeps functioning properly, but he misuses this to delete all this data thereby ensuring the network no longer operates properly.

Chapter 4
Security Objectives

These security objectives describe how the threats described in the previous section will be addressed. It is divided into:

- The Security Objectives for the TOE, describing what the TOE will do to address the threats
- The Security Objectives for the Operational Environment, describing what other entities must do to address the threats

A rationale that the combination of all of these security objectives indeed addresses the threats may be found in section 7.1 of this Security Target.

Table of Contents

4.1 Security objectives for the TOE

O.AUTHORISE

The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the wireless telecommunications network, and manage the TOE itself. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.

O.AUTHENTICATE

The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-addressand time of login.

O.AUDITING

The TOE shall support flexible logging and auditing of events.

O.PROTECT_COMMUNICATION

The TOE shall:

- protect communication between the EMS Server and the NMS and OMMs against disclosure, modification and masquerading

- protect communication between the EMS Client/CLI and the EMS Server against disclosure and modification.
- authenticate itself to the NMS and OMMs to prevent other entities masquerading as the TOE
- ensure that the NMS and OMMs authenticate themselves to prevent other entities masquerading as the NMS and OMMs.

4.2 Security objectives for the Operational Environment

OE.SERVER_SECURITY

The customer shall ensure that the EMS Server shall be protected from physical attacks.

OE.CLIENT_SECURITY

The customer shall ensure that management workstations that are used to connect to the EMS Server, either by CLI or by EMS Client, are protected from physical and logical attacks that would allow attackers to subsequently:

- Disclose passwords or other sensitive information
- Hijack the client
- Execute man-in-the-middle attacks between client and EMS Server or similar attacks.

OE.TRUST&TRAIN_USERS

The customer shall ensure that roles are only assigned to users that are sufficiently trustworthy and sufficiently trained to fulfill those roles.

OE.TRUSTED_NMS_AND_OMMs

The customer shall ensure that the NMS and OMMs can be trusted, so that they will not be used to attack the TOE.

OE.TIME

At least one OMM connected to the TOE shall supply the TOE with reliable time.

Chapter 5
Security Requirements

Table of Contents

5.1 Extended components definition

There are no extended components.

5.2 Definitions

The following terms are used in the security requirements:

Subjects

- Administrator: a role with unrestricted access rights over all resources, including right to modify critical information of accounts.
- Maintenance: a role with high access rights, but only to resources assigned to him.
- Operator: a role with limited access rights, but only to resources assigned to him.
- Supervisor: a role with only viewing rights, but only to resources assigned to him.
- Customized roles: these roles can be defined in the TOE by the Administrator (or by a configurable role who has the right to create roles) and have customizable rights.

None of the roles above has full “root” access to the TOE. This is reserved for ZTE maintenance staff that regularly service the TOE using the systems console, but this is out of scope and not described further in this ST.

Objects

Resource: An entity managed by the TOE, such as an OMM, or network equipment further downstream from an OMM, such as a base station. Also called network elements.

Operations

Operations in the TOE are divided into:

- Topology Management
- Fault Management
- Performance Management
- Configuration Management
- Maintenance Management

- Security Management

A more detailed overview of operations may be found in Appendix A. A full list of operations is outside the scope of this ST, and can be found in the TOE Guidance.

The following notational conventions are used in the requirements. Operations are indicated in **bold**, except refinements, which are indicated in ***bold italic***. In general refinements were applied to clarify requirements and/or make them more readable. Iterations were indicating by adding three letters to the component name (FTP_ITC.1.NMS).

5.3 Security Functional Requirements

The SFRs have been divided into six major groups:

- Identification & Authentication
- Roles & Authorisation
- Logging & Auditing
- Communication
- Management

5.3.1 Identification & Authentication

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified

- ***by username (in all cases), and***
- ***by IP-address (if so configured for that user)***
- ***by MAC-address (if so configured for that user)***

and ensure that the user is allowed to login at this time (if so configured for that user) before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated ***by password*** before allowing any other TSF-mediated actions on behalf of that user.

