AGORA-NG User Manual – Resource Manager

Version 6.10-3

Last Updated January, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

OL-31407-01

CONTENTS

Contents

LIST OF FIGURES

LIST OF TABLES

Chapter 1
SUMMARY

This user manual details the general concepts and procedures of the AGORA-NG Network Management System (NMS). This document comprises the context environment of the AGORA-NG within the TMN (Telecommunication Management Network Forum) as like as the system architecture and corresponding technical description and requirements, setup procedures and basic configuration and activation of the main software modules relating the basic resource management functions.

In addition to this user manual an AGORA-NG technology dependent user manual should also be referred to, according with specific network provisioning aspects.

Chapter 2
TECHNICAL DESCRIPTION

AGORA-NG Platform

AGORA-NG is a modular, scalable and multi-user platform, based on Web and Java EE technology. It offers a centralized view of a network created by multi technology devices. This allows an efficient and effective management of network resources according to the operator's business goals.

AGORA-NG manages several telecommunication devices including legacy (nx64, ATM, xDSL and SDH) and state-of-the-art technologies (as MPLS and GPON).

AGORA-NG users can interoperate with a variety of applications through a graphical user interface (GUI) for all management operations: network provisioning, maintenance and monitoring.

A set of Northbound Interfaces (NBI) is also available allowing easy integration with third-party management/information systems.

Goals

The AGORA-NG application set is designed to provide a supervision system for transport and access networks, while also taking into account the diversity of technologies installed on these networks.

Its main goals are:

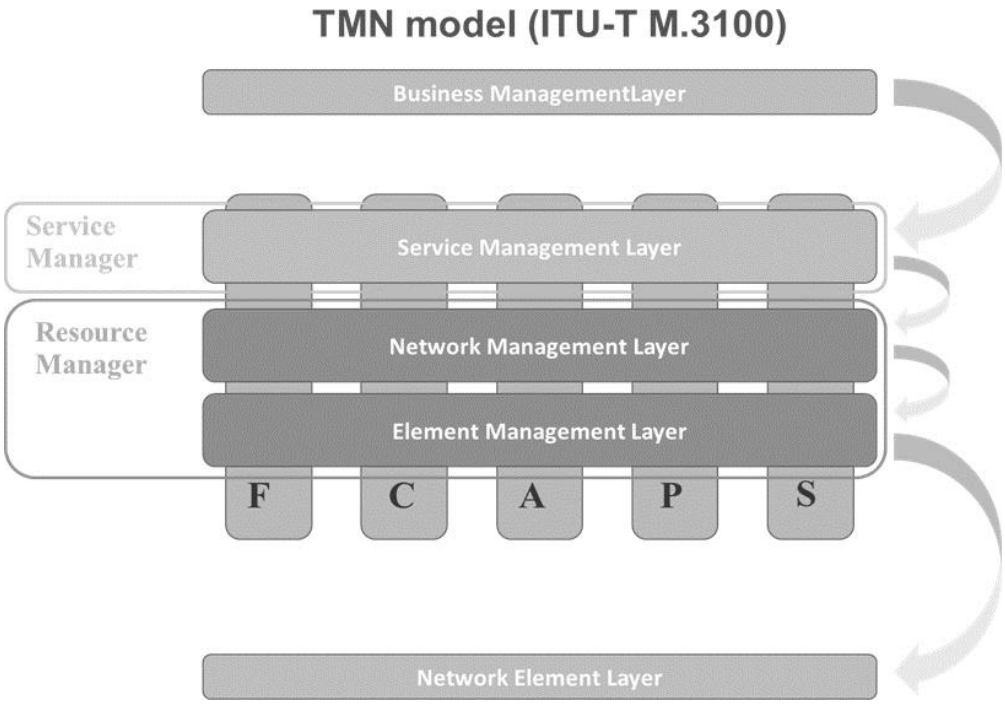
- Manage multi-technology and multi-supplier devices;
- Centralize alarm functions at a single point (device integrity status);
- Carry out remote and automatic device configuration;
- Deploy device inventory information (stock, location, constitution, etc.);
- Store historical alarm and performance data;
- Be independent and adaptable to the operator organizational structures;
- Be a multi-user system with simultaneous support for various graphical sessions;
- Support different access profiles, with user validation;
- Make use of IP interfaces for interconnecting system components;
- Expose open interfaces for connecting to other management/information systems.

Features

AGORA-NG implements the TMN network Element Management responsibility Level (EML) for each network element and the Network Management Level (NML) in the Resource Manager (Assure Pack) module. The level of Service Management responsibility is implemented in the Service Manager (Assure/Provision Pack) module.

Each of these levels implement a set of functionalities normally referred as FCAPS (fault management, configuration management, accounting management, performance management and security management) as represented in **Figure 1**.

Figure 1. TMN responsibility levels



Technological Scope

AGORA-NG supports the family of device/technology types deployed to customers at the device level.

One of the technological families supported by AGORA-NG is:

- GPON product line (OLTx family);

Geographical Scope

AGORA-NG is independent of geographical scope. It offers wide coverage, supporting all abovementioned technologic families being deployed in the manageable network. It requires a direct or proxy-based management communication with each network element.

User access to the system is also independent of the user's location.

Figure 2. Geographical Scope

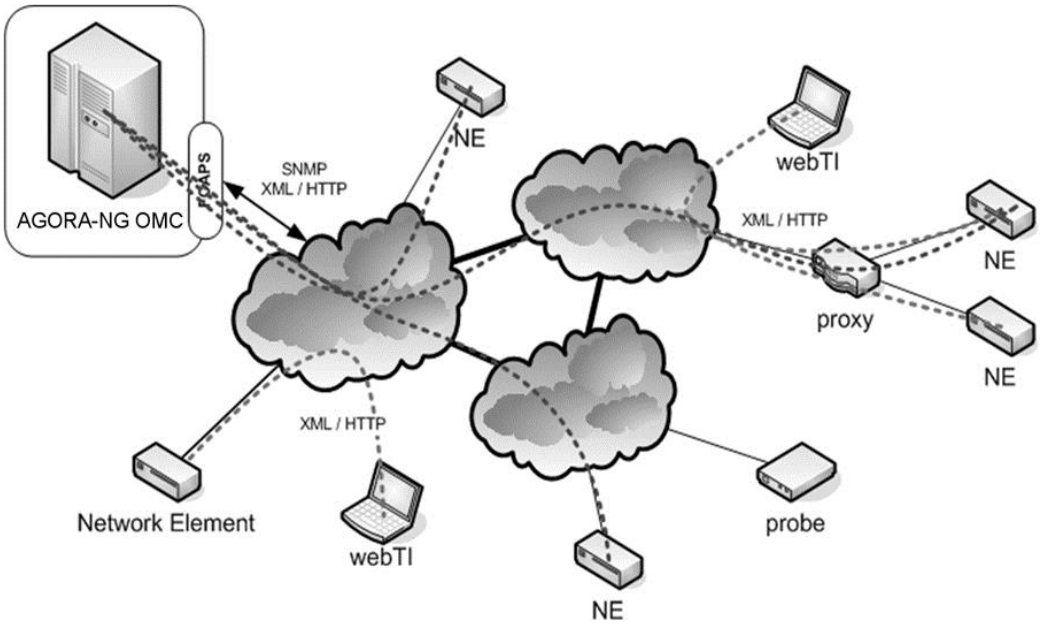


Figure 2 represents the communication between the AGORA-NG platform and the manageable network elements. This communication is ensured via an IP based DCN (Data Communications Network) implemented either as an out-of-band network (over a distinct, separated data network) or in-band (with dedicated channels over the data plane links, and therefore sharing resources and path with the data plane).

Enterprise Scope

AGORA-NG is designed to provide a flexible logical network organization for better adaptation with the operator own organization, considering the geographic distribution, different management teams with different management scopes and with different levels of authorization.

Two types of network elements organization are possible: a physical view and a logical view.

The physical view of the network offers a hierarchical structure where each network element belong to a single node (domain). This structure normally mirrors the operator geographical distribution and domain organization.

The logical view is more flexible since it allows each network element to be include in several management domains. Together with user authorization mechanisms, this enables a powerful and flexible user management control, where each user can manage only a set of management domains and network elements, and each network element or management domain can only be managed by a set of users.

Architecture

AGORA-NG is based on Java EE application servers and it has a modular architecture with different components and applications. Together they provide a complete and scalable management solution.

Portability is achieved since all components are Java language or Web technologies based allowing for a wider flexibility on HW and SW requirements and therefore reducing installation costs.

The envisaged modular architecture ensures a very scalable solution:

- The installation of each components depends on the deployment scenario avoiding unnecessary processes when they are not required;
- The abovementioned installation flexibility is also applicable to technology packs, adding features and options to the user interface and/or northbound interfaces depending on the installed technologies;
- Each application can be installed in a different co-located server distributing the workload among them, this also allows the AGORA-NG servers to grow as the network grows, adding more computing power only when necessary;

To increase the network management resilience and keeping the network operational and manageable even after a disaster situation, a high availability (HA) solution is available for AGORA-NG. Geographical redundancy can be achieved with the HA solution in an active stand-by master/slave configuration. Data is replicated and synchronized between both servers but only one is active in each instance. The server handover is transparent both to the users and to the manageable network.

AGORA-NG Functional components

Figure 3 shows the application functional architecture. The main modules are showed as well as their relationships.

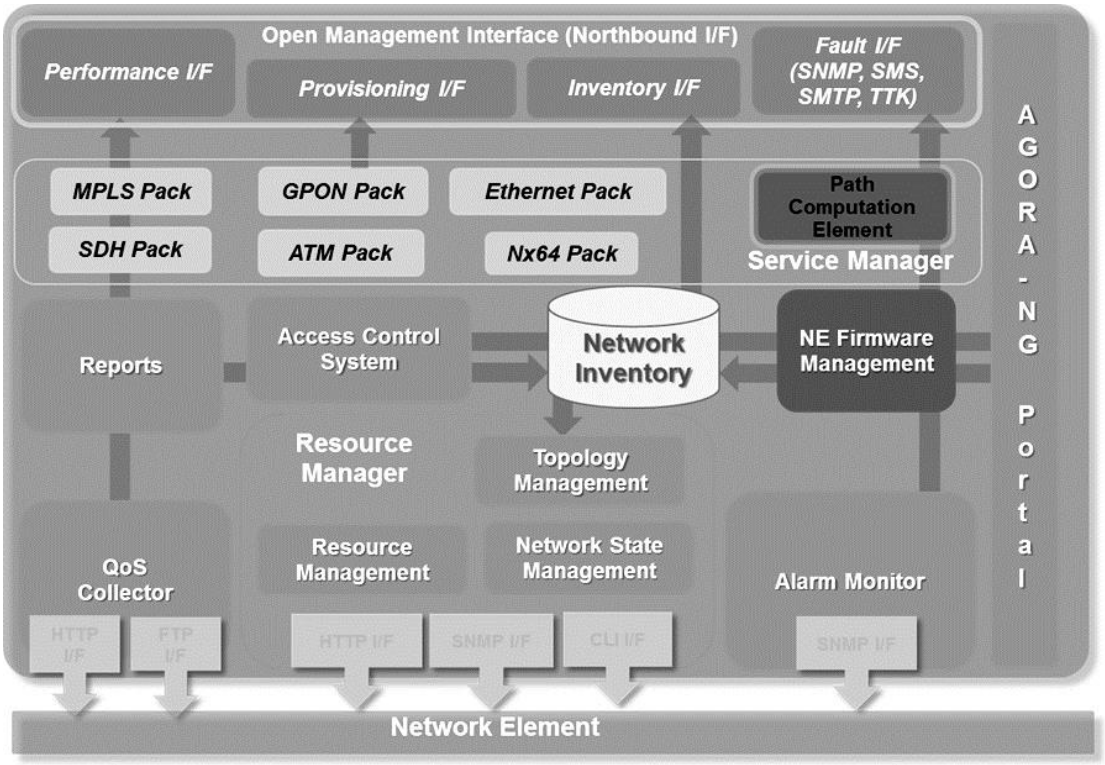
AGORA-NG follows a client-server three-tier architecture with a separation of the presentation, domain and data storage layers.

Reports, QoS Collector, Access Control System, Resource Management, Topology Management, Network State Management, Alarm Monitor and AGORA-NG Portal are the core componentes. Outside Resource Manager componentes, there are auxiliary modules which complement that one. Service Manager modules add technology specific management operations. Northbound Interfaces (NBI) are used for integration with third-party OSS platforms. Southbound Interfaces boxes identify the communication mediators with the managed network elements.

The Portal module provides access to the application modules. This is the entrance point of all users and the application launcher for the remaining applications. Working together with the Access Control System module, the Portal also guaranties Single Sign On (SSO) between all available applications.

The access control module, optionally integrated with LDAP, performs user authentication and access management, based on the combination of access profile and authorized domains.

Figure 3. Application architecture



The Resource Manager modules implement discovery, insertion and remote configuration of network elements, using SNMP, HTTP or Telnet/CLI interfaces. These modules also provide the framework for the remaining application components.

The Alarm Monitor module receives the alarms (SNMP traps) centralizing the operation on them. It can identify problems, set by pre-defined conditions, and notify other external systems by SMS, SMTP or TTK.

Based on the received alarms, the resource manager state machine, implemented by the Network State Management module, updates the state of each entity allowing a faster preview of the network state and avoiding a non-efficient polling of the network.

The Topology Management module manages the graphical elements and its relative position in each existing logical diagram.

The QoS Collector module continuously collects performance data created and published in each network element.

The Reports module is used to generate reports over the existing stored information.

Data persistence is ensured by an Oracle 11g database and it is represented in the figure by the Network Inventory box.

Several technology specific Service Manager components are available and can be combined depending of the deployed technologies.

The Path Computation Element is a module common to all Provision Packs and calculates the shortest path between two points. This module implements the MPS algorithm and allows the definition of inclusion and exclusion of nodes and links, in order to adapt the calculation with needs.

AGORA-NG exposes a Northbound Interface (NBI) for interoperability with third-party management platforms.

The available NBI is organized according with the following operational groups:

- Inventory Interface, for registering manageable network equipment's and track the number of equipment, cards and interfaces on the network;
- Fault Management Interface, which relays SNMP traps to alarms integrators systems;
- Provisioning Interface, to handle the provisioning activities on the network;
- Performance and Diagnostics Interface, to monitor the active state of the network elements and services.

The NBI is based on SNMP and HTTP/REST communication with JSON objects. It is also available a TL1 NBI for Provisioning, Performance and Inventory operations as shown in **Table 1**.

Table 1. Used protocols for the different NBI

	SNMP	HTTP/ REST	TL1	Exported file
fault	X	--	--	--
performance & diagnostic	--	X	X	X
provisioning	--	X	X	--
inventory	--	X	X	X

Figure 4. Mediation with OSS systems

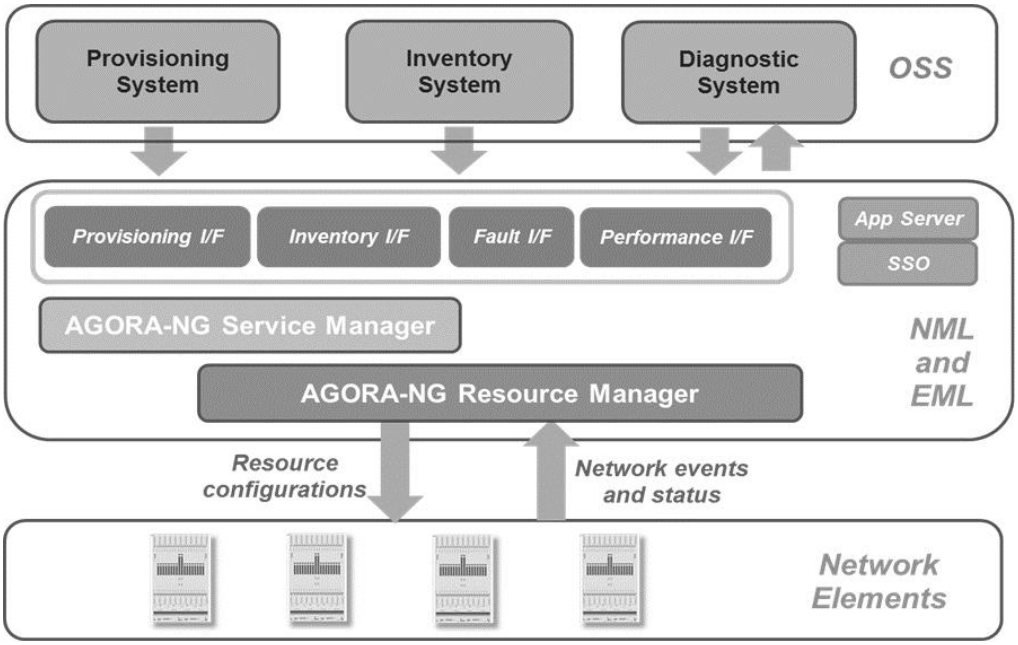


Figure 4 shows AGORA-NG mediation to OSS applications using the available NBIs to interact with different OSS functional modules.

Besides the abovementioned protocols, performance data or inventory reports can be exported as files either be periodically or on-demand.

AGORA-NG Processes

The different functional components represented in **Figure 3** are supported in several running processes and threads.

The next table shows the major active processes of the AGORA-NG application.

Table 2. AGORA-NG main processes

Process	Description
oracle database	Data storage for user and network information.
assurepack	Comprehends most of the Resource Manager functional components: topology; configuration; state and data normalization.
alarmmonitor	Fault management: event management; alarm relay.
reports	Executed upon request and display user reports for: alarms, performance and inventory.
mediator	Handles communication with the network elements.
portal	Session management (with Single Sign On) and AGORA-NG user interface launcher.
snmpdaemon	Collects events from the network and forwards them to assurepack.
performance	Extracts, transforms and loads performance data from the network
nbi-rest	Publishes northbound interface operations using HTTP/REST
nbi-snmp	Relays alarms (northbound interface) using SNMP
nbi-tl1	Publishes northbound interface operations using TL1.

Data storage and replication are ensured by an Oracle Database.

Assurepack is the main process for AGORA-NG. It handles all management business logic, ensuring both resource management and service management.

Portal, alarmmonitor, reports are complementary applications included in the AGORA-NG framework:

- Portal – application launcher, user authentication and single sign on
- Alarmmonitor – alarm monitoring and management, alarm relaying
- Reports – delivery of data reports (inventory, alarms and performance)

All communication with the network elements is handle through a set of mediator processes. These processes create the necessary abstraction of the equipment specific communication constrains.

Snmpdaemon handles receiving asynchronous events from the network elements forwarding them to the alarmmonitor application.

Interoperation with external third-party tools and applications are achieved via NBI. They are supported in a set of protocol daemons, namely nbi-rest, nbi-snmp and nbi-tl1.

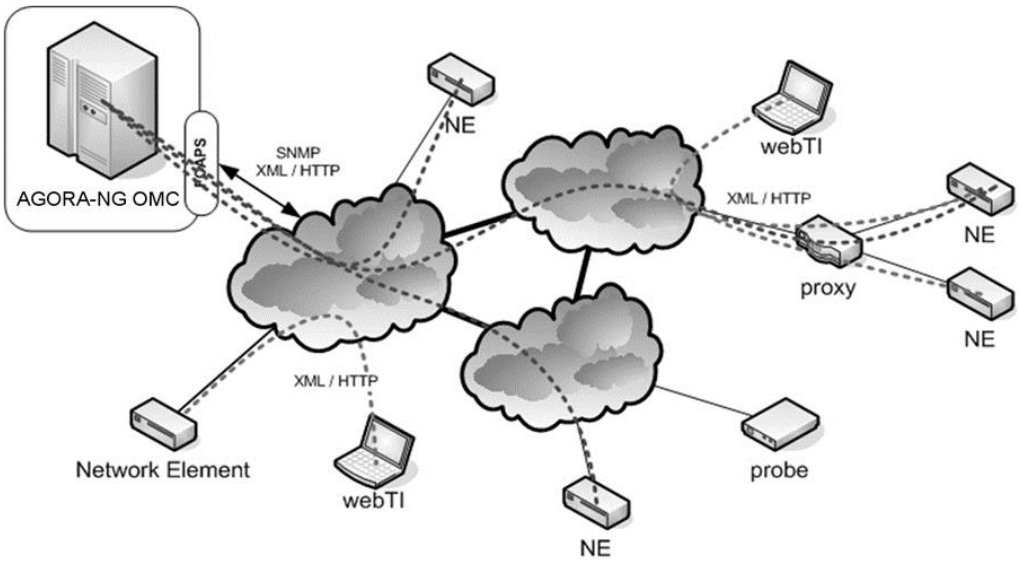
Interfaces

AGORA-NG management system runs on top of IP based networks to communicate with the network equipment's, the client interface applications and external OSS.

Communication between the management system and the equipment is mainly performed by SNMP and HTTP.