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session

- ***when [9]the allowed work time (if so configured for that user) expires, or***
- ***when one of the user roles is being locked while he is logged in.***

9. The sentence was refined to make it more readable.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect **when an administrator configurable positive integer within 2-3** unsuccessful authentication attempts occur related to **the same user account**.

FIA_AFL.1.2When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **lock the account**[10]

- **until unlocked by the administrator, or**
- **until an administrator configurable positive integer within [24-infinity] of hours have passed, if the account has not been set to permanent locking.**

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that ***passwords*** meet:

- **At least 6 characters including three of the four types: number, small letter, capital letter, other characters**
- **cannot be the same as the user name, the user name twice[11], the username in reverse[12] or a common dictionary word**
- **can be configured to expire after a configurable amount of time < 6 months**
- **can be configured to be different from the previous 5 or more passwords when changed**

FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same ***user***.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **1** sessions per ***user and a configurable limit of***:

- ***20 sessions for Mode[13] 1***
- ***50 sessions for Mode 2***
- ***100 sessions for Mode 3***
- ***200 sessions for Mode 4***

for all users together.

5.3.2 Roles & Authorisation

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **Administrator**

10. Unless this account has been set to unlockable.
11. If the username is chang, “changchang” is not allowed.
12. If the username is chang, “gnahc” is not allowed.
13. Modes are hardware configurations. See the TOE description for details.

- **Maintenance**
- **Operator**
- **Supervisor**
- **customized roles.**

FMT_SMR.1.2 The TSF shall be able to associate users with ***one or more*** roles.

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **Role Policy** on **all roles and resources** and all operations among ***roles*** and ***resources and the TOE***.

FDP_ACC.2.2 The TSF shall ensure that all operations between any ***role*** and any ***resource*** are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Role Policy** to objects based on the following: **all roles, all resources**[14].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among ***roles*** and ***resources and the TOE*** is allowed:

- **for the roles Administrator, Maintenance, Operator and Supervisor, as defined in Appendix A**
- **for the customized roles, as defined by their customization**
- **the Administrator and appropriately customized roles can perform the functions in FMT_SMF.1**[15]
- **if a user has multiple roles, it is sufficient if only one role is allowed to do the operation**
- **while a role is locked no user has this role**

FDP_ACF.1.3, FDP_ACF.1.4 ***(refined away)***.

5.3.3 Logging & Auditing

The TOE maintains 3 separate logs:

- A security log for authentication events
- An operation log for operations performed by users
- A system log for EMS server tasks that are not directly related to users performing operations

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

14. The attributes have been refined away as there are no relevant attributes.
15. Note that these are also among the functions defined in Appendix A, but the list at FMT_SMF.1 is in more detail as it is more relevant to the security of the TOE.

1. Start-up and shutdown of the audit functions ***(in the system log)***
2. ***(refined away)***

In the security log:

- **authentication success/failure**
- **user account is locked**
- **user account is unlocked**
- **user account is enabled**
- **user account is disabled**

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

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. ***(refined away)***
3. ***(in the system log): task start and end time) (in the security log): access method, client IP address***

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator and suitably customized roles** with the capability to read **operation log, system log and security log** 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.

FAU_STG.1 Protected audit trail storage

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 **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall **overwrite the oldest stored audit records**[16] if the audit trail is full.

5.3.4 Communication

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall[17] prevent the **disclosure or modification of all data** when it is transmitted between the **EMS Client and the EMS Server**.

16. The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.
17. Reference to policy refined away since the policy would simply restate the requirement

FTP_ITC.1.CLM Inter-TSF trusted channel

FTP_ITC.1.1 The ***EMS Server*** shall provide a communication channel between itself and ***the CLI*** 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 ***EMS Server*** shall permit the ***EMS Server and the CLI*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The ***EMS Server*** shall initiate communication via the trusted channel for **providing the results of commands to the CLI**.

FTP_ITC.1.NMS Inter-TSF trusted channel

FTP_ITC.1.1 The ***EMS Server*** shall provide a communication channel between itself and ***the NMS*** 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 ***EMS Server*** shall permit the ***EMS Server and the NMS*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The ***EMS Server*** shall initiate communication via the trusted channel for **transporting network performance data, configuration data and alarms to the NMS**.

FTP_ITC.1.OMM Inter-TSF trusted channel

FTP_ITC.1.1 The ***EMS Server*** shall provide a communication channel between itself and ***OMMs*** 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 ***EMS Server*** shall permit ***the EMS Server and the OMMs*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The ***EMS Server*** shall initiate communication via the trusted channel for

- **commanding the OMMs**
- **requesting and receiving small amounts of data from the OMMs.**

5.3.5 Management

FMT_SMF.1 Specification of Management Functions

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

Management function	Related to SFR[18]
Set whether a user can only login from certain IP-addresses, and if so, which IP addresses	FIA_UID.2
Set whether a user can only login from certain MAC-addresses, and if so, which MAC-addresses	FIA_UID.2
Set whether a user can only login at certain times, and if so, at which times	FIA_UID.2
Set the time that a user may remain logged in while inactive	FTA_SSL.3
Set whether a user is only allowed to work at certain times, and if so, at which times	FTA_SSL.3
Set the number of allowed unsuccessful authentication attempts	FIA_AFL.1
Set the number of hours that an account remains locked	FIA_AFL.1
Set whether a user account should be: ● unlockable, or ● locked (either permanently or temporarily) when it exceeds the number of allowed consecutive unsuccessful authentication attempts.	FIA_AFL.1
Unlock a user account	FIA_AFL.1
Set whether a user password expires after a certain time, and if so, after how long	FIA_SOS.1
Set whether the new password of a user must be different from the last n passwords when the password is changed by the user and configure n	FIA_SOS.1
Set the maximum number of concurrent sessions for the same user	FTA_MCS.1
Create, edit and delete customized roles	FMT_SMR.1
Add or remove roles to/from users	FMT_SMR.1
Add or delete types of events to be logged in the security log	FAU_GEN.1.1
Create, edit and delete user accounts	-
Disable/enable[19] user accounts	-
Lock/unlock[20] roles	-

5.4 Security Assurance Requirements

The assurance requirements are EAL2+ALC_FLR.2 and have been summarized in the following table:

18. This column of the table is for reference only, and is not part of the SFR.

19. The effect is the same as locking of a user account, but disabling is actively done by the administrator, while locking a user account is done by failing to authenticate too many times.

20. Locking and unlocking roles is done by the administrator. The effect is that any user with that role loses all access rights provided by that role, unless he has those rights also by a non-locked role.

Assurance Class	Assurance Components	
	Identifier	**Name**
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.2	Flaw reporting procedures
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

The following refinements apply to the SARs:

- ADV_ARC.1 is refined with "***The developer shall show, as part of the security architecture description, that the firewall in the EMS Server is configured to close all unnecessary ports.***"
- ATE_COV.1 is refined with "***The developer tests in the test documentation shall include penetration testing of the appropriate TSFI with recent versions of the OpenVAS and MetaSploit[21] penetration testing tools.***"

21. See www.openvas.org and www.metasploit.com

5.5 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL2+ALC_FLR.2. The reasons for this choice are that:

- EAL 2 is deemed to provide a good balance between assurance and costs and is in line with ZTE customer requirements.
- ALC_FLR.2 provides assurance that ZTE has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with ZTE customer requirements.
- The refinements are derived from ZTE customer requirements as well.

This page intentionally left blank.

Chapter 6
TOE Summary Specification

Authentication: The TOE supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.

General:

This functionality is implemented through a standard login screen.