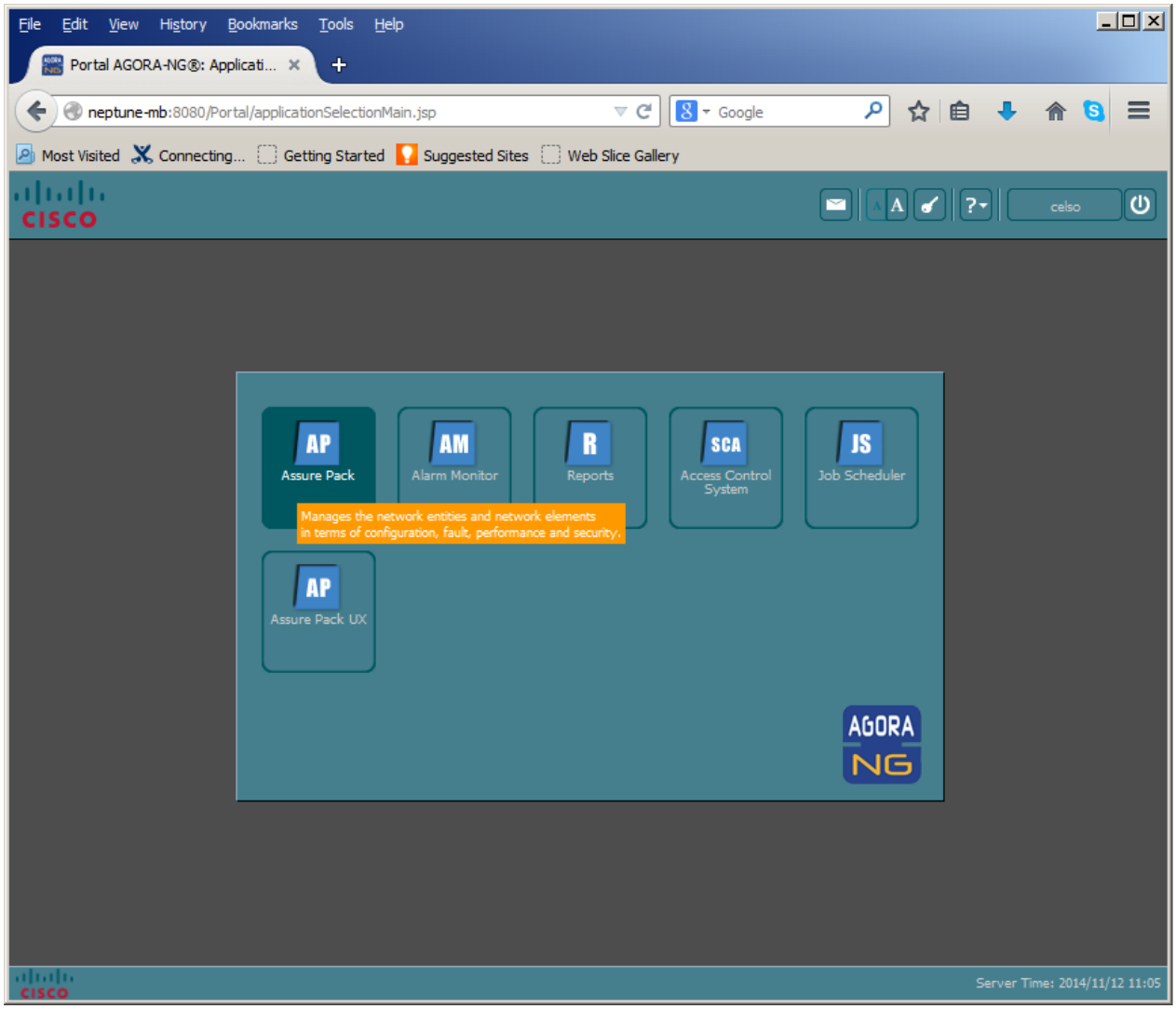
Some smaller equipment, such as CPEs, are not directly managed. They do not have an IP based agent, thus delegating that role to another network element that acts as a management proxy. As an example, the GPON ONUs delegate the management interfaces to the correspondent OLT.

Figure 5. Management network architecture



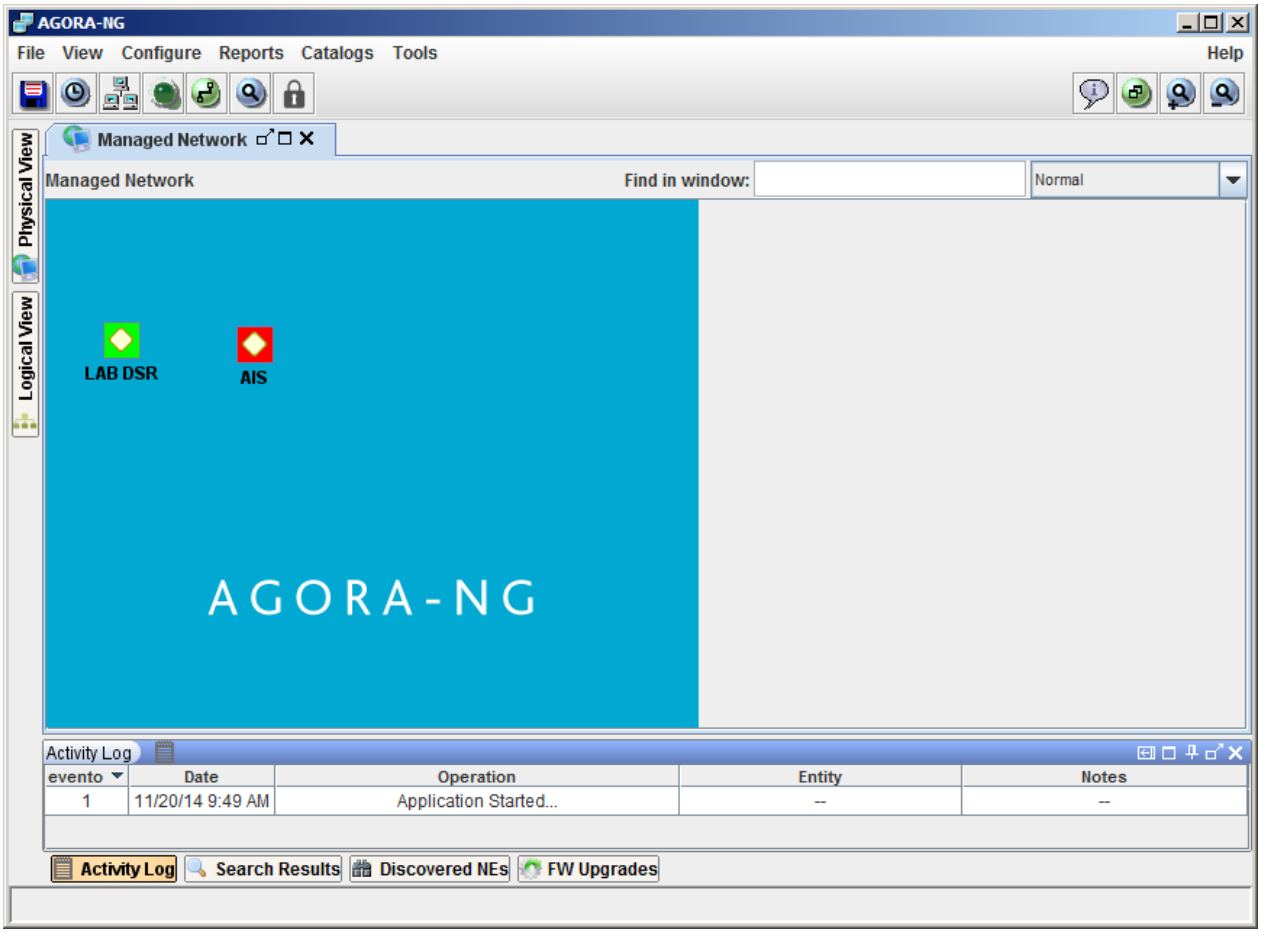
Users access AGORA-NG through an IP network using a web-browser to launch the AGORA-NG Portal (**Figure 6**).

Figure 6. AGORA-NG Portal



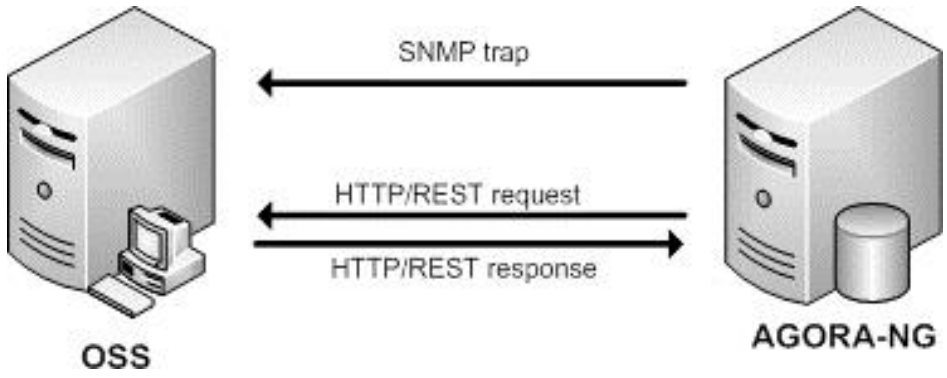
After a successful authentication the different installed AGORA-NG applications are shown in the application launcher window.

Figure 7. AGORA-NG GPON Service Manager web application



Third-party management tools such as OSS applications can use AGORA-NG through a M2M set of interfaces: the northbound interfaces.

Figure 8. NBI protocols



Deployment

AGORA-NG is a flexible and scalable solution. Depending on the customer needs there are different possible deployment scenarios:

- Single-Server
- Distributed-Server
- High Availability

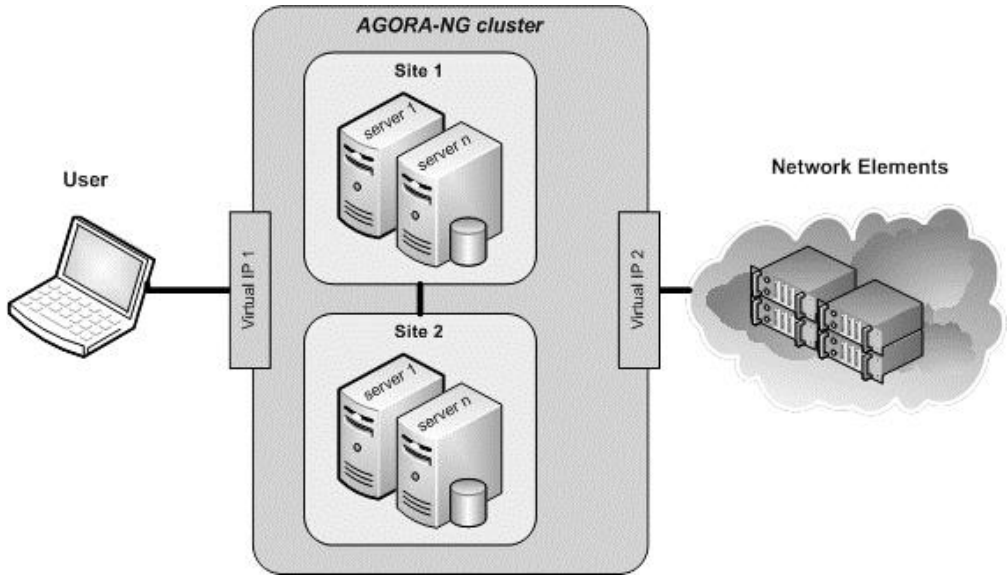
Choosing the right deployment strategy depend mainly in:

- Network growth forecast – if it is foreseen a rapid network growth, servers should be dimensioned for the foreseen network size;
- Cost management – adding servers as the network grows following a pay as you grow strategy
- Number of simultaneous users / concurrent operations

AGORA-NG Servers' Topology

Figure 9 introduces the different elements of a physical AGORA-NG installation.

Figure 9. AGORA-NG servers' topology

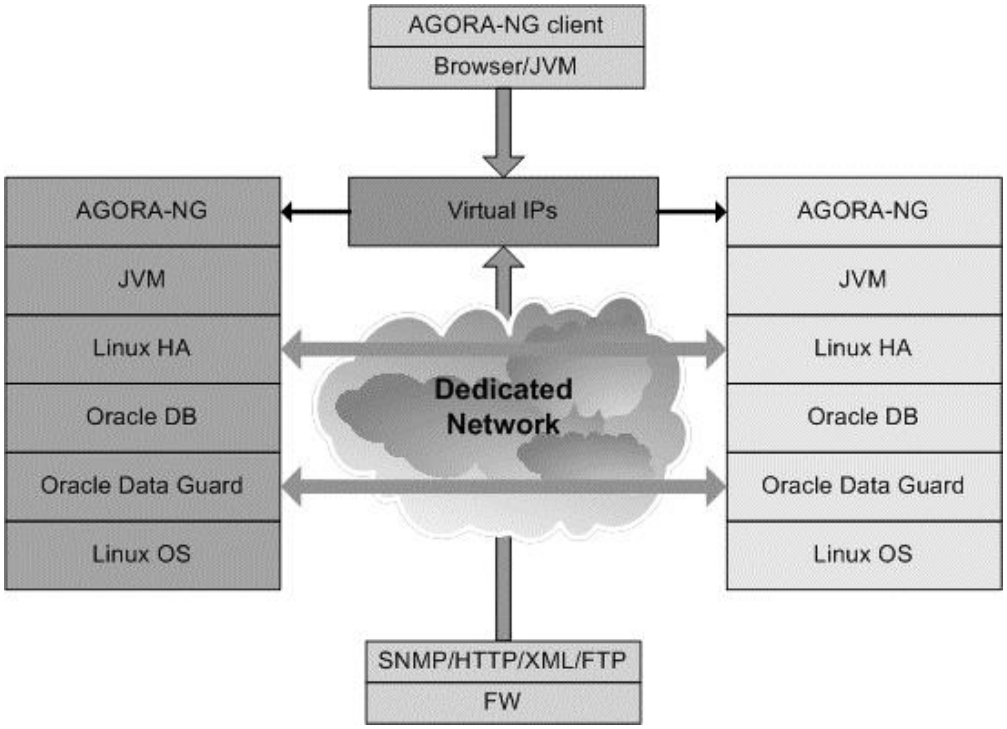


An AGORA-NG cluster represents a logical instance of the solution. A cluster can have 1 single site (and therefore the cluster and the site will be the same) or 2 distinct sites for High Availability scenarios: a Master site and a Slave site.

The cluster behaves as a single logical unit to the external systems exposing a set of virtual IP interfaces. From the user network (client) or the network equipment's perspective, the AGORA-NG will have the same IP addresses either the active site is site 1 or site 2.

Figure 10 shows how AGORA-NG is seen from the user client application and from the network equipment. It is also shown the application stack within each site and the communication between sites.

Figure 10. AGORA-NG processes in a cluster environment



Each AGORA-NG site has a physical AGORA-NG instance. This physical instance can be installed in a single server or can distribute the different AGORA-NG applications and components among different servers (e.g. installing the Oracle Database on a separated server).

Single-Server

This is the minimal size netwo rk. It is recommended for small to medium networks.

With a Single-Server configuration all AGORA-NG processes run in the same HW and SW also sharing resources with the Oracle Database.

Distributed-Server

A Distributed-Server configuration is recommended for medium to large networks.

With this configuration the different AGORA-NG processes can be distributed between different servers (therefore CPUs and OS), reducing the load on each server and ensuring a higher isolation between applications. The most typical scenario is to install the Oracle Database in a separated server, which also minimize the number of ORACLE DB licenses.

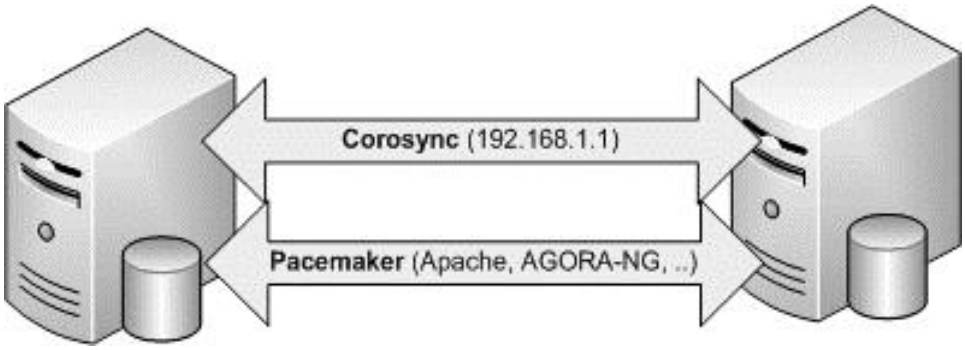
High-availability

AGORA-NG suite provides a high availability solution that relies on the Linux-HA project[1] for automatic system switchover and Oracle Data Guard[2] for active/standby database configuration that provides continuous synchronization between database instances.

Using the high availability solution the AGORA-NG system services are exposed using a virtual IP address that remains the same even after system failure and switchover. **Figure 11** shows how Linux-HA "corosync" and "pacemaker" projects work together in order to restore a fully working system without any impact on the network configuration. Corosync is used as a heartbeat protocol that detects system failure and triggers services start-up through pacemaker.

For more information about the high availability solution and setup instructions, follow links provided in the references.

Figure 11. High Availability solution



High Availability solution is available either with single server sites, distributed server sites or in a hybrid scenario (a distributed master site and a single server slave site).

Product Line

GPON product line

OLT equipment family systems are reliable modular Optical Line Termination (OLT) equipment specially devoted for fiber network infrastructures either Point-to-Point (P2P) Active Ethernet (AE) or Point-to-Multipoint (P2MP) FTTx Gigabit Passive Optical Network (GPON) architectures as well as assuring next generation PON technologies as XGPON-1 and NGPON2 (TWDM PON).

[1] http://www.linux-ha.org/wiki/Main_Page

[2] http://docs.oracle.com/cd/E25054_01/server.1111/e17157/architectures.htm#autoId6

Table 3. GPON product line

	Description
ME4620-OLT	Reliable high availability system that uses common element 1+1 protection (Power, Control, Switching and Processing) and load balancing LACP at the Uplink interfaces. Supports Voice, Data and Video services.
ME4600 ONT-RGW	Optical Network Termination equipment with residential gateway features included
ME4600 ONT-SFU	Optical Network Termination equipment without residential gateway features

GPON Boards and Interfaces Mapping

Uplink Line Card unit

Table 4. Uplink line card unit

Equipment	Board Module	Description	Interfaces
ME4620-OLT	ME4600-UMX-4x10GE	Module that interfaces with the Service Provider Network. Supports P2P topology	4x10GbE (XFP modules)

GPON Line unit

Table 5. GPON line unit

Equipment	Board Module	Description	Interfaces
ME4620-OLT	ME4600-AMX-16GPON	Provides sixteen class B+ or C+ GPON interfaces	16 PON (XFP modules)

Active Ethernet Line unit

Table 6. Active Ethernet line unit

Equipment	Board Module	Description	Interfaces
ME4620-OLT	ME4600-AMX-48GE	Provides 48 bidirectional Active Ethernet ports. Supports P2P or Uplink topology per port	48xGE/FE Active Ethernet. Bidirectional CSFPs modules (1000BASE-BX)

Switch Fabric unit

Table 7. Switch fabric unit

Equipment	Board Module	Description	Interfaces
ME4620-OLT	ME4600-XCO-640	Has a 640 Gbps switching capacity, four 10GbE internal connections and one O&M for each of the uplink and client boards	2xETH management interfaces G1 and G2 (RJ45) 1xUSB serial management interface MISC (Alarms/conditions and ACK indicators) contacts

FAN unit

Table 8. Fan unit

Equipment	Board Module	Description	Interfaces
ME4620-OLT	ME4620-OLT-FAN	Fan Module	-

DCN Planning

Network Management is the general term used to define the process by which one (or more management systems) controls and manages a network composed of transport and access equipment.

In order to accomplish the network management the communication must be established between each network element and its corresponding management system. The collective term for all these communication paths is "**DCN - Data Communication Network**".

The DCN transports network management traffic between network elements and their respective OSS, making them a vital link between the service network and the network operations center (NOC). These management data are messages from management systems to network elements and vice versa. The data could be:

- Alarms
- Protection switching events
- Performance data
- Configuration commands
- Measurements

Purpose

This document describes the management features in the most common DCN design scenarios. The DCN network scenarios of this document are typical. The NEs' may be used in many other combinations and mixtures. Being dependent from different network topologies, it is impossible to describe all the inter-working cases.

The Scope of the guideline includes:

- **Dimensioning**: This document contains information about NEs and describes how they are connected. It explains their function within the DCN Scenarios.
- **Inter-working**: The goal of this document is to provide a short guideline for the inter-working between the different types of Network Elements

DCN boundaries

The internal DCN refers to the communication network between NEs.

The external DCN refers to the communication network between the OSS, NSM and the GNE (Gateway Network Element). Usually, this network is based on TCP/IP.

Gateway Network Element (GNE)

A GNE is connected directly to the DCN, usually through an Ethernet port. As a rule, the interfaces used to connect the DCN are the GE1 or GE2 Ethernet ports.

The GNE has an attached subnetworks of NEs and provides remote access to these NEs by means of Embedded Control Channels (ECC).

The GNE performs Intermediate System (IS) network layer routing functions for ECC messages destined to any NE within the subnetwork.

DCN design

When designing the DCN network, the service provider must take into account the performance characteristic of all the routers, including the routing engine in the network element.

In general, the DCN network is a large TCP/IP network spread across a large geographic area with several hops and with resiliency built on top of IP or MPLS protection mechanisms.