FIA_UID.2, FIA_UAU.2, FIA_AFL.1

Whenever a user of the TOE wishes to use the TOE, the user needs to use either the graphical EMS-client or the CLI. The first action required by the user is then to log-in.

The TOE allows theAdministrator[22] to configure (for each user), how that user must log-in:

- The user must always provide a username and a password
- Whether the user can only login from a predefined IP-addresses and/or MAC-address
- Whether the user is only allowed to be logged in during a certain time interval (e.g. office hours)
- Whether an account is unlockable or not, and when an account is not unlockable:
  - → how many times a user can fail consecutive authentication attempts before that account is locked
  - → how the account is unlocked by the Administrator or until a predefined time elapses

FTA_MCS.1

Even if all of the above is correct, the user can still be denied access when:

- the user is already logged in
- too many other users are already logged in

FTA_SSL.3

The TOE will log a user out when:

- The Administrator locks one of the roles that that user currently has. The user can subsequently log in again, but he will not have that role.
- The user is only allowed to be logged in during a certain time interval, and this interval expires.

FIA_SOS.1

22. Or a customisable role that has been assigned this right. Note that this footnote applies to all uses of the term “Administrator” in this section.

Whenever the user has to provide a new password to the TSF (all passwords expire in 6 months or less), these passwords have to meet certain rules to ensure that the passwords cannot be easily guessed or broken by brute force. Passwords that do not meet these rules are rejected by the TOE.

Authorization: The TOE supports a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the wireless telecommunications network, and manage the TOE itself.

General

This functionality is implemented by the TOE not providing access to certain actions:

- by graying them out in the EMS Client
- by returning an error message in the CLI

or certain resources

- by not displaying these resources in the EMS Client
- by returning an error message in the CLI

for users whose roles do not allow this.

FMT_SMR.1, FDP_ACC.2, FDP_ACF.1, FMT_SMF.1

The TOE allows management of the telecommunications network by different users. The TOE can be configured to give each user precisely the access to the resources of the telecommunication network that user needs to do his job. To assist in this, the TOE has a number of pre-defined roles:

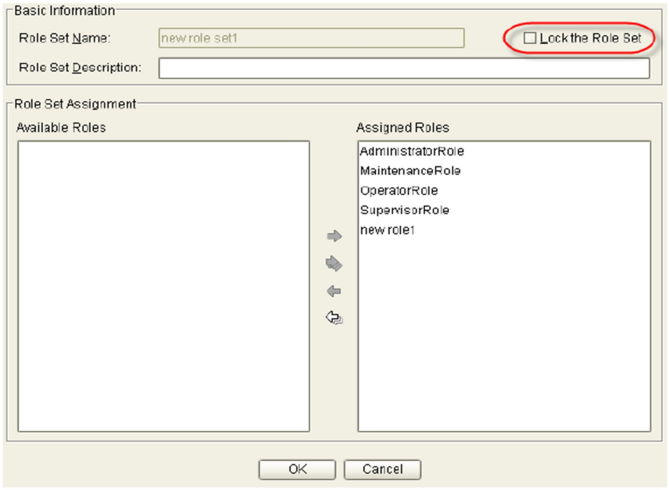
- Administrator: a role with unrestricted access rights over all resources
- Maintenance: a role with high access rights, but only to resources assigned to him
- Operator: a role with limited access rights, but only to resources assigned to him
- Supervisor: a role with only viewing rights, but only to resources assigned to him

and can assign these roles to specific users.

The role of Administrator is a global role: he has all rights for all resources. The other three roles are assigned per resource, that is: a user can have the Maintenance role for one resource, but Operator role for another, and no role at all for all other resources.

Finally, theAdministrator[23] can manage the TOE itself (see section 5.3.5 Management for a list of management functions), through a series of configuration and management screens. An example (how to lock a role) is given here:

23. Or a customisable role that has been assigned this right.

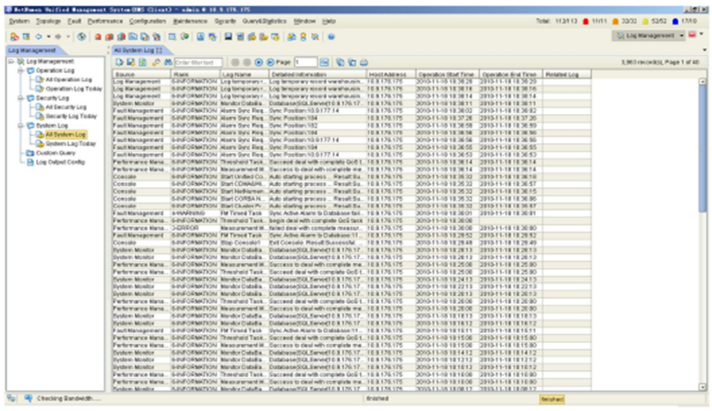


Note that none of the roles above has full “root” access to the TOE. This is reserved for ZTE maintenance staff that regularly service the TOE using the systems console, but this is out of scope for this ST.

Accounting: The TOE supports flexible logging and auditing of events.

General

This functionality is implemented by a set of screens like this log viewing screen:



FAU_GEN.1, FAU_SAR.1, FAU_STG.1, FAU_STG.4

The TOE maintains 3 separate logs:

- A security log for authentication events
- An operation log for operations performed by users
- A system log for server tasks that are not directly related to users performing operations (including starting and stopping the TOE)

The logs are only accessible to the Administrator[24], who is only able to read the logs (not modify/delete them). Once logs become full, the oldest records are overwritten.

24. Or a customisable role that has been assigned this right.

Secure communication: The TOE protects communication between the EMS Server and the NMS, OMMs, EMS Client and CLI masquerading, disclosure and modification

FTP_ITC.1.CLM, FTP_ITC.1.NMS, FTP_ITC.1.OMM, FDP_ITT.1

As shown in Figure 1-1, the TOE maintains communication between the EMS Server and the:

- EMS Client
- CLI
- NMS
- OMMs

All of these use standard protocols (such as SSH, SNMPv3 and SFTP) that protect against disclosure, modification and masquerading. In addition, the EMS Server obtains a NTP time signal from one of its OMMs, using the standard MD5-authentication to protect against masquerading and modification (disclosure is not relevant as time is public).

Chapter 7
Rationales

Table of Contents

7.1 Security Objectives Rationale

Assumptions/OSPs/ThreatsObjectives	
OSP.FLEXIBLE_MANAGEMENT The TOE must be able to support: ● a flexible role-based authorization framework with predefined and customizable roles, both to manage the wireless telecommunications network, and to manage the TOE itself. ● a flexible authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of: IP/MAC-address, time of login. ● flexible logging and auditing of events.	This OSP is primarily implemented by the combination of three security objectives: ● O.AUTHORISE that restates the first item of the OSP ● O.AUTHENTICATE that restates the second item of the OSP, and ● O.AUDITING that restates the third bullet of the OSP Additionally, to perform logging (part of the third item), the TOE must have a time source. OE.TIME states that this time source will be one of the OMMs connected to the TOE
T.UNAUTHORISED TA.ROGUE_USER performs actions on the TOE that he is not authorized to do.	This threat is countered by three security objectives: ● OE.TRUST&TRAIN that ensures that only users that are properly trusted and trained will be able to gain access to certain roles ● O.AUTHENTICATE that ensures users are properly authenticated so the TOE knows which roles they have ● O.AUTHORISE that ensures that only users with certain roles can do certain actions. So the only way that a user can perform a management action is when he has a role, and the only way he can get this role is if he is properly trained and trusted. Therefore this threat is countered.