Some NEs are directly connected to this DCN network. Others are beyond these NEs (See Gateway Network Element chapter). In order to manage these NEs other technologies have to be used. Namely:

- For GPON Networks:
  The OLT is directly managed through an IP assigned to the OLT. All the ONTs connected to this OLT are managed through OAM mechanisms (see GPON Management chapter). In this case the OLT act as a proxy, keeping the configurations parameters of all ONTs. The ONTs have no IP address for management purposes. Instead, a unique serial number is used to configure them, through the OLT.

- For SDH and MPLS Networks:
  All NEs have an IP or OSI address previously assigned. Routing tables are exchanged between nodes in order to keep available paths for OAM packets.

The routing engine in the network elements (NEs) can typically support a routing table of dozens of entries.

For SDH networks, as a rule of thumb, a packet should not have to make more than seven hops on the DCC to enter the DCN because of bandwidth limitations and the performance of the router in the network element. As the size of the ring approaches 16 nodes, a second GNE must be added to the ring.

For GPON networks, the OLT can be managed through its local Ethernet Port at which an IP address (out-of-band management) is assigned or using the Uplink Ethernet ports (in-band management), at which IP addresses are assigned. Using this last option a given VLAN and bandwidth is normally assigned so that it won't interfere with the data plane.

The first step for designing a DCN network is to gather information about a particular network environment. The natural geographic groupings of rings should be identified and a breakdown of the average central office size should be computed. This information is required for planning the DCN.

Following are the questions that need to be answered before the design process is begun:

1. What is the number of nodes in the network today?
2. What is the growth rate (number of nodes added per year) of the network?
3. How many network elements does the service provider want to place in an area to start with?
4. Does the service provider want to leave room for growth within an area?
5. How many central offices does the service provider have in the DCN?
6. Does the service provider want to support a single GNE or dual GNEs?
7. What is the average ring size?
8. How many rings can be aggregated into a single area?
9. How many rings are in a large, medium and small-sized central office?

OAM

Operations, administration and management/maintenance processes, activities, tools and standards.

ITU-T Y.1731 - Fault management and performance monitoring;

IEEE 802.1ag - Connectivity fault management;

IEEE 802.1ab - Link layer discovery;

IEEE 802.3ah - Ethernet in the First Mile;

ITU G.8031 - Ethernet protection switching.

OAM over MPLS Transport Networks example

For internal DCN, interconnecting MPLS NEs, the following technology applies:

MPLS is based on a subset of MPLS technologies with additional transport functionalities, as in traditional transport networks, making it a reliable, scalable, and cost optimized packet-based transport technology.

MPLS introduces additional transport functionalities such as comprehensive OAM capabilities, survivability, data-plane/control-plane separation, and static provisioning of bidirectional services. This is in addition to well-accepted MPLS functionalities such as Quality of Service (QoS), scalability, traffic engineering and Layer 2 packet forwarding. The result is the ability to provide network operators with full control over their packet networks.

MPLS has Enhanced OAM tools

- Continuity Check (CC) for fast failure detection
- Alarm Indication Signal (AIS) for fault isolation

- Remote Defect Indication (RDI) for fault isolation
- Loopback (LB), similar to IP ping, for basic maintenance
- Loss/delay measurement for detection of performance degradation

MPLS OAM provides the same OAM concepts and methods which are available in legacy transport networks, including

- Fast failure detection
- Alarm suppression
- Remote defect indication
- Protection switching

OAM packets are carried on Generic Associated channel (G-Ach). OAM and data packets are carried on the same path, therefore enabling simpler and faster monitoring of the PW and LSP layers.

MPLS OAM introduces the functional components, Maintenance End Point (MEP) and Maintenance Intermediate Point (MIP), which enable running OAM packets between two end points, such as:

- Continuity checks (CC) messages allowing fast detection of loss of connectivity, as well as connection mis-configuration. The CC messages are sent periodically by MEP and monitored for Loss of Continuity (LOC) by each MEP/MIP. The transmission interval can be set to a minimum of 3.3ms, allowing for very fast-failure detection.
- Delay and Loss Measurements (DM/LM) allowing the detection of performance degradations.
- Loopback (LB) messages allowing on-demand bidirectional diagnostic test for connectivity check and failure localization.
- Alarms suppress enabling fault localization while avoiding unnecessary alarms propagation. AIS and RDI are sent to the remote sides in case of LOC detection.

This means that a TCP/IP channel can be built upon this OAM channel, allowing the NEs to see each other within a L3 network.

Interface with the remote NMS

The Matrix units provide communication with the remote management platform through units' G1 connector, requiring a 10/100/1000 BASE-T physical interface.

Local management interface

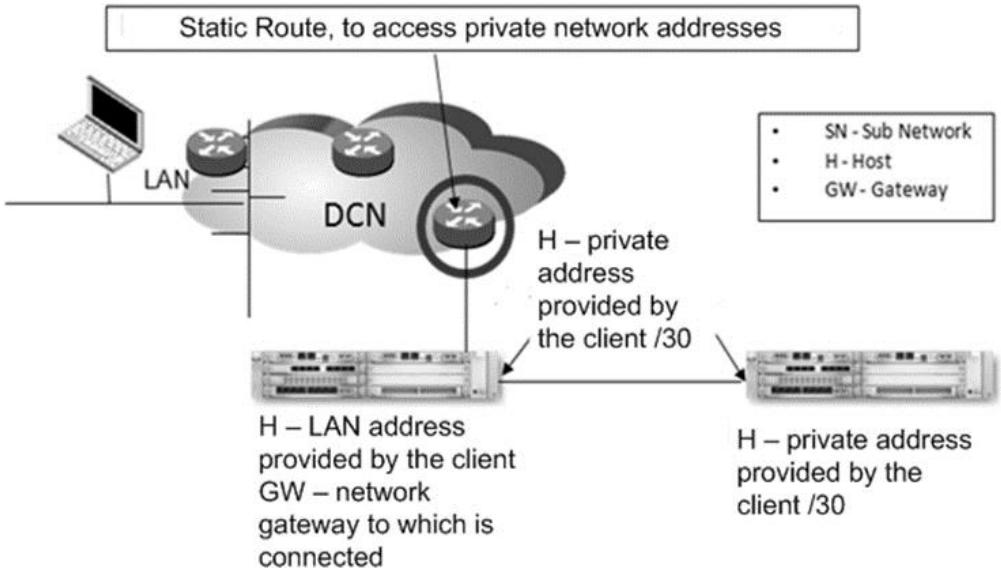
Matrix units offer a physical interface 10/100/1000 BASE-T (called G2) for local management purposes.

- IP addressing criteria:
    - Private network for interconnecting pathways, will be a single class C, shared by the various structures. This will minimize the unnecessary use of private IPs;
    - n DCN addresses (/xx) will be assigned for each network allowing y NE management;
    - Each class (256 addresses) is divided into different sub-networks taking into account the maximum number of structure elements;
    - Each network node, except GNE (address and mask assignment defined in the DCN), will be assigned an IP from the previously defined range, taking into account a 4 addresses subnet (/30) for each unit,

two hosts (one of the hosts is for the equipment and other may be for equipment that is connected to this Ethernet interface);

- Given that these addresses are not broadcast outside the network (GNE), the same range of addresses can be used in different structures for interconnecting pathways. Network will use 256 addresses – A.B.C.0 (/24), for all networks;
- Allocating addresses in the interconnecting pathways has to be done considering use of four addresses (/30) for each path. It is possible to define up to 64 interconnecting pathways per structure;
- A static route must be created in the router that connects to t he GNE to reach the GNE network devices;
- An IP route must be configured in the GNE indicating the network GW to which it is connected.

Figure 12. Private addresses

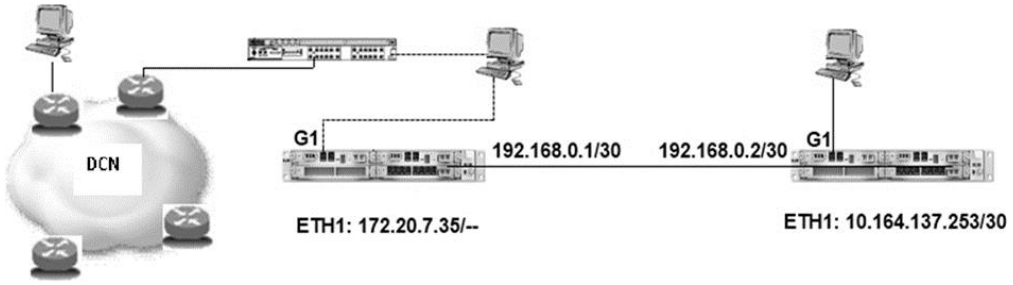


System connection

- When G1 interface is busy, it is possible to connect to the matrix units G2 interface (local management) using 192.168.200.101 or 192.168.200.102 addresses (if the matrix units are in slot 1 or 2, respectively). This method will avoid disturbances in the remote management platform communications. In the PC network card the address 192.168.200.200 with mask 255.255.255.0 must be entered.
- This connection does not provide communication with remote devices;
- In order to ensure communication with remote devices the examples detailed below can be used.

NOTE: The connection of the matrix card G2 port to the PC network card can be done using a direct or crossover network cable.

Figure 13. Communication with a remote NE



Example 1:

- In order to configure the PC network card, an IP and the respective mask belonging to the same network device will have to be provided. Address 172.20.70.35 must be entered in the GW network. thanks to that, it is possible to reach http://10.164.137.253 from the location where the PC is connected;
- Remote machine should respond.

Example 2:

- It is possible to reach http://10.164.137.253 in case lacks an available address on the network by disconnecting the LAN cable from G1 and configuring the PC network card using 172.20.7.36/24 and the respective GW with 172.20.7.35;
- Remote machine should respond.

Example 3:

- For above cases, it is possible (for previous cases) to access the machine with address 172.20.7.35 from the device 10.164.137.253, ensuring that the PC is connected to G1 LAN interface and the PC network card has been configured with IP 10.164.137.254, mask 255,255,255,252 and 10.164.137.253 address in the respective GW;
- This way it is possible to reach http://172.20.7.35;
- Remote machine should respond.

IP over Data Communication Channel (DCC)

For internal DCN interconnecting SDH NEs the following technology applies:

The IP over DCC feature uses the SDH Operation Administration and Maintenance (OAM) channel to manage devices. SDH standards support extensive operations, administration, management, and provisioning (OAM&P) capabilities.

The following overhead bytes are specified in the standards as the OAM channels that carry management information, alarms, and management commands:

- D1 to D3 bytes of the Section overhead
- D4 to D12 bytes of the Line overhead

These overhead bytes are referred to as the data communication channel (DCC). The Line-level DCC is a 576 kbps OAM channel; the Section-level DCC is a 192 kbps OAM channel.

Similar to MPLS networks, using this channel the SDH NEs see each other within a L3 network.

GPON Management

For internal DCN interconnecting OLTs and ONTs NEs the following technology applies:

The embedded OAM and PLOAM channels manage the functions of the PMD and GTC layers. The OMCI provides a uniform system of managing higher (service defining) layers.

The embedded OAM channel is provided by field formatted information in the header of the GTC frame and are meant to be used mostly for bandwidth granting and Dynamic Bandwidth Assignment signaling.

The ONT can be fully managed by OMCI or have a set of functionalities being managed by TR-069.

The OLT can be directly connected to the external DCN (out-of-band) using its Ethernet Management Ports or be managed through the internal DCN (in-band) using a given VLAN and sharing the uplink port bandwidth.

There are two management ports, G1 and G2 in front panel of the Matrix card.

G1 is the interface that should be used for the DCN connection, since it has a configurable IP address.

G2 is the interface that should be used for local access to the Equipment since it has a fixed IP address, 192.168.200.###. The last part of the IP address depends on the slot the Matrix card is inserted in. For the matrix card inserted in slot 1 (Left) the G2 IP address is 192.168.200.101. For the matrix card inserted in slot

OSI over DCC

As SDH rings grow in both size and number, telcos must deploy higher bandwidth and more scalable DCN networks to manage SONET/SDH network elements.

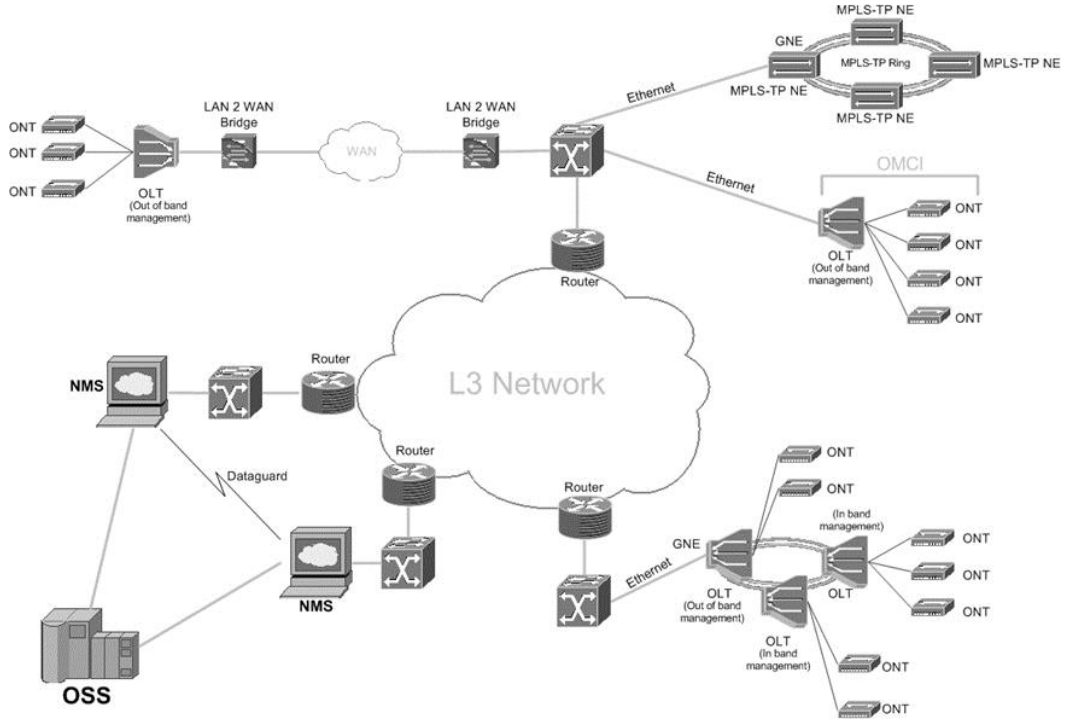
OSI protocol stacks used in SDH network elements for management require that the DCN be able to use OSI to route to and from the network element and its associated OSS, in addition to the higher bandwidth requirements.

ITU-T Recommendation M.3010 defines the architectural requirements for a Telecommunications Management Network (TMN) to support management network operators in planning, provisioning, installing, maintaining, operating, and administering telecommunications networks and services. Within that document, the ITU describes the DCN, which provides the communications backbone between network elements and OSSs.

Applications

A typical DCN application is depicted below:

Figure 14. Typical DCN network



In this topology OLTs and MPLS nodes have an IP address assigned. Routes can be exchanged by using RIP, OSPF or IS-IS mechanisms.

The NMS can access any of the devices, as they share the same L3 network. Devices can see each other or rules can be defined to limit this access.

Users must consider a rule of thumb of 2 Mbit/s required per OLT and MPLS NE for management purposes. For the OLT, if this rule is followed all the ONTs directly connected will be managed without any constraints.

Actions that require higher bandwidth usage, such as firmware download or database synchronization, may benefit from more bandwidth allocated.

Care must be ensured when defining routes and allocating tunnels as the communication between NMS and NEs takes place not just when the user is configuring but also constantly as alarms and reports are being generated by the NE and exported towards the NMS and its northbound interface.

QoS mechanisms can be configured to guarantee access under congestion situations.

Rules

Some rules to be followed:

- Correctly configure the gateway of each NE. The GNE has an important role on the DCN, routing packets to the proper destination.
- Use unique IPs for each of the NEs to avoid routing errors or conflicts
- Any IP class address can be used except the following ones: 127.x.x.x (loopback) and, 192.168.1-201.x.
- Ethernet ports within the same chassis must belong to different subnets
- Static routes can be defined. These have priority over dynamic routes learnt

Chapter 3
SETUP

Equivalent network size

Estimating the hardware resource requirements of the management platform is highly influenced by the number of managed network elements. More equipment and devices mean more management events and operations consuming more communication and processing resources.

Moreover the weight of each network element type may vary. The total number of elements is just a first approach to estimating the real impact on the management servers, since the management overhead of each network element type must also be considered.

This section will provide the information required to estimate the equivalent network size considering the overhead of each network element as well as the number of network elements.

The equivalent network size is a weighted measure of the network complexity considering the number of manageable equipment diversity and number and its impact on the management platform.

An accurate estimation of the equivalent network size is mandatory for the initial deployment planning but also as the network grows. This will ensure the proper performance of the applications at all times.

The following table shows the network element overhead associated with managing each network element type.

Table 9: NE overhead coefficients

Network Element Type	Network Element Overhead Coefficient
ME4601-OLT	1
ME4620-OLT	3
ONU	0.003
ME4600-ONU-48V	1
MPLS equipment	3

The obtained coefficient for each network element type will be used to affect its weight in the overall summation.

The following expression shows how to calculate the equivalent network size according to the planned number of physical network elements:

$$x = \sum_{t} n_t \times \rho_t$$

x- equivalent network size

t- number of different network element types

nt- number of network elements of a type

ρt- network element overhead coefficient

For example, to calculate the equivalent network size when deploying 20 ME4620-OLT and 500 000 ONU we must solve the following expression:

$$x = 20 \times 3 + 500000 \times 0.003$$

$$x = 1560$$

This means that the equivalent network size for the referred example is 1560.

Knowing the equivalent network size allows the categorization of the network size according to the following table:

Table 10: Network size reference

Network size	Number of equivalent network element	Estimated number of events per second
tiny	1 - 2500	5 - 40
small	2500 - 5000	40 - 80
small-medium	5000 - 7500	80 - 120
medium	7500 - 10000	120 - 160
medium-large	10000 - 12500	160 - 200
large	12500 - 17500	200 - 280
huge	17500 - 20000	280 - 320

The network size categories defined by the previous table will be used throughout the rest of the document.

Table 10 also defines the recommended event rate capacity range for each network size category. A medium sized network, for example, is dimensioned to handle up to 160 events/s. Higher values can be reach during short periods of time without significant performance degradation.

For each deployment scenario, the correspondent size class must correspond to the highest between equivalent network elements and required events/s handling capacity.

AGORA-NG server resources requirements depend not only on the network size but also in the expected number of concurrent operations.

Concurrent operations are triggered by:

- Network events
- User operations (using the applications GUI)
- M2M operations (using Northbound Interfaces)

While planning a deployment scenario, the identification of the network size class must be revised to include the weight of the required concurrent operation capacity.

Table 11 shows the correction coefficient for the equivalent network size, to include the weight of the concurrent operations.

Table 11: Concurrency coefficient

Concurrent operations range	Concurrency coefficient
0-5	1
6-10	1,1
11-15	1,3
16-20	1,6
21-25	2

Using the previous example (20 ME4620-OLT + 500K ONUs), for an expected number of 10 concurrent operations, the equivalent network size must be adjusted as follows:

$$x' = 1560 \times 1{,}1$$

$$x' = 1716$$

A second example:

requirements

200 MPLS equipment

50 ME4620-OLT

800000 ONT

20 concurrent operations

results

$$x = 200 \times 3 + 50 \times 3 + 800000 \times 0.003 = 3150$$

$$x' = 3150 \times 1{,}6 = 5040$$

Considering only the weight of each equipment type the equivalent network size would be 3150, this mean that this network should be considered as small size.

Adding the concurrent operations requirement, the new revised equivalent network size is now 5040, changing the network class to a small-medium size.

Deployment scenarios

AGORA-NG is a distributed system therefore it may be deployed not only in a single node configuration, but also in a distributed, multiple nodes configuration.

Selecting the best scenario is highly dependent on the network overhead (equivalent network size) and has a direct impact on the performance and responsiveness of the network management platform.

Even though the decision must be taken wisely, AGORA-NG allows the migration from single to multiple node scenarios with minor administration effort. This pay as you grow strategy reduces initial CAPEX, distributing the investment costs through time and relating those costs with business revenues and growth.

AGORA-NG may be split into different process bundles (packs) defined by their features. These bundles are tightly coupled by the set of fault, performance and provisioning operations:

- **Database bundle** refers to the Oracle Database module. It is accessed by all other modules and, therefore, its resource needs are tightly coupled to the total volume of fault, performance and provisioning operations.
- **Fault bundle** refers to network events handling modules and suffers little impact from provisioning operations. Resource needs are mostly related to the equivalent network size.
- **Performance bundle** includes modules that are decoupled from both provisioning operations and fault events. Resource needs are uniquely related to the equivalent network size.
- **Provisioning bundle** includes provisioning and inventory operations and its resource needs are tightly coupled to the number of users and concurrent operations.