Assumptions/OSPs/ThreatsObjectives	
T.AUTHORISED TA.ROGUE_USER performs actions on the TOE that he is authorized to do, but these are undesirable and it cannot be shown that this user was responsible.	This threat is countered by: ● OE.TRUST&TRAIN that ensures that only users that are properly trusted and trained will be able to gain access to certain roles. This should go a long way to prevent the threat from being realized. ● Should this prove insufficient, O.AUDITING will ensure that the actions of the user can be traced back to him. Together these two security objectives counter the threat.
T.UNKNOWN_USER TA.NETWORK gains unauthorized access to the TOE and is able to use its functionality.	This threat is countered by: ● OE.CLIENT_SECURITY, preventing the attacker to gain access to the clients ● O.AUTHENTICATE, preventing the attacker to gain access to the EMS Server Together these two security objectives counter the threat.
T. NETWORK TA.NETWORK is able to: ● Modify traffic on the network or ● Impersonate the TOE and thereby perform management actions on other entities on the network that the TOE manages or provide false information to the NMS.	This threat is countered by O.PROTECT_COM-MUNICATION that protects traffic between the TOE and the entities that are managed to the TOE against disclosure, modification and masquerading. The same O. PROTECT_COMMUNICATION protects traffic between the TOE and the clients against disclosure, modification and masquerading. Therefore this threat is countered.
T.PHYSICAL_ATTACK TA.PHYSICAL gains physical access to the TOE (either client or server) and is able to use its functionality.	This threat is countered by two security objectives: ● OE.SERVER_SECURITY stating that the server part of the TOE must be protected from physical attack ● OE.CLIENT_SECURITY stating that the client part of the TOE must be protected from physical attack Together these two counter the entire threat.
A.TRUSTED_NMS_AND_OMMs It is assumed that the NMS and OMMs are trusted, and will not be used to attack the TOE.	This assumption is upheld by the objective OE.TRUSTED_NMS_AND_OMMs which restates the assumption.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O.AUTHORISE The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the wireless telecommunications network, and manage the TOE itself. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.	This objective is met by: ● FMT_SMR.1 stating the predefined and customizable roles ● FDP_ACC.2 and FDP_ACF.1 defining a Role Policy, which states how the various roles manage the network and the TOE. These also state that only roles can perform actions (operations on resources) and therefore users can only do this when they have the correct role ● FMT_SMF.1 configuring all of the above Together, these SFRs support a flexible, role-based authorization framework.
O.AUTHENTICATE The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address, time of login.	This objective is met by: ● FIA_UID.2 stating that identification will be done by username, password, IP/MAC-address, login time ● FIA_UAU.2 stating that users must be authenticated ● FIA_SOS.1 stating that passwords must have a minimum quality ● FIA_AFL.1 stating what happens when authentication fails repeatedly ● FTA_SSL.3 logging users off when they are no longer allowed to work or when their role is locked ● FTA_MCS.1 preventing a user of having too many sessions or all users together having too many sessions ● FMT_SMF.1 configuring all of the above Together, these SFRs support a flexible authentication framework.
O.AUDITING The TOE shall support flexible logging and auditing events.	This objective is met by: ● FAU_GEN.1 showing which events are logged in the security log and system log ● FAU_SAR.1 showing that the logged events can be audited and by whom ● FAU_STG.1 showing how the audit logs are protected ● FAU_STG.4 stating what happens when the audit log becomes full ● FMT_SMF.1 configuring all of the above

Security objectives	SFRs addressing the security objectives
	Together, these SFRs support a flexible logging and auditing framework.
O.PROTECT_COMMUNICATION The TOE shall: ● protect communication between the EMS Server and the NMS and OMMs against disclosure, modification and masquerading ● protect communication between EMS Client/CLI and the EMS Server against disclosure and modification ● authenticate itself to the NMS and OMMs to prevent other entities masquerading as the TOE ● ensure that the NMS and OMMs authenticate themselves to prevent other entities masquerading as the NMS and OMMs	This objective is met by: ● FTP_ITC.1.NMS protecting the communication between TSF and NMS from modification and disclosure and ensuring that TSF and NMS authenticate (“assured identification”) themselves to each other, thus preventing masquerading ● FTP_ITC.1.OMM protecting the communication between TSF and OMMs from modification and disclosure and ensuring that TSF and OMMs authenticate (“assured identification”) themselves to each other ● FTP_ITC.1.CLM protecting the communications between CLI and the EMS Server from modification and disclosure of data ● FDP_ITT.1 protecting the communications between EMS Client and EMS Server from modification and disclosure of data Together these SFRs cover all parts of the objective.

7.3 Dependencies

SFR	Dependencies
FAU_GEN.1	FPT_STM.1: met in the environment by OE.TIME
FAU_SAR.1	FAU_GEN.1: met
FAU_STG.1	FAU_GEN.1: met
FAU_STG.4	FAU_GEN.1: met FAU_STG.1: met
FDP_ACC.2	FDP_ACF.1: met
FDP_ACF.1	FDP_ACC.1: met by FDP_ACC.2 FMT_MSA.3: not met, since there are no security attributes
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1: not met, as the policy was refined away, the dependency is unnecessary.
FIA_AFL.1	FIA_UAU.1: met by FIA_UAU.2
FIA_SOS.1	-
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2

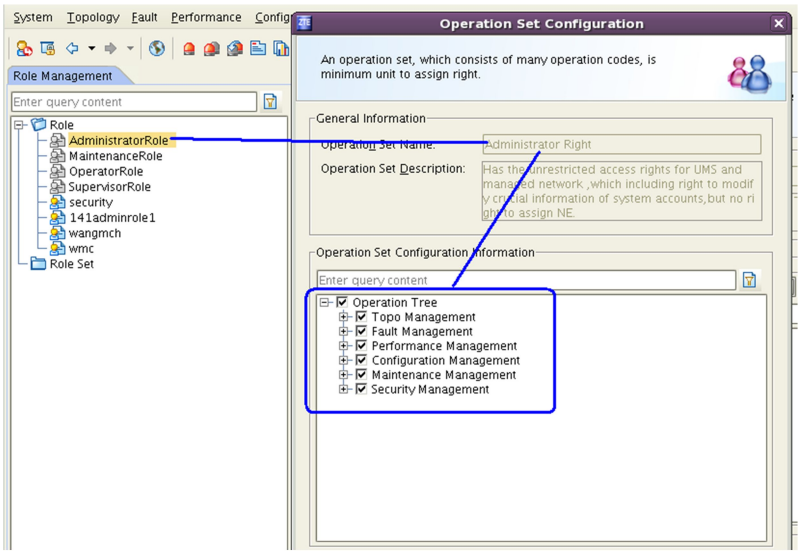
SFR	Dependencies
FIA_UID.2	-
FMT_SMF.1	-
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2
FTA_MCS.1	FIA_UID.1: met by FIA_UID.2
FTA_SSL.3	-
FTP_ITC.1.CLM	-
FTP_ITC.1.NMS	-
FTP_ITC.1.OMM	-
FMT_SMF.1	-
SAR	**Dependencies**
EAL 2	All dependencies within an EAL are satisfied
ALC_FLR.2	-

This page intentionally left blank.