Single Server

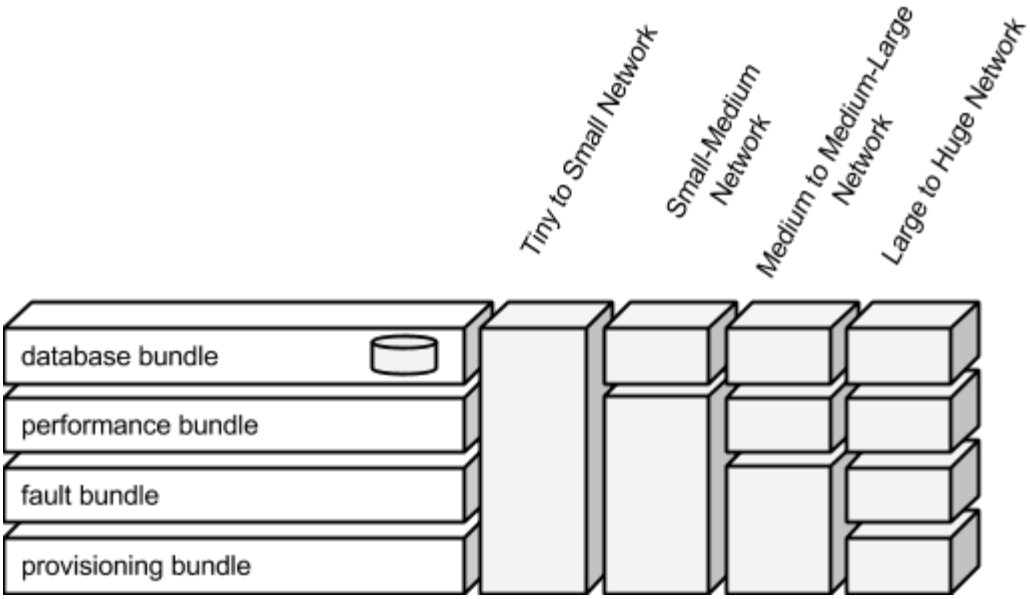
In the single server mode all AGORA-NG bundles are installed in the same node (server). This approach is usually recommended for small to medium scale networks and it may be later upgraded to a multiple node scenario (distributed server).

Distributed Server

In the distributed server mode AGORA-NG bundles may be deployed in different servers reducing the load on each server and ensuring a higher isolation between applications. From a logical perspective all servers belonging to this distributed group behave as a single AGORA-NG instance server.

The following diagram shows the mapping between the expected network size and the division of the bundles between servers.

Figure 15: Application bundles mapping



There are four possible deployment scenarios according to the network size classification:

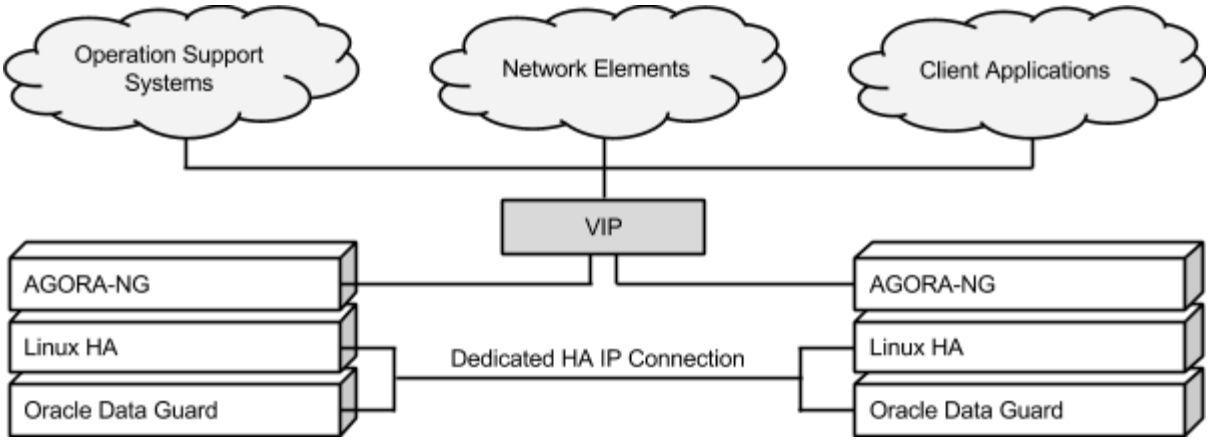
- **tiny to small networks** may be deployed on a single server without compromising management performance and responsiveness expectations.
- **small-medium networks** should be deployed on two servers. Database should have a dedicated server while all other bundles should be executed on a second dedicated server.
- **medium to medium-large networks** should be deployed on three servers. Database and performance bundles should have a dedicated server each. Fault and provisioning bundles may share the same server.
- **large to huge networks** should have one dedicated server per bundle.

High Availability

While selecting the right deployment scenario may improve the performance and responsiveness of the management system, improving the management platform availability requires additional planning.

AGORA-NG suite provides a high availability solution that relies on the Linux-HA project for automatic management system switchover and Oracle Data Guard for active/standby database configuration since it provides continuous synchronization from the active to the standby database.

Figure 16: Redundancy setup



High availability deployment scenarios are flexible enough to have the master and slave sites working in different deployment modes.

Master site may be deployed using a higher hardware specifications than the slave site. This helps reducing hardware costs by trading off performance and responsiveness while the service is assured by the slave site. As an example, the Master site can be composed of 4 distinct servers (one for each application bundle), while the Slave site can be a single server. Although unbalanced, this configuration reduces CAPEX trading cost per performance and assumes that a Slave site exists mainly for temporary situations (maintenance, malfunctions or disasters). Normal operation should be resumed as quickly as possible.

Application High Availability and Disaster Recovery

In a high availability deployment scenario, AGORA-NG services are exposed using a virtual IP address that is independent of the active server. Linux-HA “corosync” and “pacemaker” project processes work together in order to restore a fully working system without any impact on the network configuration. Corosync is used as a heartbeat protocol that detects system failure and triggers services start-up through pacemaker.

The deployment of the solution requires the installation of two sites that may be geographically separated. However, both sites must be known to outer systems using the same virtual IP address. This requirement allows the system to switchover transparently without requiring any additional configuration of the network elements, third party systems or client applications. The whole process is therefore transparent for everything outside the management platform scope.

Virtual IP address will be configured only on the active server. When a server switches from active to standby, the virtual IP address is removed, and on the other server it is done exactly the opposite.

Besides the virtual IP address both sites must be connected through a dedicated, inter-site HA IP connection used to detect system failures. The network connection between sites must be reliable and with low latency to prevent unnecessary switchovers. On a failover scenario, if DBs are not sync, data will be lost.

Database High Availability Architectures

AGORA-NG delegates all database related issues to the Oracle Database processes. This includes database high availability.

Oracle offers several high availability options[3], AGORA-NG a default solution is based on Oracle Database with Oracle Data Guard[4].

Deploying the management infrastructure

The previous section has introduced several definitions and principles necessary for the proper planning of the management platform for AGORA-NG.

To achieve the best performance of AGORA-NG a few pre-requisites are required. These requirements must be considered when preparing the server platform and the network and before the AGORA-NG installation and deployment.

The network class size if obtained using the number of manageable equipment as well as their type, the expected capacity for event handling and the expected concurrent operations capacity.

The physical architecture for each network class size is recommended considering the expected network growth.

Based on the previously options, the recommended HW and SW characteristics are now presented.

Hardware requirements

AGORA-NG server hardware general requirements are identified in the next table.

[3] http://docs.oracle.com/cd/E25054_01/server.1111/e17157/architectures.htm
[4] http://docs.oracle.com/cd/E25054_01/server.1111/e17157/architectures.htm#autoId6

Table 12: AGORA-NG Server HW requirements

Requirement	Description
CPU	Intel Xeon based server min 1x6 Core
RAM	8Gb to 64Gb depending on the manageable network size
HDD	Above 100Gb of disk capacity. (the total necessary capacity depends on the number of managed elements and the log expected capacity)
HDD protection	To ensure data protection a RAID system is recommended but not mandatory. The specific type of RAID and the number of used HDD depends on scenario and customer needs.
Net 1	100/1000Gbps Ethernet adapter for interconnection with the manageable network (and optional also with the users network)
Net 2	Optional 100/1000Gbps Ethernet adapter for isolation of both users and equipments networks

The table shows minimal requirements for CPU, RAM and HDD. These are the most scale dependent resources.

AGORA-NG best performance is currently achieved by using, at least, Intel Xeon E5 processors. Other processor types may be used but will require additional tests.

The size of the network has a direct and strong impact on AGORA-NG performance, therefore the servers must be dimensioned taking the network growth expectations into consideration.

Table 13 shows the server HW requirements (CPU and RAM) for each network class size. The requirements for each application bundle are also included.

This table allows planning the AGORA-NG platform servers, either in a single server configuration (column with Total values), or in a distributed server configuration, considering the requirements for each bundle independently. Combining different bundles is possible resulting in a partial sub-total for the correspondent server.

Table 13: Server HW requirements per network class size

	Database Bundle	Performance Bundle	Fault Bundle	Provisioning Bundle	Total
Tiny	2 CPU 2 GB RAM	1 CPU 2 GB RAM	1 CPU 2 GB RAM	2 CPU 2 GB RAM	6 CPU 8 GB RAM
Small	2 CPU 2 GB RAM	1 CPU 4 GB RAM	1 CPU 2 GB RAM	4 CPU 4 GB RAM	8 CPU 12 GB RAM
Small-Medium	4 CPU 4 GB RAM	2 CPU 8 GB RAM	2 CPU 4 GB RAM	4 CPU 8 GB RAM	12 CPU 24 GB RAM
Medium	4 CPU 8 GB RAM	4 CPU 8 GB RAM	2 CPU 4 GB RAM	6 CPU 12 GB RAM	16 CPU 32 GB RAM
Medium-Large	6 CPU 8 GB RAM	6 CPU 8 GB RAM	4 CPU 4 GB RAM	8 CPU 12 GB RAM	24 CPU 32 GB RAM
Large	6 CPU 16 GB RAM	6 CPU 16 GB RAM	4 CPU 12 GB RAM	8 CPU 20 GB RAM	24 CPU 64 GB RAM
Huge	8 CPU 16 GB RAM	8 CPU 16 GB RAM	6 CPU 12 GB RAM	10 CPU 20 GB RAM	32 CPU 64 GB RAM

AGORA-NG has no strong recommendation on the hardware vendor as long as the abovementioned requirements are met. Nevertheless, the following table displays a list of servers from the CISCO UCS family that may be used as an example.

Table 14: CISCO UCS C-Series Rack Servers

	CISCO UCS C24 M3 Server	**CISCO UCS C240 M3 Server**	**CISCO UCS C460 M4 Server**
Class	SMB/Entry Enterprise	Enterprise	Mission Critical
Processor Family	Intel® Xeon® E5-2400 family	Intel® Xeon® E5-2600 family	Intel® Xeon® E7-4800 v2 or E7-8800 v2 family
Supported Number of Processor Cores	4 - 16	2 - 16	12 – 60
Memory	Max 384 GB	Max 768 GB	Max 6 TB
Single Server Scenario	up to medium networks	up to large networks	up to huge networks

As an example, when deploying a large network we have several options:

1. With a single server solution is chosen then the recommended hardware is:

   Single Server

   CISCO UCS C240 M3 Server

   2x12 CPU

   64 GB RAM

2. With a distributed server solution, using a dedicated server for each of the process bundles (database, performance, fault and provisioning) then the recommended hardware is:

   Database Bundle

   CISCO UCS C240 M3 Server

   1*6 CPU

   16 GB RAM

   Performance Bundle

   CISCO UCS C240 M3 Server

   1*6 CPU

   16 GB RAM

   Fault Bundle

   CISCO UCS C240 M3 Server

   1*4 CPU

12 GB RAM

Provisioning Bundle

CISCO UCS C240 M3 Server

2*4 CPU

20 GB RAM

Software Requirements

AGORA-NG server software requirements are:

- Red-Hat based Linux Operating System with version 6.4 or above (x86_64)
- Oracle Database 11g

The recommended Linux distributions are Red Hat, Oracle Linux or CentOS.

The Oracle database edition will depend on the deployment type:

Table 15: Oracle editions

Oracle Edition	Scenario
Oracle Database Express Edition 11g	Demonstration server
Oracle Database Standard Edition 11g	Small size network with no High-Availability option
Oracle Database Enterprise Edition 11g	Medium to Large size networks High-Availability option

For both the Standard and the Enterprise Editions an update patch is also required:

Oracle Database update 11.2.0.4

If the customer scenario complies a medium to large size network an additional pack should also be required:

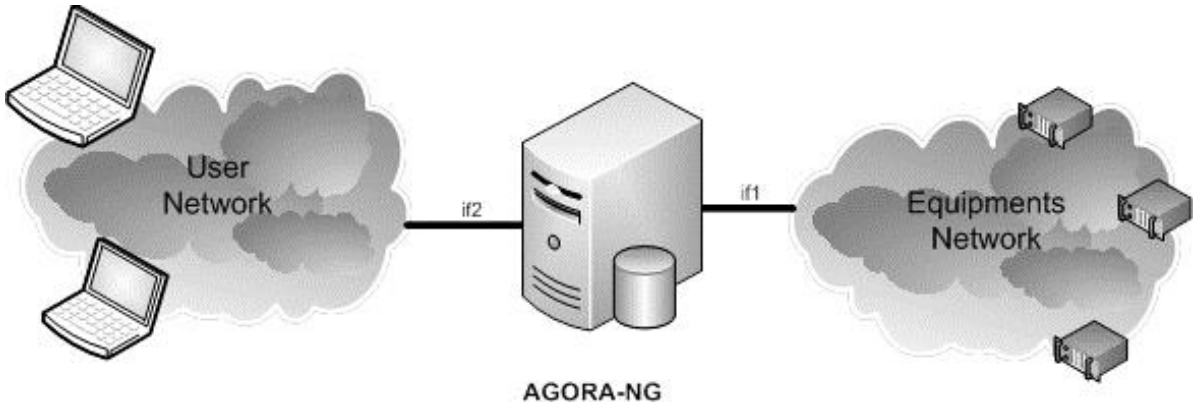
Oracle Database Partitioning Option Pack

Network Requirements

AGORA-NG interacts with both users and the manageable equipment with IP based protocols.

The next figure represents the logical interfaces existing on the AGORA-NG platform.

Figure 17: User and NE network logical interfaces



Although the recommended scenario is to use two physically distinct network adapters and IP interfaces, both if1 and if2 can be a single physical and IP interface.

Figure 18: Intra-Site logical interface

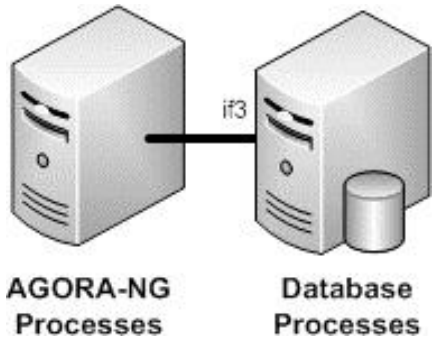


Figure 18 represents the logical interface between co-located servers in a distributed server configuration (see deployment scenarios). This interface (if3) is used internally in the communication between the different components and processes that are part of the entire AGORA-NG solution.

Figure 19: Intra-Cluster logical interface

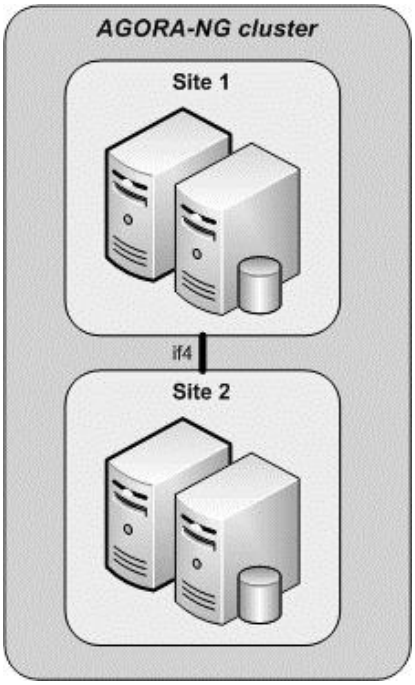


Figure 19 represents the logical interface between two geographical remote sites in a High-Availability configuration (see deployment scenarios). This interface (if4) is used internally in the communication between the different components and processes that ensure the synchronization between both the Master and the Slave sites and ensure the High-Availability protocols.

Table 16: AGORA-NG network interface Requirements

interface	min BW / max. latency	ports/protocols
If1 (network equipments)	1 Mbps / 300 ms	telnet 23/tcp ssh 22/tcp http 80/tcp snmp 161/udp snmp 162/udp ftp 21/udp tftp 69/udp
if2 (users & nbi)	256 Kbps / 300ms	proprietary 1698/tcp proprietary 1699/tcp proprietary 4473/tcp proprietary 5044/tcp proprietary 5045/tcp proprietary 5046/tcp proprietary 8609/tcp proprietary 8680/tcp proprietary 8683/tcp proprietary 8690/tcp proprietary 8692/tcp proprietary 8693/tcp proprietary 5057/tcp proprietary 6045/tcp proprietary 6055/tcp http 8080/tcp http 8680/tcp http 8880/tcp http 8080/tcp http 8680/tcp http 8880/tcp Snmp 162/udp
if3 (intra-site)	100 Mbps /	all
if4 (high-availability)	10 Mbps /	proprietary 1522/tcp proprietary 8899/udp proprietary 8898/udp

Client Requirements

AGORA-NG client applications are OS independent since they are built with cross-platform standard technologies such as HTTP/HTML web pages and Java swing.

For a better user experience the recommended minimum configuration for the client PC are:

- 1Gb of available RAM;
- Latest generation Web-browser (FF, Chrome, IE9+);
- Min 1280x768 px screen resolution

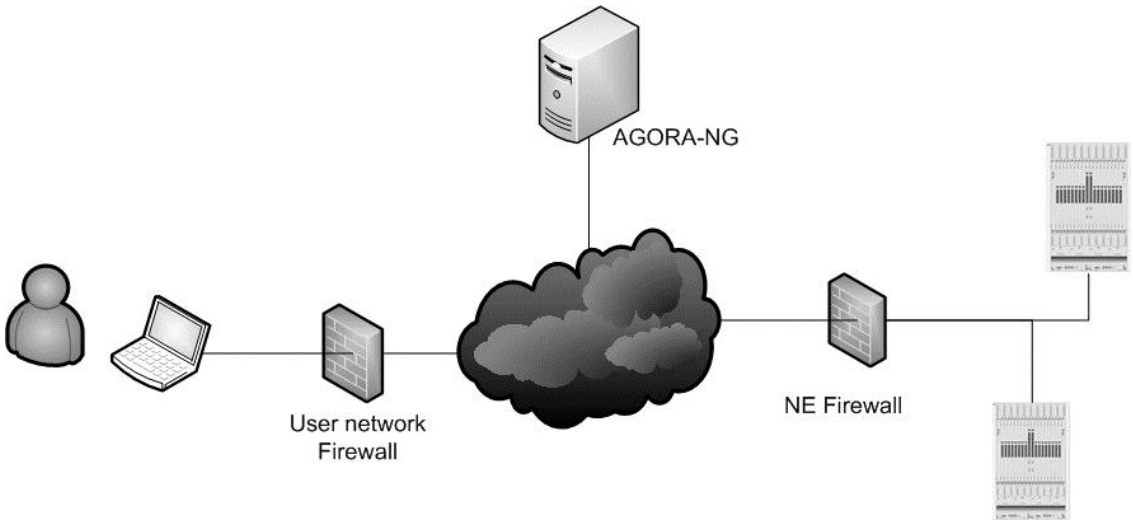
Chapter 4
CONFIGURATION

Prerequisites

Data Communication Network

The Management Communications Network has a structure similar to that shown in next figure.

Figure 20. Data Communications Network



The ports that must be opened in both firewalls are listed in the following tables.

Table 17: Used ports per module – user firewall

Module	TCP Ports
Portal (offset 600)	1698, 1699, 4473, 5044-5046, 8609, 8680, 8683, 8690, 8692, 8693, 5057, 6045, 6055
assurepack (jboss offset 800)	1898, 1899, 4673, 5244-5246, 8809, 8880, 8883, 8890, 8892, 8893, 5257, 6245, 6255
Apache Web server	8080

Table 18: Clustering used ports – NE firewall

Module	Ports
SNMP	UDP 161, 162
FTP, SSH, Telnet, http, TFTP	TCP 21, 22, 23, 80, 69

In case of using clustering:

Table 19: Clustering used ports – user firewall

Module	Portos TCP ports
Portal (offset 600)	1700-1702, 1761, 1762, 4158, 5047, 5048, 49752, 49753
assurepack (jboss offset 800)	1900-1902, 1961, 1962, 4358, 5247, 5248, 49952, 49953

Software

Before installing AGORA-NG it is necessary to ensure the installation of some external software packages. It is assumed the use of RHEL, CentOS or Oracle Linux operating system.

- JDK 1.6_0_*
- Apache 2.*
- Oracle 11g (any Edition)
- ProcMail
- tftp (this aplication belongs to Xinetd for the above menthioned OS)
- vsftp

Java and Jboss installation

Java and Jboss may be installed in two distinct ways:

a) YUM - this method should be used when the machine where the installation is performed has access to aYUM server;

b) RPM - this method should be used when the machine where the installation is performed does not have access to a YUM server.

In order to check if there is connectivity with a YUM server, access http://"yum server URL"/repo address and check if a page with a file list is shown.

In order to increase the application servers Jboss 5.1 with HornetQ under Linux, performance, it is advisable to install the Linux-native asynchronous I/O access library libaio.