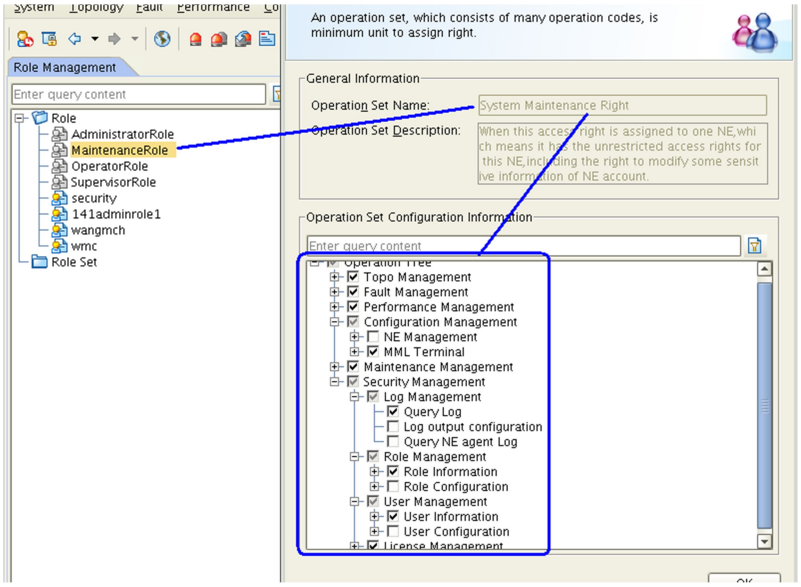
Appendix A
Roles and Operations

This Appendix provides a graphical overview of which roles can do what operations for the various roles.

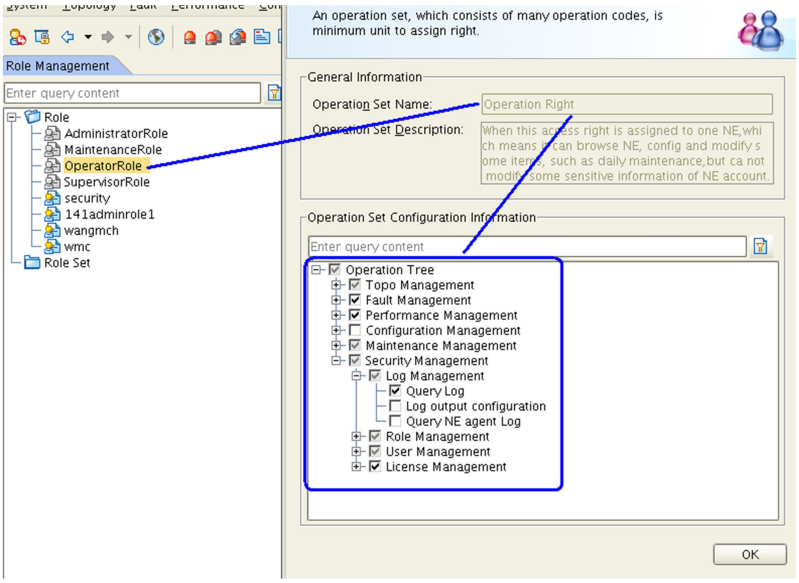
A.1 Administrator



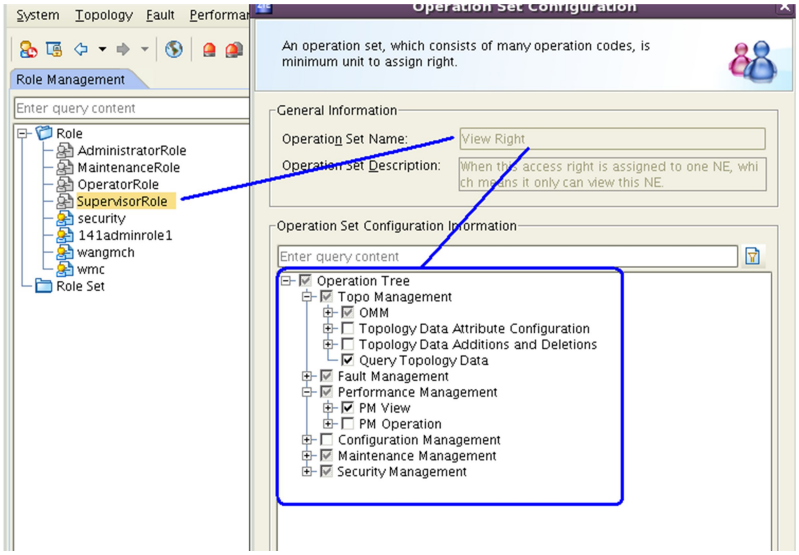
A.2 Maintenance



A.3 Operator



A.4 Supervisor



Figures