Installation through YUM

It is necessary to install the next configuration files from the YUM repositories:

http://"yum server URL"/repo/ext-mirror-java-sun-1.6.repo	**jdk6**
http:// "yum server URL"/repo/ext-generic.repo	**JBOSS AS 5.1 hornetQ**

Install Jdk and Jboss in the following order in order to prevent problems with the jdk version.

$ yum install jdk-sun-1.6.2
$ yum install jboss-jdk6-5.1.0
$ yum install jboss-hornetq2.1.2-jdk6-5.1.0

RPM installation

This installation method requires that the Service Provider make RPM files available.

It is possible to obtain these files using the following commands:

Perform the RPMs download replacing the 'X' with the most current version available in the repository. A list of the available versions can be obtained by accessing the browser address where the file is located.

$ wget http://"yum server URL"/repo/ext-mirror/java/sun/1.6/x86_64/jdk-6uX-linux-amd64.rpm
$ wget http://"yum server URL"/repo/ext-generic/el5/x86_64/sun-jdk-1.6.0_X.ptin.el5.x86_64.rpm
$ wget http://"yum server URL"/repo/ext-generic/el5/x86_64/jboss-jdk6-5.1.0-X.ptin.el5.noarch.rpm
$ wget http://"yum server URL"/repo/ext-generic/el5/x86_64/jboss-hornetq2.1.2-jdk6-5.1.0-X.ptin.el5.noarch.rpm

After the RPMs availability it is possible to install them using the following commands:

$ rpm -i jdk-6uX-linux-amd64.rpm
$ rpm -i sun-jdk-1.6.0_X.ptin.el5.x86_64.rpm
$ rpm -i jboss-jdk6-5.1.0-X.ptin.el5.noarch.rpm
$ rpm -i jboss-hornetq2.1.2-jdk6-5.1.0-X.ptin.el5.noarch.rpm

Oracle 11g

The appropriate Oracle 11g version should be installed according with the Oracle [1] manual.

Oracle instance

In the case of Oracle 11g version set the "SEC_CASE_SENSITIVE_LOGON" parameter to "FALSE" in order that is not logon case sensitive, and disable "password expiration".

These requirements can go against the clients security rules. If they are not implemented it is necessary to take this into account in DB instance connection configurations.

```
$ rpm -i jdk-6uX-linux-amd64.rpm
$ rpm -i sun-jdk-1.6.0_X.ptin.el5.x86_64.rpm
$ rpm -i jboss-jdk6-5.1.0-X.ptin.el5.noarch.rpm
$ rpm -i jboss-hornetq2.1.2-jdk6-5.1.0-X.ptin.el5.noarch.rpm
```

Access to the entire network (Network Access - Disable ACL). This has to be done at least for the application machines communication network.

```
begin
  begin
    dbms_network_acl_admin.drop_acl(
      acl => 'all-network-PUBLIC.xml'
    );
  exception
    when others then null;
  end;
  dbms_network_acl_admin.create_acl(
    acl => 'all-network-PUBLIC.xml',
    description => 'Network connects for all',
    principal => 'PUBLIC',
    is_grant => true,
    privilege => 'connect'
  );
  DBMS_NETWORK_ACL_ADMIN.ADD_PRIVILEGE(
    acl => 'all-network-PUBLIC.xml',
    principal => 'PUBLIC',
    is_grant => true,
    privilege => 'resolve'
  );
  dbms_network_acl_admin.assign_acl(
    acl => 'all-network-PUBLIC.xml',
    host => '*'
  );
end;
/
commit;
```

In case Oracle XE assigns "GRANT EXECUTE ON <package> TO PUBLIC" or to every created user by the following internal packages:

```
# to the AGORA-NG user
```

STANDARD
UTL_FILE
UTL_TCP
 # to the SCA user
UTL_SMTP
UTL_HTTP (v4.5.0 do sca)

Check, change instance parameters (instance user system):

- open cursors = 900
- sessions = 900
- process = 600

Show command:

- "show parameter <parameter>"

Change command:

- "alter system set <parameter> = <value> scope = spfile;"

Shutdown and startup in order that new values are enabled:

- shutdown immediate
- startup

Apache

It is necessary to modify the "/etc/httpd/conf/httpd.conf" file and:

Configure user and group:

User agorang
Group jboss

Configure timeout:

Timeout 900

Configure DocumentRoot:

DocumentRoot "/opt/ptin/agorang/share/www"

and

<Directory "/opt/ptin/agorang/share/www">

Configure Listen:

```
Listen 8080
Listen 8081
```

Configure mod_proxy adding and adapting the following lines:

```
<IfModule mod_proxy.c>
<Proxy *>
  Order deny,allow
  Deny from all
  Allow from all
</Proxy>

ProxyRequests Off
ProxyPreserveHost On
ProxyReceiveBufferSize 8048
ProxyTimeout 7200

ProxyPass /JobScheduler http://hostname:8880/JobScheduler
ProxyPassReverse /JobScheduler http://hostname:8880/JobScheduler

ProxyPass /Portal http://hostname:8680/Portal
ProxyPassReverse /Portal http://hostname:8680/Portal

ProxyPass /plrelatorios http://hostname:8380/plrelatorios
ProxyPassReverse /plrelatorios http://hostname:8380/plrelatorios

ProxyPass /servletGateway http://hostname:8680/servletGateway
ProxyPassReverse /servletGateway http://hostname:8680/servletGateway

ProxyPass /sca http://hostname:8680/sca
ProxyPassReverse /sca http://hostname:8680/sca

ProxyPass /alarmmanagerlaunch http://hostname:8680/alarmmanagerlaunch
ProxyPassReverse /alarmmanagerlaunch http://hostname:8680/alarmmanagerlaunch

ProxyPass /assurepacklaunch http://hostname:8680/assurepacklaunch
ProxyPassReverse /assurepacklaunch http://hostname:8680/assurepacklaunch

ProxyPass /ejap http://hostname:8630/ejap
ProxyPassReverse /ejap http://hostname:8630/ejap

ProxyPass /AlarmMgrRepSearch http://hostname:8630/AlarmMgrRepSearch
ProxyPassReverse /AlarmMgrRepSearch http://hostname:8630/AlarmMgrRepSearch

ProxyPass /provisionPackEla http://hostname:8330/provisionPackEla
ProxyPassReverse /provisionPackEla http://hostname:8330/provisionPackEla

ProxyPass /provisionPackNx64 http://hostname:8280/provisionPackNx64
ProxyPassReverse /provisionPackNx64 http://hostname:8280/provisionPackNx64

ProxyPass /provisionPackSdh http://hostname:8230/provisionPackSdh
```

```
ProxyPassReverse /provisionPackSdh http://hostname:8230/provisionPackSdh

ProxyPass /provisionPackAtm http://hostname:8180/provisionPackAtm
ProxyPassReverse /provisionPackAtm http://hostname:8180/provisionPackAtm
</IfModule>
```

Configure ERROR

```
Alias /error/ "/opt/ptin/agorang/share/www/errors/"

<IfModule mod_negotiation.c>
<IfModule mod_include.c>
<Directory "/opt/ptin/agorang/share/www/errors">
AllowOverride None
Options IncludesNoExec
AddOutputFilter Includes html
AddHandler type-map var
Order allow,deny
Allow from all
LanguagePriority en es de fr
ForceLanguagePriority Prefer Fallback
</Directory>
```

Uncomment ErrorDocument 404, 502, 503

Configure Virtual Host

```
<VirtualHost *:8081>
DocumentRoot /opt/ptin/agorang/data/na-lite
</VirtualHost>
<Directory "/opt/ptin/agorang/data/na-lite/repository/firmware">
Options Indexes FollowSymLinks
 IndexOptions NameWidth=* FancyIndexing VersionSort XHTML SuppressIcon
SuppressColumnSorting SuppressDescription SuppressHTMLPreamble SuppressLastModified
SuppressRules SuppressSize
</Directory>
```

Recall

Restart Apache:

```
$ su - -c "service httpd restart"
```

Note: This command may return an error if some of the ports are already being used or the user and group have not yet been created. This may happen in a base installation.

Check automatic start:

$ su - -c "chkconfig --list httpd"

Note: Runlevel 2, 3, 4, 5 must be “on”

Set service to automatic start:

$ su - -c "chkconfig httpd on"

Set tftp file:

This <"/etc/xinetd.d/tftp"> file must have the directory configured to <"/opt/ptin/agorang/data/downloads">

Installation

Complete installation steps

Step 1

Install the Operational System (OS) with specific file systems or in a generic way. Include if possible, the most part of the needed OS basic software, e.g. apache, mysql, tftp,…

At the OS level if a specific file system is used:

- /opt/ptin
- /u01/app
- /logs
- /oradata
- /oraback
- /oraarch
- /desempenho

Otherwise if a generic file system is used it is necessary to create the previous structure.

In the “/oradata”, “/oraback” and “/oraarch” directories it is necessary to create a directory with the intended instance name (8 characters). This is the SID that will be used in the creation.

Step 2

Install Oracle database software, previously checking the OS level Oracle prerequisites.

Step 3

Create a reference points database instance (dbca):

- Select “Custom Database”
- Global Database Name and SID = [AGORABD] (may be another name, maximum 8 characters)
- Disable “Configure Enterprise manager”
- Select “Use the Same Administrative Password for All Accounts”
- Select “Use Common Location for All Database Files” and place “/oradata”
- Uncheck Fast Recovery Area
- Select “Enable Archiving” and enter in “Edit Archive Mode Parameters…”
    - Change in “Archive Log File Format” the “dbf” extension to “arc”
    - In the grid first position place “/oraarch/SID”
- Disable all options
- Select Custom in Memory
    - Minimum values SGA=1024 PGA=640
- Sizing, increase “Processes” to 600 (this value may be changed after creation)
- Character Sets
    - Database Character Set = “WE8ISO8859P15 – ISSO 8859-15 West European”
    - Default Language = “Portuguese”
    - Default Territory = “Portugal” or “Brazil”
- Change the “Redo Log Groups” size from 51200K to 102400K

Change the parameters after the instance creation.

Step 4

Install Assurepack base RPMs. The “database” RPM can be installed after the first global configurations and also after the database schemas have been created.

Step 5

Install RPM “database”. Complete schemas.

Step 6

Place the other products (AlarmMonitor, Mediator, ….).

Installation packages

Assure Pack

AGORA-NG Assure Pack is comprised by a module set whose installation depend on the intended scenario.

Table 20: AssurePack modules

Package	Type	Description	Where to install
agorang-ap-lib	RPM	Base package of any other system package. Includes start/stop scripts.	All machines.
agorang-ap-client	RPM	JBoss app with frontend.	Frontend machines.
agorang-ap	RPM	JBoss app with core services.	Backend machine, with DB access.
agorang-database	RPM	Scripts for creating and updating the data model. PL-SQL packages.	Machine with DB access, with sqlplus, preferably the same of agorang-ap.
agorang-static-common-repo	RPM	Static content available in the GUI, such as maps and pictures.	Frontend machines.
agorang-alarmMonitorGw	RPM	Communication modules with Alarm Monitor.	Machine with DB access, with sqlplus, preferably the same of agorang-ap.

Alarm Monitor

Table 21: Alarm Monitor module

Package	Type	Description	Where to install
Alarm Manager	See Alarm Monitor section	Alarms management module.	DB access.

SCA

Table 22: SCA module

Package	Type	Description	Where to install
SCA	JAR	Accesses control system.	DB access.

Reports

Table 23: Reports modules

Package	Type	Description	Where to install
agorang-reports	RPM	Reports component integration	Reports machine
agorang-reports-database	RPM	Reports component integration (pl-sql component)	Reports machine

QoS Collector

Table 24: QoS Collector modules

Package	Type	Description	Where to install
agorang-qoscollector **agorang-qoscollector-database**	RPM	QoS Collector component integration.	Performance data collecting machine.
agorang-qoscollector-udp	RPM	QoS Collector component integration – data collecting via UDP.	Performance data collecting via proprietary protocol (legacy equipments).

Provision Pack

Table 25: Provision Pack modules

Package	Type	Description	Where to install
agorang-pce	RPM	Base package of any other system package. Includes start/stop scripts.	All the machines
agorang-pce-database	RPM	JBoss app with frontend	Frontend machines
agorang-ppXYZ	RPM	JBoss app with frontend	Frontend machines
agorang-ppXYZ-database	RPM	JBoss app with frontend	Frontend machines

Northbound Alarms Interface (optional)

Table 26: Northbound Alarms Interface module

Package	Type	Description	Where to install
agorang-nb-alarm-interface	RPM	Enables alarm forwarding to external systems.	Machine where agorang-alarmMonitorGw is installed.

Northbound Inventory Interface (optional)

Table 27: Northbound Inventory Interface module

Package	Type	Description	Where to install
agorang-nb-inventory-interface	RPM	Registration interface for external systems consultation	Machine where agorang-ap is installed.

Northbound GPON Interface (optional)

Table 28: Northbound GPON Interface module

Package	Type	Description	Where to install
agorang-nb-gpon-interface	RPM	GPON provisioning and diagnostics interface, by external systems.	Machine where agorang-ap is installed.

Northbound DSL Interface (optional)

Table 29: Northbound DSL Interface module

Package	Type	Description	Where to install
agorang-nb-dsl-interface	RPM	DSL diagnostic interface, by external systems.	Machine where agorang-ap is installed.

Installation procedures

YUM installation

AGORA-NG RPMs are not yet available through YUM.

RPM installation

The RPM installation packages are installed/updated by the operating system tool.

 # rpm -Uvh ...

Manual installation

Some of the modules can only be manually installed. The installation instructions are described in the next sections.

Alarm Monitor

In order to install the Alarm Monitor component, follow the next steps:

- Create alarmmon user

 # useradd -g ptin -d /opt/ptin/alarmmon -m -s /bin/bash -G jboss alarmmon

- Open the jboss-4.2.3.GA-jdk6 compacted file and place it in /opt/jboss/
- Copy Alarm_Monitor packet to /opt/ptin/alarmmon/
- Update the files owner in /opt/ptin/alarmmon/ (as root user):

 # chown -R alarmmon:ptin
 # chown alarmmon:ptin .var_env_*

- In /opt/ptin/alarmmon/lib/ insert/replace the JDBC ojdbc* drivers with the correct version of the SQL_Client installed in the machine
- In /opt/ptin/alarmmon/lib/ insert/replace the sca.jar newest version of the installed SCA
- Create the directories structure for the logs and symbolic links:

 # mkdir /logs/ptin/alarmmon
 # mkdir /logs/ptin/alarmmon/alarmmonitor
 # ln -s /logs/ptin/alarmmon/alarmmonitor /opt/ptin/alarmmon/jboss-server/alarmmonitor/log
 # ln -s /opt/ptin/alarmmon/lib/sca.jar /opt/ptin/alarmmon/jboss-server/alarmmonitor/lib/sca.jar
 # ln -s /opt/ptin/alarmmon/lib/ojdbc6.jar /opt/ptin/alarmmon/jboss-server/alarmmonitor/lib/ojdbc6.jar
 # ln -s /logs/ptin/alarmmon /opt/ptin/alarmmon/logs

- Edit .bash_profile file and insert the .var_env_jboss and .var_env_oracle entries.

Configure/check the configuration files related with this module.

SCA

SCA installation is made by copying the following two files to specific locations.

Table 30: SCA installation files

File	Destination
sca.jar	~/lib
sca.war	~/share/portal/deploy/app

sudo configuration

Add the next line into the sudoers file:

agorang ALL=NOPASSWD:/opt/ptin/agorang/etc/init.d/agorangctrl

 # vi /etc/sudoers

License

Ensure that the license is available in conf/ap-configuration/conf.jar/xlic.lic file.

DB schemas update

In the sqlplus execute the files shown in the next table by the order shown.

The following scripts are alternatives, depending on whether or not is intended to use partitioning.

Passo02-AppGestor-tabelasBase-ComPartitioning.sql

AMschema/Passo02-AppGestor-tabelasBase-ComPartitioning.sql

Passo02-AppGestor-tabelasBase-SemPartitioning.sql

AMschema/Passo02-AppGestor-tabelasBase-SemPartitioning.sql

In each step is indicated the DB user where the sql file should run.

Invoke the sqlplus utility, enter the user name and password and run the file,

 # vi /etc/sudoers

Table 31: Database schemas update files

sql File	User DB
Passo01-system-tablespaces_users.sql Passo01-system-tablespaces_users.sql (*) of AM	SYSTEM
Passo02a-AppGestor-tabelasBase-ComPartitioning.sql Passo02b-AppGestor-tabelasBase-SemPartitioning.sql	AGORANGGESTOR
Passo03-AppGestor-gera_grants.sql	AGORANGGESTOR
Passo03-AppGestor-grants.sql (This file has been created in the previous step)	AGORANGGESTOR
Passo04-App-gera_sinonimos.sql	AGORANGGESTOR
Passo04-App-sinonimos.sql (This file has been created in the previous step)	AGORANG
Passo05-App-prePreenchidos.sql	AGORANG
Passo06-PGrafGestor-tabelasBase.sql	PGRAFGESTOR
Passo07-PGrafGestor-gera_grants.sql	PGRAFGESTOR
Passo08-PGraf-gera_sinonimos.sql	PGRAF
Passo08-PGraf-sinonimos.sql (This file has been created in the previous step)	PGRAF
Passo09-AppGestor-CriaDirectorio.sql	AGORANGGESTOR
Passo02-AppGestor-schema-integracao_agorang_ComPartitioning.sql Passo02-AppGestor-schema-integracao_agorang_SemPartitioning.sql	AGJ2GESTOR
Passo03-AppGestor-gera_grants.sql	AGJ2GESTOR
Passo03-AppGestor-grants.sql (This file has been created in the previous step)	AGJ2GESTOR
Passo04-App-gera_sinonimos.sql	AGJ2
Passo04-App-sinonimos.sql (This file has been created in the previous step)	AGJ2
Passo05-App-prepreenchidos-integracao_agorang.sql	AGJ2
Passo06-App-schema-integracao_agorang.sql	AGJ2
step1_SYSTEM_install_tablespaces.sql	SYSTEM
step2_SYSTEM_create_users.sql	SYSTEM
step3_AppGestor_gestor_schema.sql	SCA_GESTOR
step4_AppGestor_insert_prePreenchidos.sql	SCA_GESTOR
step5_AppGestor_cliente_schema.sql	SCA_GESTOR
step6_AppGestor_job_remove_sessions	SCA_GESTOR
step7_AppGestor_job_clean_log_tables.sql	SCA_GESTOR
step8_AppGestor_job_sync_ldap_users.sql	SCA_GESTOR

step9_AppGestor_job_update_acronyms.sql	SCA_GESTOR

PL-SQL procedures update

Install PL-SQL packages using the next command:

 # dbtools ~/src/database/plsql

When requested, the schema manager user, the schema user (client) and their passwords must be entered.

User owner (AppGestor): <agoranggestor>
Password: <pwd_agoranggestor>

User (App): <agorang>
Password: <pwd_agorang>

In case of script execution success the result is as shown below.

Compiling schema...

PL/SQL procedure successfully completed.

Checking if there is any invalid package...

no rows selected

Upgrade

RPM installation

Install RPMs using the command referred in “RPM installation” section.

The system will output an installation result like the example shown below.

```
Preparing...                ########################################### [100%]
   1:agorang-ap-lib         warning: /opt/ptin/agorang/conf/agorang.cfg created as
/opt/ptin/agorang/conf/agorang.cfg.rpmnew
########################################### [ 14%]
Fixing permissions
   2:agorang-static-common-r########################################### [ 29%]
   3:agorang-ap-client      ########################################### [ 43%]
   4:agorang-alarmMonitorGW ########################################### [ 57%]
```

```
   5:agorang-ap          ############################################ [ 71%]
/var/tmp/rpm-tmp.89499: line 29: fg: no job control
   6:agorang-database    ############################################ [ 86%]
Connected to jdbc:oracle:thin:@itanium:1521:AGORANG
/opt/ptin/agorang/src/database/schemas/6.2.0/28-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/29-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/30-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/31-defines.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/32-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/33-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/34-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/35-AS-ScaGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/36-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/37-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/38-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/39-AS-AppGestor.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/39-defines.sql
/opt/ptin/agorang/src/database/schemas/6.2.0/40-AS-AppGestor.sql
Number of database schema files that should be run: 14
   7:agorang-lightpad    ############################################ [100%]
```

Configurations Update

The warning lines in the previous section (line 3 of the previous example) indicate that a configuration file has its structure changed in this version, but not superimposed because the former has already been customized in this platform.

The user should compare the original file with the new file (saved as *.rpmnew) and decide whether to remove the old, remove the new or merge both. The same should be done when the warning is related with the rpmsave extension, where the former has been saved with this extension and the new has been put into use.

The RPMs update process also indicates a list of scripts for updating the database that should run sequentially and manually in the DB. With the agorang operating system user, sqlplus tool should start with DB user suited to run each script.

- AppGestor – login/pass: agoranggestor/agorang
- PGrafGestor – login/pass: pgrafgestor/pgraf
- SCA – login/pass: sca_gestor/sca_cliente
- Alarm Monitor – login/pass: agj2gestor/agj2

Access schemas directory (cd src/database/schemas/6.2.0/) and execute the following command:

“sqlplus agoranggestor” (pass: agoranggestor)

a) In SQL update the DB executing in order each of the indicated schemas whem RPMs have been installed. Eg: “@10_AS_AppGestor.sql”;

b) After each schema execution end the commit command must be executed: “commit;”;

Lastly, it is necessary to recompile the PL-SQL packages.

a) In the plsql directory (cd src/database/plsql), execute the “dbtools .” command (login/pass AppGestor: agoranggestor; login/pass App: agorang).

Administration

Configurations

Due to packets installation, several configuration files which are located in the agorang user $HOME, must be checked and set.

Each file has their own configuration instructions.

Table 32: Configuration files

File	Description
~/.agorang/agorang	Setting environment variables used by AGORANG
~/.agorang/oracle	Setting environment variables used by Oracle tools
~/.agorang/tnsnames.ora	Settings for oracle DB access via sqlplus
~/conf/agorang.cfg	agorangctrl settings
~/conf/apClientManager.properties	SCA access module specific settings
~/conf/alarmMonitorGW/conf/jndi/beanLocations Config.properties	AM access settings
~/conf/alarmMonitorGW/conf/config.properties	alarmprocessorgw and statemachinegw specific settings
~/conf/portal-configuration/conf.jar/properties/*.properties	Portal specific settings
~/conf/ap-configuration/conf.jar/jobscheduler.properties	Schedules
~/conf/portal-configuration/conf.jar/conf/jndi/beanLocationsConfig.properties	Alarm Monitor access settings
~/conf/portal-configuration/conf.jar/jnlp-ap-system.properties	AP client settings
~/conf/portal-configuration/conf.jar/conf/jndi/beanLocationsConfig.properties	Portal access settings
~/conf/000-configuration/conf.jar/*-jndi.properties	AP access settings
~/conf/000-configuration/conf.jar/*.properties	AP services internal settings
~/share/www/documentation//.html	HTML pages for documentation customization, warnings, etc.
~/share/www/Mapas/	Images available for Assure Pack windows background

The following sections provide module specific configuration files.

Alarm Monitor

Alarm Monitor module specific configuration files are located in the agorang user $HOME.

Table 33: Alarm monitor configuration files

File	Description
~/conf/alarmmonitor/datasources	datasources settings
~/conf/alarmmonitor/properties	specific settings

Mediator

Mediator module specific configuration files are located in the agorang user $HOME.

Table 34: Network Gateway configuration file

File	Description
~/conf/mediator	Host settings (HOST_IP)

Reports

Reports module specific configuration files are located in the agorang user $HOME.

Table 35: Reports configuration file

File	Description
~/conf/000-configuration/conf.jar/reports.properties	Reports module specific settings.

QoS Collector

QoSCollector module specific configuration files are located in the agorang user $HOME.

Table 36: QoS Collector configuration files

File	Description
~/conf/qoscollector/global/desempenho.properties	global settings
~/conf/qoscollector/global/qoscollector-ds.xml	datasource settings
~/conf/qoscollector/extractor/META-INF/jboss-service.xml	equipments activation settings to collect

Provision Pack

Provision Pack module specific configuration files are located in the agorang user $HOME.

Table 37: Provision Pack configuration file

File	Description
~/conf/000-configuration/conf.jar/resources-ppXYZ.properties	XYZ module specific settings

Northbound Alarms Interface (optional)

Northbound Alarms Interface module specific configuration files are located in the agorang user $HOME.

Table 38: Northbound Alarms Interface configuration file

File	Description
~/conf/nb-alarm-interface/alarms2others.properties	Northbound Alarms Interface module specific settings

Northbound Inventory Interface (optional)

There are no Northbound Inventory Interface module specific configuration files.

However it is necessary to ensure the dbtools utility execution on the ~/share/inventoryXml/lib directory after installing this module.

 # dbtools ~/src/database/plsql/inventoryXml

A cron entry should be added to allow periodic updating of the XML files that describe the registered entities. This entry should run the script:

~/bin/inventory-nb.sh

Northbound GPON Interface (optional)

There are no Northbound GPON Interface module specific configuration files.

Northbound DSL Interface (optional)

There are no Northbound DSL Interface module specific configuration files.

Control service

AGORANG control service is configured in the ~/conf/agorang.cfg file and must be replicated on all platform machines.

A module settings begin with a line with the format [servicename] followed by multiple attributes/values lines with the format attribute=value.

The possible attributes are:

Table 39: Control service

Parameter	Value	Mandatory (default)
Host	hostname or ip where the module is installed	yes
User	User name that is going to start the process	no (agorang)
Depends	List (separated by commas) of the modules from which it depends	no
Dependents	List (separated by commas) of modules that depend on it	no

In order to enable/disable just comment/uncomment the module configuration lines.

Customization

Create a symbolic link in /opt/ptin/agorang/share/www/skins/ to choose the intended background color.

$ ln -s <color> default

In the <color> field is assigned the intended color directory

In ~/share/www/Mapas must be placed the image files that will be available for association with managed domains.

For /opt/ptin/agorang/conf/gui/, should be transferred the icons corresponding to the required customization, according to the next match:

Table 40: Customization files

File	Use
AppLogo100x100.png	Application icon, 100x100 format
iconFavIcon16x16.ico	Application icon, 16x16 format
iconMaxi170x170.png	Application icon, 170x170 format
logoClient.png	Customer Logo, which appears in the Portal header
logoFooter.png	Web Applications Logo footer

mainContainerBottomBackgroundImage.png	Lower range of the Portal applications selection window
ManufacturerLogo.png	Icon of the Assure Pack top left windows
splash.jpg	Splash screen JPEG of the Assure Pack application entry and "About" window

To customize the colors with which Working and Protection of MPLS circuits topology paths underscore is done, the ~/share/www/config/assurePackColors.properties file can be used.

Launching the modules control service

Start agorang control service:

$ sudo ~/etc/init.d/agorangctrl start

Check if agorangctrl is correctly running, executing the next command:

$ agorang status

Launching the application

AGORANG control scripts work in distributed environments where different modules can be run on different machines. This feature allows checking the status and, stop and start the modules, from any machine that has the service properly configured.

After configuration it is possible to use the agorang command in order to manage the several modules status.

$ agorang
usage: agorang [start|stop|restart|status [servicename]]

This command allows performing an operation (start, stop, restart, status) over a specific module or on all modules, in case the servicename parameter is not specified.

Table 41: Application launch parameters

Parameter	Description
Start	Starts the specified module and all modules on which it depends.

Stop	Ends the specified module and all modules that depend on it.
Restart	Ends the specified module and all modules that depend on it. At start up it ensures that all modules which depend on and who depend on it, are started.
Status	Checks if the module is in operation. This command only checks if the process is still active. Does not perform any logic validation on the module correct operation.

There is a special module (keeper) that is responsible for monitoring other modules state. When detects a stopped module, it starts it. So, if it is intended to stop temporarily a module, the keeper should be stopped in advance.

Geographic Redundancy

The clustering system is based on two components. An infrastructure for machines cluster creation itself and a management and resources allocation system. Corosync software plays the first role and Pacemaker software the second.

Corosync and Pacemaker installation

Install the necessary software in the cluster machines.

```
$ yum install -y corosync pacemaker
```

Corosync configuration

Authentication key

Execute 'corosync-keygen' command in one of the machines in order to generate an authentication key. The key is created in '/etc/corosync/authkey'.

```
$ corosync-keygen
```

Copy the '/etc/corosync/authkey' file for the other machines.

Install the authentication key in the other machines.

```
$ install -D --group=0 --owner=0 --mode=0400 /<path_to_authkey>/authkey /etc/corosync/authkey
```

Configuration file

Create the '/etc/corosync/corosync.conf' file in one of the machines with the content described below, and copy it to all other machines (this configuration uses unicast).

```
# disable compatibility with older versions
compatibility: none
totem {
   version: 2
   # Limit generated nodeids to 31-bits (positive signed integers)
   clear_node_high_bit: yes
   # Disable encryption
secauth: off
   # How many threads to use for encryption/decryption
threads: 0
interface {
      # The following values need to be set based on your environment
      ringnumber: 0
      # List of the cluster members IP addresses, change accordingly
      member {
         memberaddr: 192.168.1.1
      }
      member {
         memberaddr: 192.168.1.2
      }
      # network address to bind to. If local interface is 192.168.1.0 mask 255.255.255.0 then this value is
192.168.1.0
      bindnetaddr: 192.168.1.0
      # the port on which to communicate
      mcastport: 5405
   }
# enable unicast
   transport: udpu
}
amf {
   mode: disabled
}
service {
    # Load the Pacemaker Cluster Resource Manager
    name:     pacemaker
    ver:      0
}
aisexec {
      user:   root
      group:  root
}
# log configuration, adjust as needed, currently logging to syslog and file, new everyday with weekly
rotation
logging {
      fileline: off
      to_stderr: no
      to_logfile: yes
      logfile: /var/log/corosync.log {
```

```
            missingok
            compress
            notifyempty
            daily
            rotate 7
            copytruncate
    }
        to_syslog: yes
        syslog_facility: daemon
        debug: off
        timestamp: on
        logger_subsys {
            subsys: AMF
            debug: off
            tags: enter|leave|trace1|trace2|trace3|trace4|trace6
        }
}
```

Firewall configuration for Corosync communication

Corosync uses two UDP ports. The mcastport port and the port immediately below, both specified in the configuration file. In this case 5405 and 5404 ports. Configure this in all machines.

Corosync start up

Corosync is executed as a service. At Corosync start, Pacemaker starts automatically (execute this in all the machines):

```
$ service corosync start
```

Cluster communication check

After Corosync start check in all machines that all member machines IP are present in the next command output:

```
$ corosync-objctl | grep members
```

Pacemaker configuration

Pacemaker is the Cluster Resource Manager (CRM).

Although the setting exists in XML format this should never be manually edited. To configure Pacemaker the 'crm' command should be used. Running without parameters enters into an interactive configuration session. In order to enable scripting it is also possible to make all the settings by passing parameters to the crm command.

The following commands are performed on one machine only, preferably the one intended to be the principal, and the settings are automatically propagated to all cluster member machines using the infrastructure provided by Corosync.

STONITH disable

If there is no STONITH (Shoot The Other Node In The Head) resource available and configured, it is not possible to manage cluster resources without disabling STONITH support.

$ crm configure property stonith-enabled=false

Quorum policy change

A cluster has quorum if half plus one of the machines which are part of the cluster, are in agreement. In a cluster with two machines there is no quorum in case of a failure, but the machines should be able to keep the service active. For this it is necessary to ignore the fact that there is no quorum.

$ crm configure property no-quorum-policy=ignore

Auto-failback disable

In case of failure the resources migrate to the secondary machine.

In order to prevent the resources to migrate immediately to the primary machine as soon as this machine comes back online, it is necessary to indicate that resources should prefer to stay on the machine where they are and specify "how hard" if they want to be kept in the machine where they are.

$ crm configure rsc_defaults resource-stickiness=100

Add resources

Scripts in LSB and OCF formats are resources that can be managed. OCF are preferred because allow parameters passing. An OCF script must support the following actions: 'start'; 'stop'; 'monitor'; and 'meta-data'; and should support the 'validate-all' action.

Consult http://www.linux-ha.org/wiki/OCF_Resource_Agents for detailed information about the OCF resources.

When installing Corosync and Pacemaker several features are installed by the 'cluster-agents' package in '/usr/lib/ocf/resource.d/'. Inside this folder each folder is a resources provider that contains scripts that the provider provides.

If, for example, PTIN creates a script named 'recurso-ptin' obeying OCF rules and want to add it to this cluster, the later must reside in '/usr/lib/ocf/resource.d/ptin/recurso-ptin'.

Resources will be initially available on the machine where they are configured. That machine should be the primary machine, unless preferences for certain machines features are immediately configure. If primary machine fails the resources migrate to the secondary machine. The resources return to the primary machine must be done manually.

Add any resource

The generic syntax to add an existing or created resource and place it in /usr/lib/ocf/resource.d/<nome_do_fornecedor>/<nome_do_script>, is:

$ crm configure primitive nome ocf:fornecedor:script params ... op ...

Table 42: Resources parameters

Parameter	Description
name	Resource intended name
ocf	Resource type (ocf or lsb)
provider	Resource provider (for ocf only, lsb must be located in '/etc/init.d/')
script	Resource initialization script
params	Resource initialization script passing parameters
op	Resource operations

Add an IP address

Add an IP address on which the cluster must provide services. This IP address will pass to the secondary machine when the primary machine goes down.

In the example below the IP is set to 192.168.1.10 with 255.255.255.0 mask on the eth0 physical interface. This IP address will be monitored for 10 to 10 seconds.

$ crm configure primitive cluster-ip ocf:heartbeat:IPaddr params ip="192.168.1.10" cidr_mask="24" nic="eth0" op monitor interval="10s"

Resources relations configuration

Assuming the existence of two resources, an IP address with 'cluster-ip' name and a resource with "servico-generico" name, relationships between these resources can be set up.

Resources dependence

Sets up a 'colocation': a resource can only exist where the other is active. The 'INFINITY' value specifies that another resource has to exist and must be active. If the 'servico-generico' resource is automatically or manually changed, the cluster-ip service will also change to the same machine and vice-versa.

$ crm configure colocation servico-generico-com-ip INFINITY: servico-generico cluster-ip

Services start order forcing

Some services may require others to be started first in order to successfully start. To force an order in this case, 'cluster-ip' runs first and then 'servico-generico' runs after:

$ crm configure order servico-generico-depois-de-ip mandatory: cluster-ip servico-generico

Resources location / manual re-location configuration

Resources location

In order for a resource be preferably located in a machine, Pacemaker should be informed in which machine should place the resource and "how hard":

$ crm configure location prefer-node1 servico-generico 50: node1

In this case a force of 50 is attributed in order that the generic service stays in the machine whose 'uname -n' (hostname) command output is node1. 'prefer-node1' is the name intended for the preference.

Resources manual re-location

To move a resource manually to the machine with 'node1' hostname:

$ crm resource move servico-generico node1

The same 'colocation' services migrate together to the chosen host. This command causes the resource always prefer node1. To eliminate this preference:

$ crm resource unmove servico-generico

Despite the name this command does not returns 'servico-generico' resource to the machine where it was previously located, it only eliminates the preference forced by the node1 machine, and starts respecting the "force" points system to choose the machines.

FAQ

Job Scheduler module unavailability

To contemplate the Job Scheduler module support in upgrade situations, in the SCA is necessary to:

- Create the specific management system, importing the SG_AgoraNG-JobScheduler.xml file;
- Edit "AgorangNMC - Login Manager" Management System, create a new PI, named "jobScheduler" in "Selecção de módulos" profile, with management access type;
- Ensure that the user has AgorangNMC - Login Manager profile with Administrator access.

References

[1] ORACLE_11g_QuickInstallGuide. http://www.oracle.com/pls/db111/portal.portal_db?selected=11

[2] Using JBoss Behind a Firewall. https://community.jboss.org/wiki/UsingJBossBehindAFirewall

Application Management

Summary

This section describes the operation, maintenance, supervision and management tasks for the AGORA-NG application..

This section describes the following topics:

- Application modules:
  - Starting/Stopping the base module (Assure Pack)
  - Starting/Stopping other application modules
- Database:
  - Starting/Stopping the database.
  - Starting/Stopping the listener.
- Clustering Services
  - Starting/Stopping clustering services

The application's starting/stopping processes use shell scripts from the operation system. These are located in the application's owner '$HOME' directory.

The application's starting/stopping processes of the database is similar to that of a unique instance. Any of the following three methods may be used:

- SQL*Plus utility ('sqlplus')

Application location

The various modules are installed depending on client network configuration. The AGORA-NG application is installed in the following base directory:

/opt/ptin/agorang/

Each module installed can be located in:

/opt/ptin/agorang/share/<modules>

Modules
Assure Pack, Provision Pack, Portal, QoS Collect Agent, Alarm Monitor, Reports Module, Performance Module, Control Access System, TL1 Agent, Keeper and Database ([5])

Database location

Oracle 11g Database Release 2 is installed on the following directory:

/opt/app/oracle/product/11.2.0

Datafiles and archives from AGORA-NG application's database are located in:

/oradata/AGORANG or **/oradata/<SID>**

AGORA-NG's Modules and Services

This section details how to stop and start individual modules of the AGORA-NG platform and other application servers integrated into the platform.

Apache (webserver)

Login	root
App Home	/etc/httpd/
Startup on boot	check with: # chkconfig –list httpd
Manual Start	# service httpd start
Manual Stop	# service httpd stop
Verify	# service httpd status
Logs	/var/log/httpd

AGORA-NG Modules

Login	agorang
App Home	/opt/ptin/agorang
Manual Start Module	$ agorang start <module>
Manual Stop Module	$ agorang stop <module>
Global Start	$ agorang start
Global Stop	$ agorang stop
Verify	$ agorang status <module>

[5] The modules installed may differ depending on which pack is acquired.

Logs	/opt/ptin/agorang/logs/<module>

The AGORA-NG modules are identified as follows ([6]):

ap – Assure Pack

portal - Portal

snmpdaemon – SNMP Interface

reports – Reports Module

statemachinegw – NE State Gateway

alarmprocessorgw – Alarm Processor Gateway

nb-alarm-interface – External Alarm Interface

alarmmonitor – Alarm Monitor

mediator – Network Mediator

ppsdh – Provision Pack SDH

ppnx64k – Provision Pack Nx64k

qoscollector – Quality of Service Collector

keeper – AGORA-NG Module Watchdog

tl1agent – Northbound interface for GPON provisioning

ORACLE Database

Manually Starting/Stopping the ORACLE Database (without dataguard)

In order to stop the database, the following steps should be done with the user oracle:

Stop the Listener:

$ lsnrctl stop

Stop the database and put the instance "down":

$ sqlplus /nolog

> connect / as sysdba

> shutdown immediate;

> quit

Or

$ sqlplus / as sysdba

> shutdown immediate;

> quit

[6] The modules installed may differ depending on which pack is acquired.

In order to confirm that the database is down the following command should be issued:

$ ps –efww | grep oracle

In order to start the database, the following steps should be done with the user oracle:

Start the Listener:

$ lsnrctl start

Start the database and put the instance "up":

$ sqlplus /nolog

> connect / as sysdba

> startup;

> quit

Or

$ sqlplus / as sysdba

> startup;

> quit

Verify the listener's status:

$ lsnrctl status

Verify the services associated to the database's instances:

$ lsnrctl services

Manually Starting/Stopping the ORACLE Database (with dataguard)

In order to stop the database, the following steps should be done, in both primary and standby database, with the user oracle:

Stop the Listener:

$ lsnrctl stop

Stop the database and put the instance "down":

$ sqlplus /nolog

> connect / as sysdba

> shutdown immediate;

> quit

Or

$ sqlplus / as sysdba

> shutdown immediate;

> quit

In order to confirm that the database is down the following command should be issued:

$ ps –efww | grep oracle

In order to start the database, the following steps should be done, in both primary and standby database, with the user oracle:

Start the Listener:

$ lsnrctl start

Start the primary database and put the instance "up":

$ sqlplus /nolog

> connect / as sysdba

> startup;

> quit

Or

$ sqlplus / as sysdba

> startup;

> quit

Start the standby database and put the instance "up":

$ sqlplus /nolog

> connect / as sysdba

> startup mount;

> DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT FROM SESSION;

> quit

Or

$ sqlplus / as sysdba

> startup mount;

> DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT FROM SESSION;

> quit

Verify the listener's status:

$ lsnrctl status

Verify the services associated to the database's instances:

$ lsnrctl services

Database logs

The database Oracle 11g registers occurred events in the following file:

/u01/app/oracle/diag/rdbms/<sid>/<SID>/alert/log.xml

Or

/u01/app/oracle/diag/rdbms/<sid>/<SID>/trace/alert_<SID>.log

This file may be searched for errors occurred in the database, namely the most critical (ORA-06xx error family) or where the "ERROR" string occurs, issuing the following commands:

$ grep ORA-06 /u01/oracle/admin/<SID>/bdump/alert_<SID>.log

$ grep –i ERROR /u01/oracle/admin/<SID>/bdump/alert_<SID>.log

The default listener's logs are located in:

$ /u01/app/oracle/diag/tnslsnr/<hostname>/listener/trace/listener.log

Or you can check the location:

$ lsnrctl status

(...)

Listener Parameter File

/ u01/app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora

Listener Log File

/ u01/app/oracle/diag/tnslsnr/alfa/listener/alert/log.xml

(...)

Database backup

The database backups, as well as, the indexes rebuild script are cron jobs:

- The backup runs once a day. This may be checked on the cron table of the backora user:

  [oracle@hostname ~]$ crontab –l

- The indexes rebuild script runs once a week on Sundays at 07h00. This may be checked on the cron table of the oracle user:

  [oracle @hostname ~]$ crontab -l

A daily check should be done in order to confirm that the backup was performed:

[oracle@hostname ~]$ ll /opt/ptin/oracle/logs

AGORA-NG: Manual Global Stop and Start Sequence

This chapter details how to execute a global stop and start of the AGORA-NG Application.

The AGORANG platform without redundancy module, should be stopped in the following order:

1) AGORA-NG: Stop keeper Module
2) AGORA-NG: Global Stop
3) Oracle Database

The AGORANG platform with redundancy module, should be stopped in the following order:

1) AGORA-NG: Stop redundancy module

The AGORANG platform without redundancy module, should be started in the following order:

1) Oracle Database
2) AGORA-NG: Global Start

The AGORANG platform with redundancy module, should be started in the following order:

1) AGORA-NG: Start redundancy module

Global Stop without redundancy

To stop the AGORA-NG platform, please follow the set order as indicated.

- Stop AGORA-NG Watchdog (as user: agorang)

  $ agorang stop keeper

- Stop Global AGORA-NG (as user: agorang)

  $ agorang stop

- Stop Oracle Database (follow instructions in AGORA-NG: Manual Global Stop and Start Sequence)
- Stop WebService

  $ sudo /usr/sbin/httpd stop ([7])

Global Stop with redundancy

- Stop redundancy module

  $service pacemaker stop

[7] If the server is not going to be rebooted, module/service can remain online.

Global Start without redundancy

To execute a global start the AGORA-NG platform, please follow the set order as indicated as before, using the set procedures as indicated in AGORA-NG's Modules and Services.

- Start WebService

  $ sudo /usr/sbin/httpd start ([8])

- Start Oracle Database (follow instructions in AGORA-NG: Manual Global Stop and Start Sequence)
- Start AGORA-NG controller

  $ sudo /opt/ptin/agorang/etc/init.d/agorangctrl status

  $ sudo /opt/ptin/agorang/etc/init.d/agorangctrl start ([9])

  $ sudo /opt/ptin/agorang/etc/init.d/agorangctrl status

- Start Global AGORA-NG (as user: agorang)

  $ agorang start

Global Start with redundancy

- Start redundancy module

  $ service pacemaker start

Log cleaning/maintenance

Cleaning Logs

After stopping the application, if the logs aren't needed they may be deleted.

AGORA-NG modules:

Login	Agorang
App	$ cd /opt/ptin/agorang/logs/<module>
Log elimination	# rm snmpdaemon.log*
Log maintenance with the application running	# cd /opt/ptin/agorang/logs # cp /dev/null <log_file> (this action eliminates the contents of the log file reducing its size. This should be used on files like *.log)

[8] Only execute if module/service has been stopped manually or previous result returns NOK.
[9] Only execute if module/service has been stopped manually or previous result returns NOK.

Chapter 5
OPERATION

Application basic use

Application login

Entering AGORA-NG Portal the user must enter its user name and password. If the data is correctly entered all application modules are displayed.

Figure 21. System Login

To access Assure Pack (AP) application, select the corresponding symbol in the displayed modules list.

Figure 22. AGORA-NG modules selection window

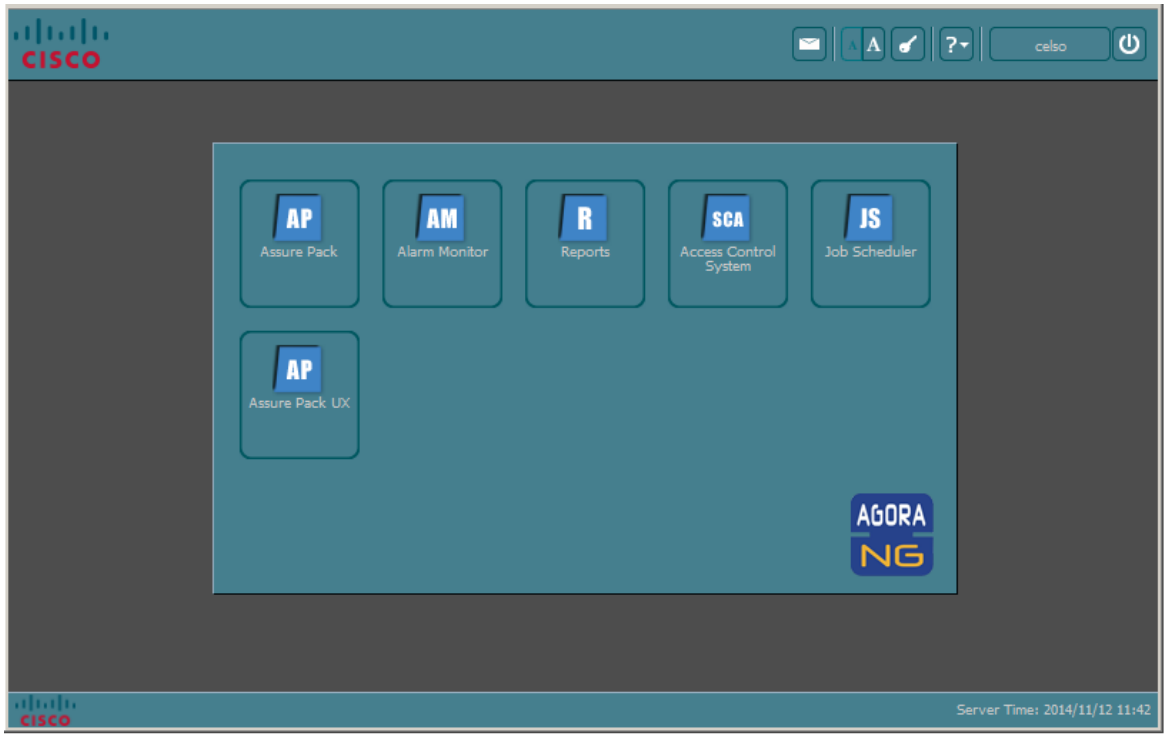
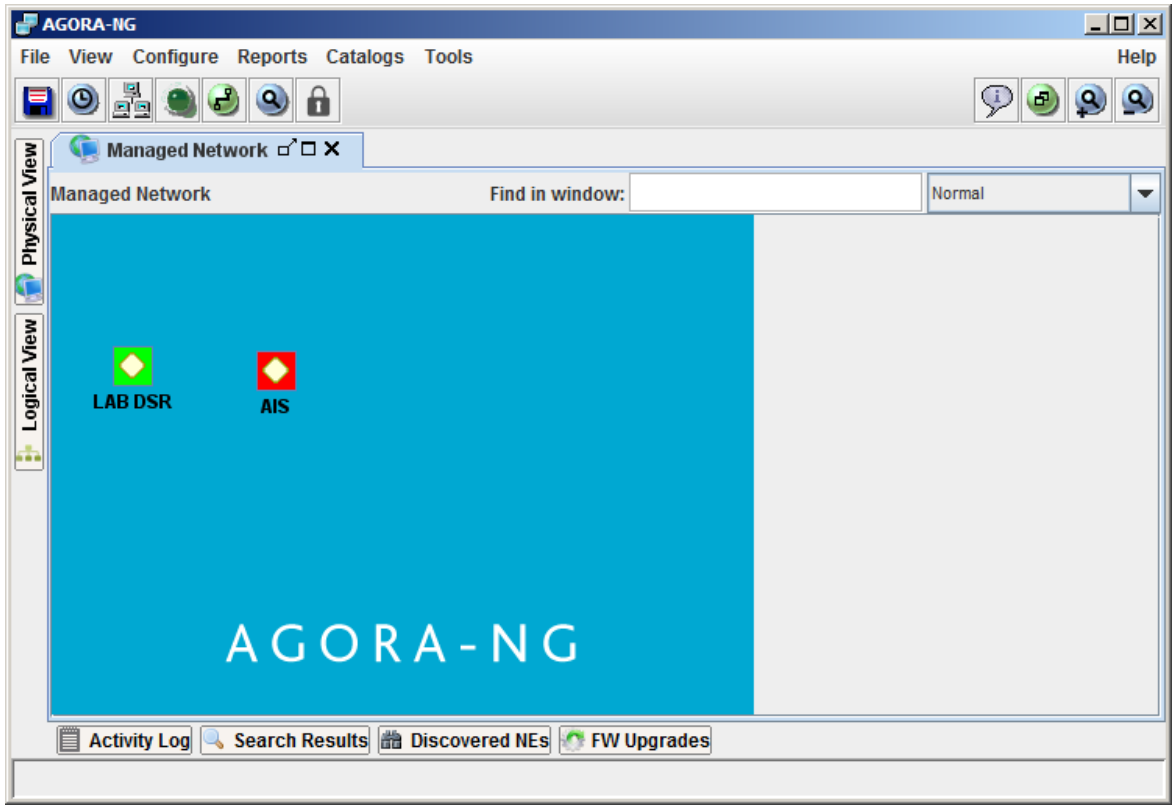


Figure 23. Application main window



Application logout

To exit the application, select the icon in the main window, or select File → Exit in the main menu bar.

Navigation structure

The Resource Manager Module is divided in two main views each one with its own characteristics.

Physical View

Managed Network where all managed elements are mainly located. All network elements are initially mapped in this view according to the operator's organization structure, it may be based on geographical information or internal hierarchical structure. Either way the application is flexible enough to allow a replica of the organization or change it, as it grows;

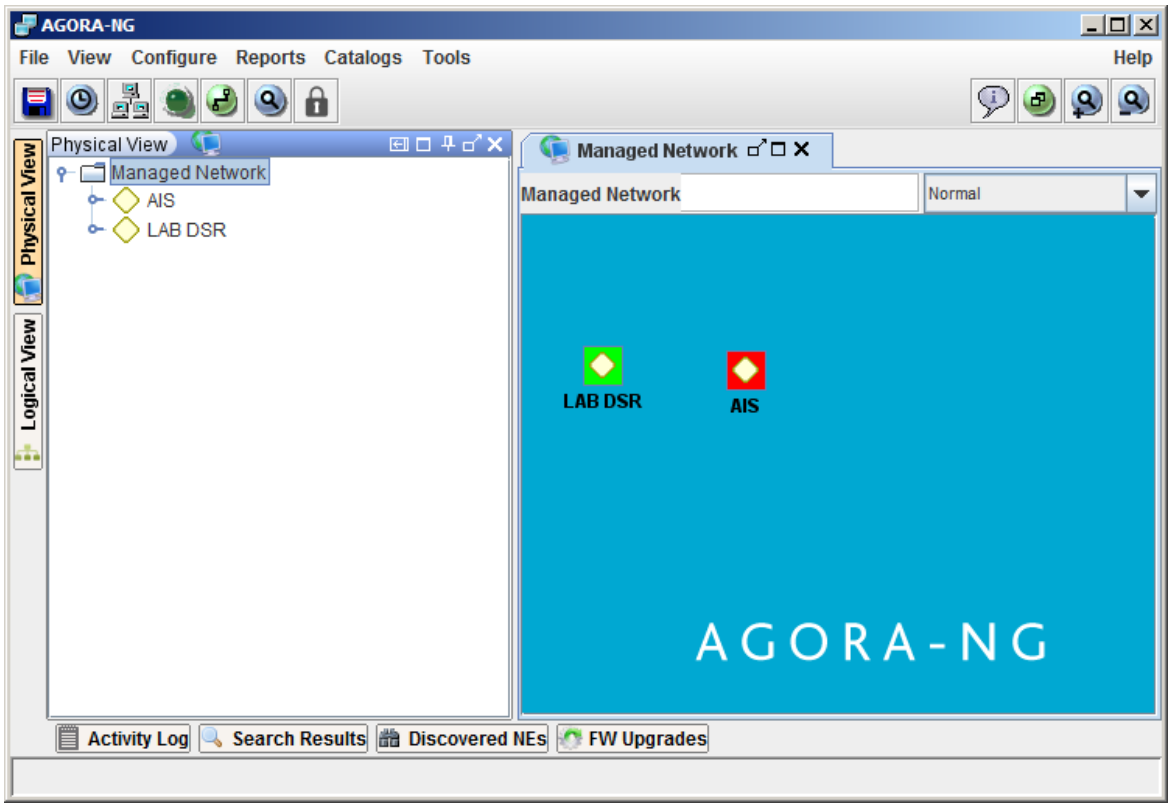
Logical View

Network representation of managed elements previously inserted in Physical View level.

In the left side of the main application window

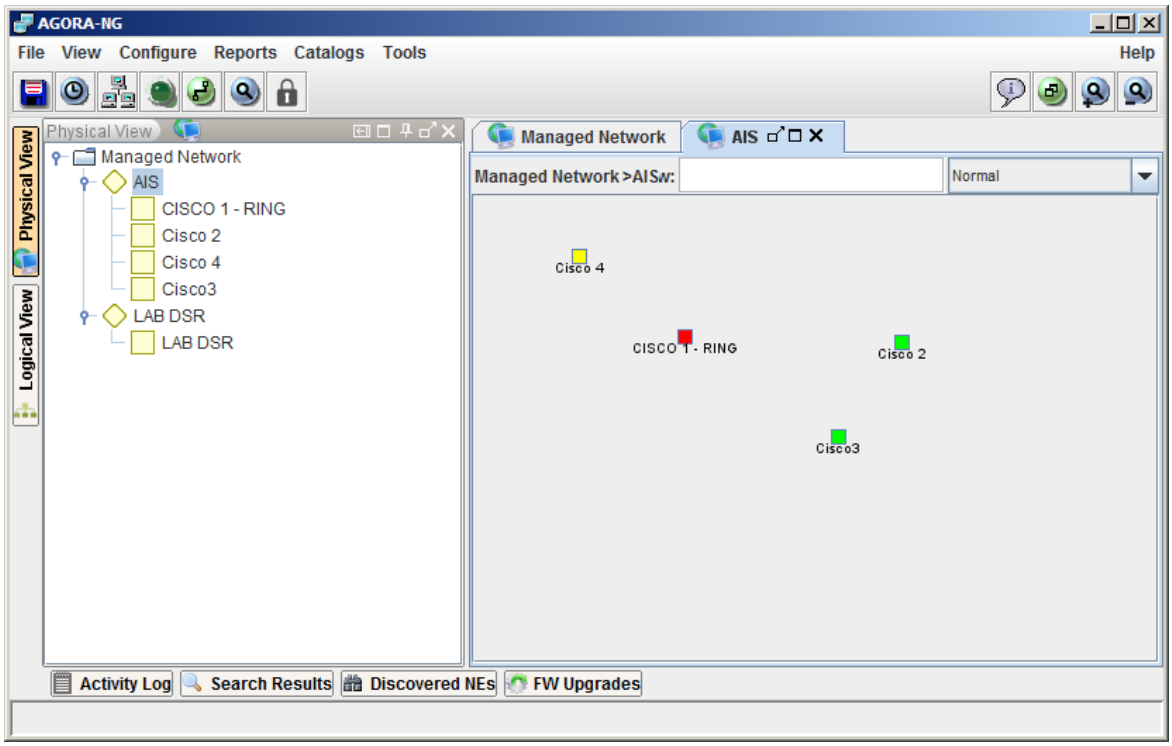
Figure 24, the Physical View, the Management View, or the Logical View can be selected.

Figure 24. Navigation structure



In each view it is possible to select the Managed Domains intended to be accessed. To start navigation through a hierarchical item (Managed Domains, Sites and Aggregators) just double click on the respective icon. Another tab is displayed with the appropriate map in the right pane, as shown in Figure 25.

Figure 25. Managed Domain panel



Full path navigation is always present while “drilling down/up” a hierarchical item. The hierarchal navigation is graphically viewed by a tree (left side of the window) or by separated tabs (Navigation Bar). It is always possible to select over each level to see its representation, Figure 26.

Managed Domains can be hierarchical (Managed Domains can contain other Managed Domains). This entity is used as an “access point” for user profile validation. Users with administrator profile will be presented with all configured Managed Domains, other user profiles will have access only to configured authorized Managed Domains.

Typically and depending on the selected view, the hierarchical structure is composed of three levels.

Physical View:

1st level (Managed Domains)

2nd level (Sites)

3rd level (Technological Group) (*)

Logical View:

1st level (Managed Domains)

2nd level (Geographical Group) (*)

3rd level SubNetwork Group

(*) optional level

Entities Managed Domain (MD), Site, Geographical Group, SubNetwork Group are described in further sections on this document.

Figure 26. Managed Domain Sites representation

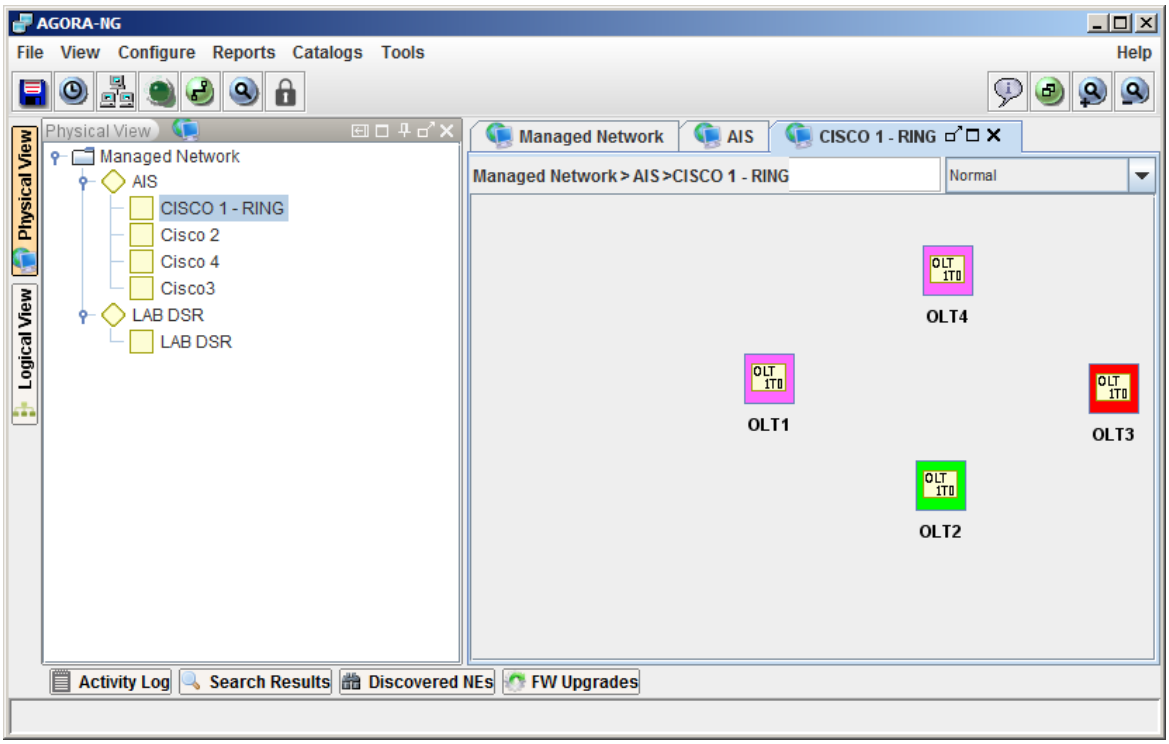
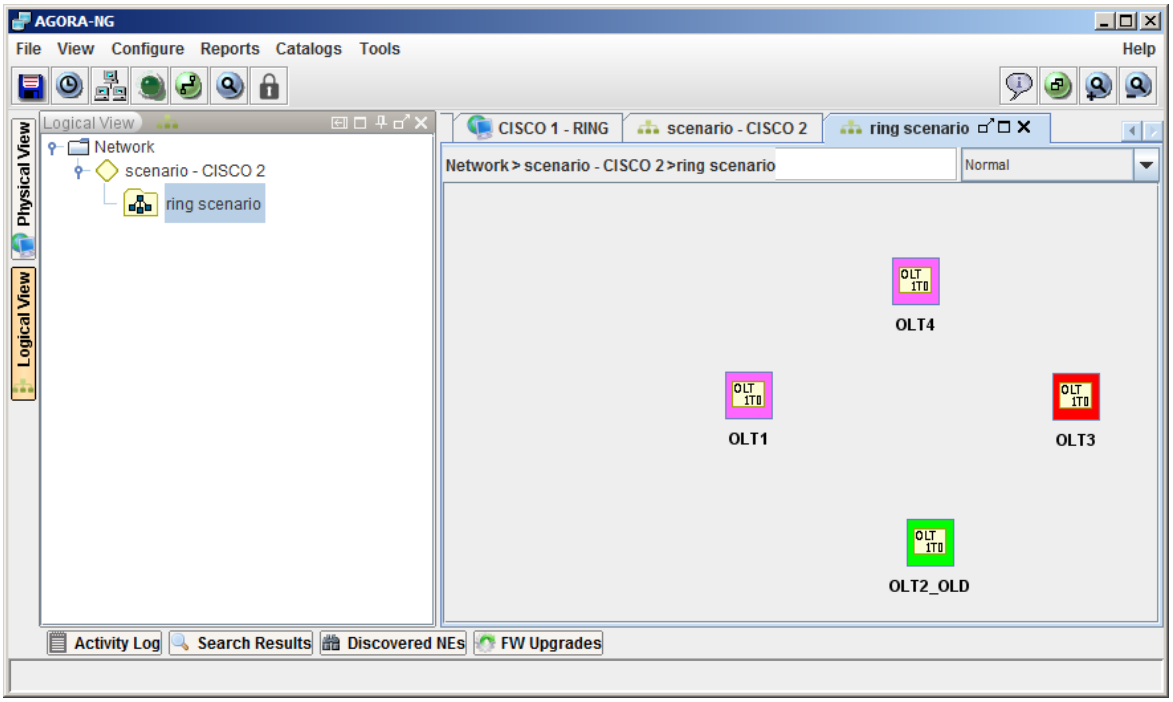


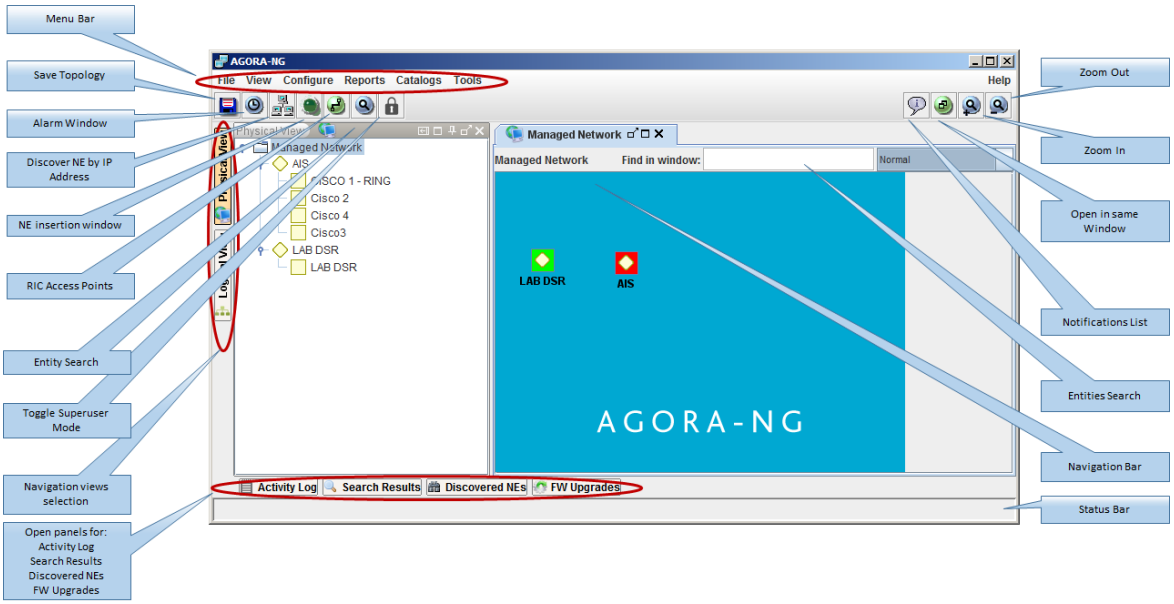
Figure 27. Network level representation



Typical window features

A typical application window is as shown in Figure 28, which also has its features shown.

Figure 28. AGORA-NG typical main window



Bar and Pop-up Menus

All windows that represent the network topology have the menus shown below. Access to menu items depends on the user profile.

In the next section figures are shown menu options that are common to all technologies and menu options only available in a specific technology context.

In the referred figures, the options that are overshadowed are not available in the respective mode view.

File menu

In this menu the user can save the nodes of a map, in an intended position (as long as it has permissions for this operation).

Figure 29. General file menu

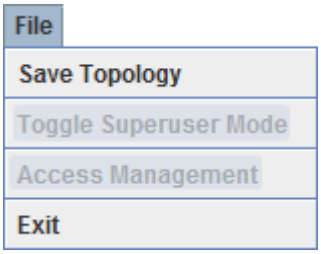
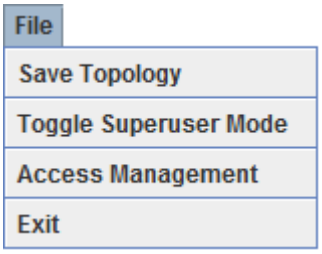


Figure 30. Technology specific file menu



View menu

In this menu the user may view Network Topology Entities and Links, Alarms and Performance Parameters, inserted Circuits and their termination and intermediate points, and the pending alarms associated with equipment's already inserted in managed network.

It is also possible to consult the Activity Log, Search Results, Discovered NEs, FW Upgrades and Notifications List.

Figure 31. General view menu

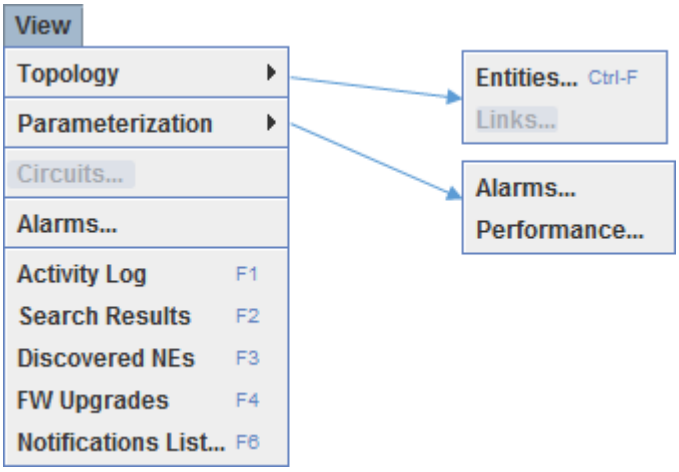
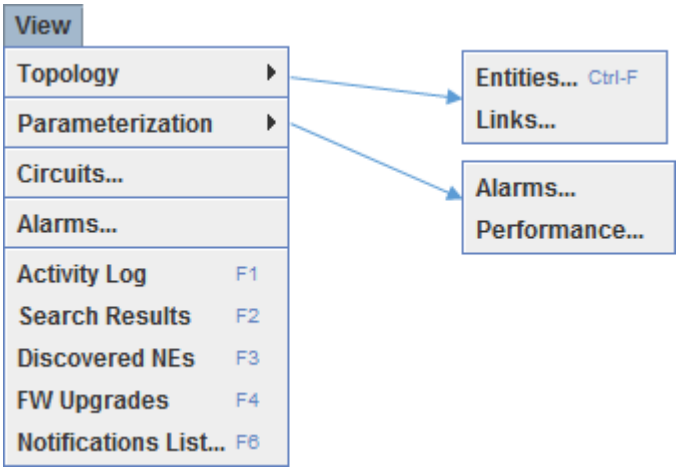


Figure 32. Technology specific view menu



Configure menu

In this menu the user may configure Network Topology entities, Alarms and Performance parameters, Circuits, Download Equipment Firmware Versions, NE Discovery, and RIC Access Points.

Figure 33. General configure menu

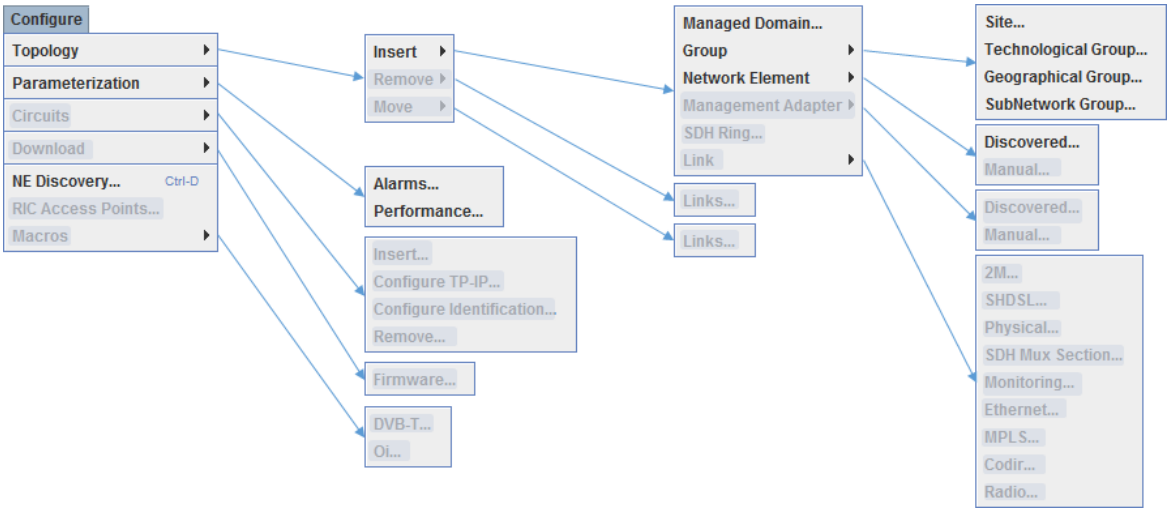


Figure 34. GPON configure menu

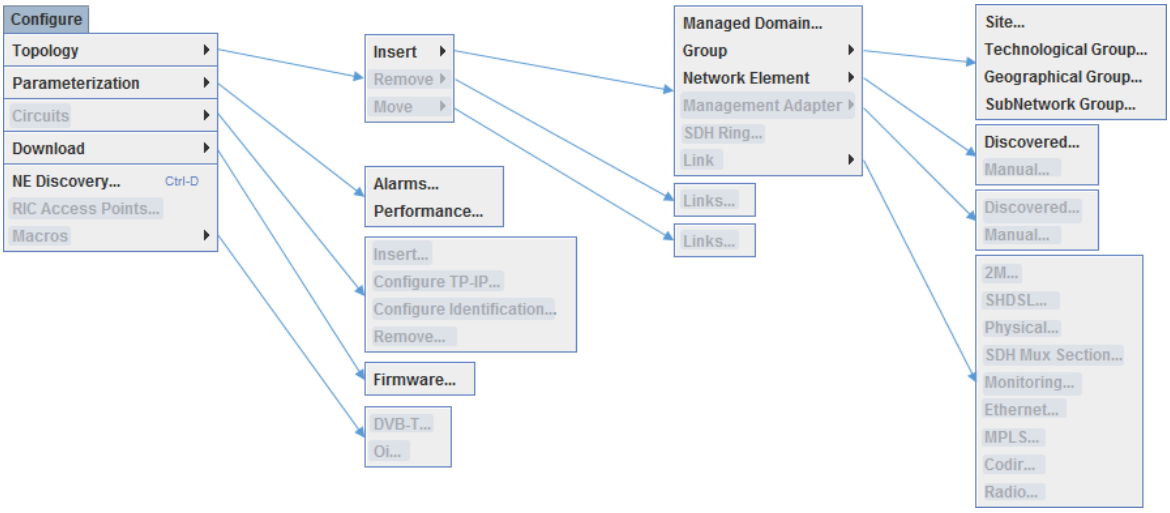


Figure 35. MPLS configure menu (not available)

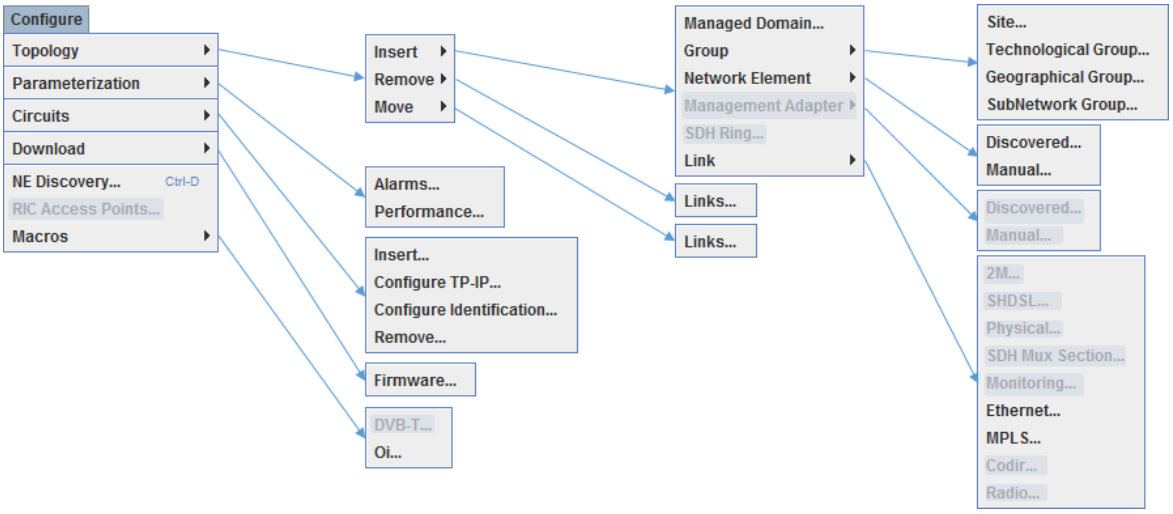


Figure 36. SDH configure menu (not available)

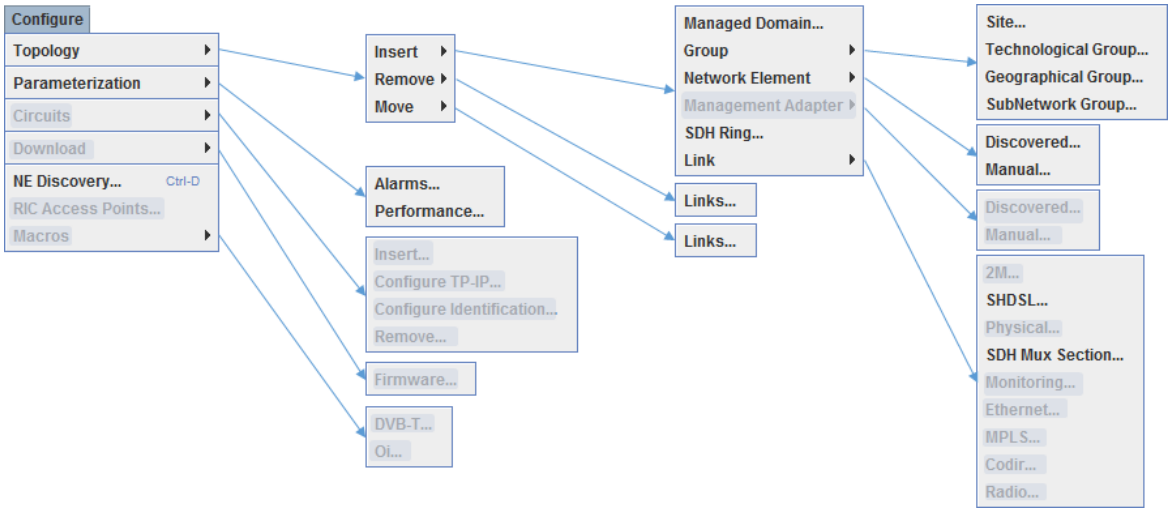
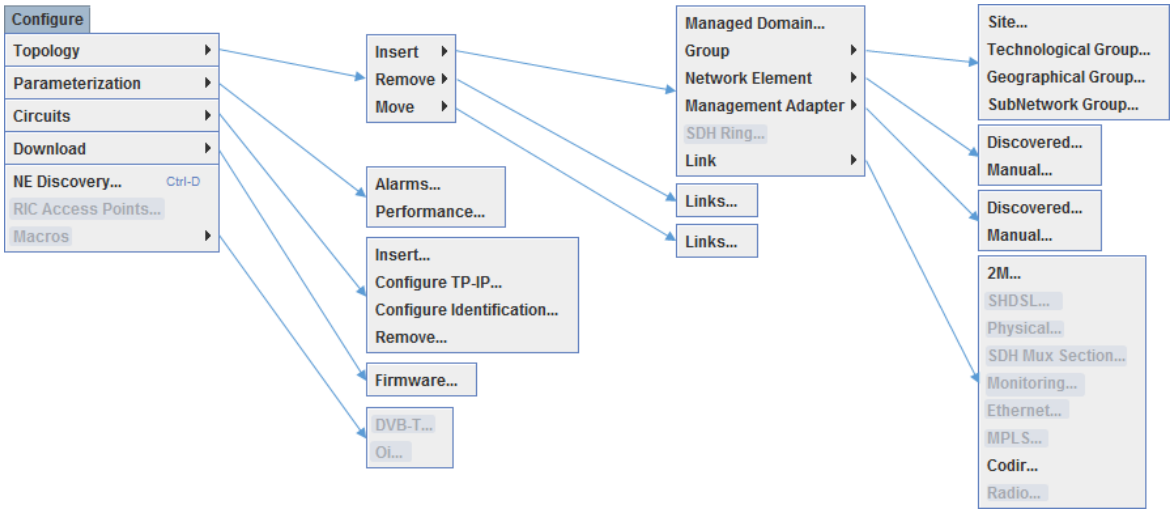


Figure 37. Nx64K configure menu (not available)

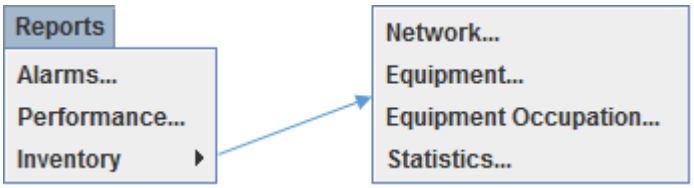


Reports menu

The user can perform Alarms, Performance and Inventory.

Inventory Reports may be generated for network, equipment, equipment occupation and statistics.

Figure 38. General reports menu



Catalogs menu

The user can enter mappings between IP addresses ranges and managed domains, consult or change (only users with management profile) equipment types catalogs, equipment models and create several profile types (xDSL, ATM, DCME, MPLS, Ethernet, GPON traffic and service), filters, SDH sub-networks and remote commands.

These catalog entities are global they are created and parameterized without any reference to a particular managed element.

Figure 39. General catalogs menu

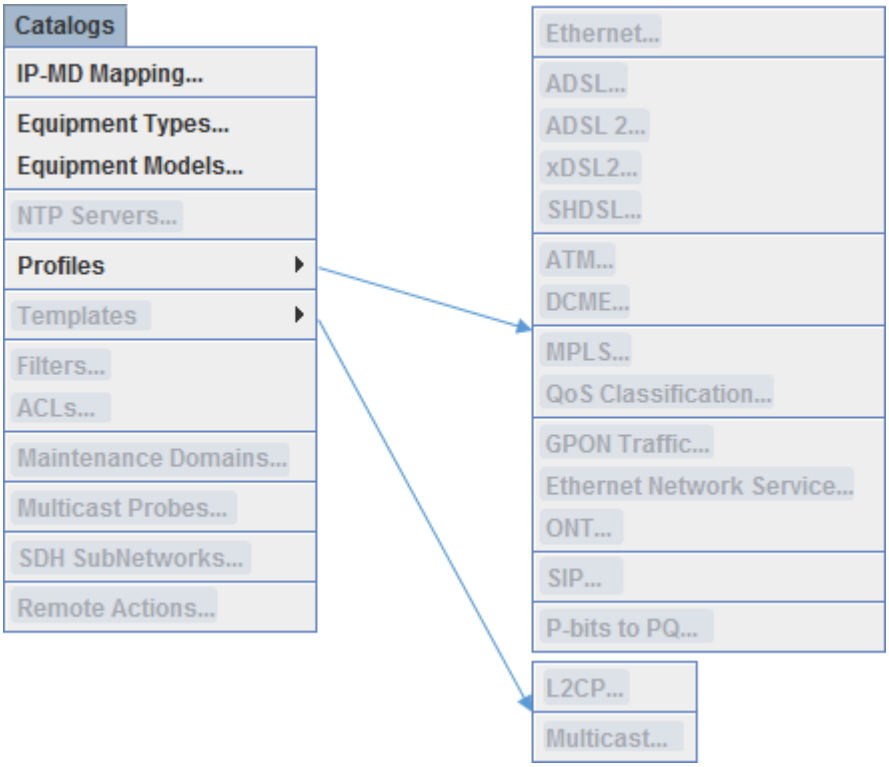


Figure 40. GPON catalogs menu

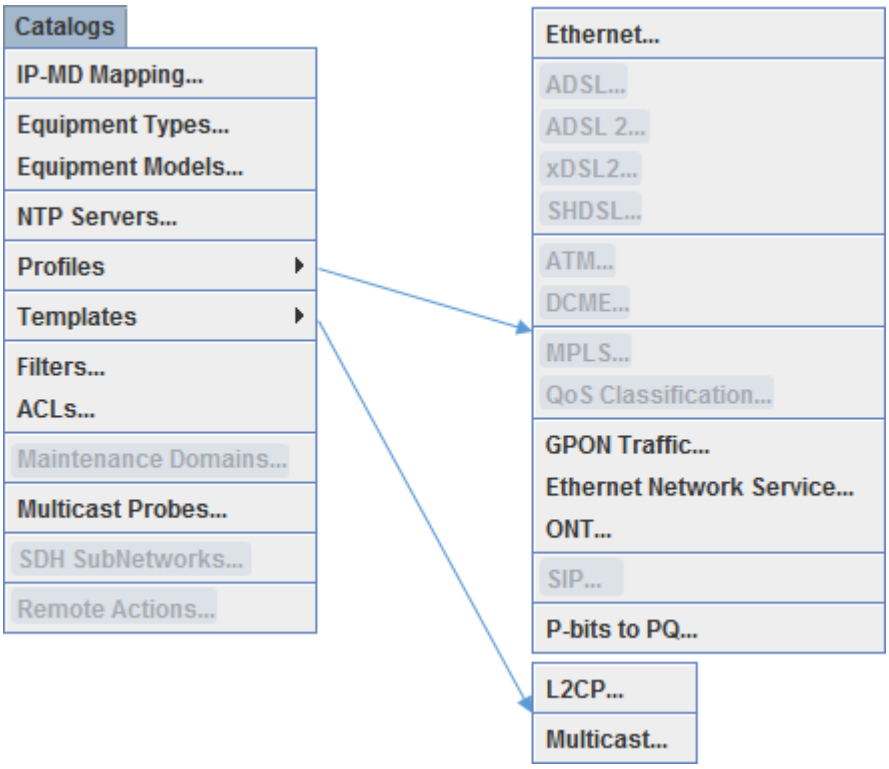


Figure 41. MPLS catalogs menu (not available)

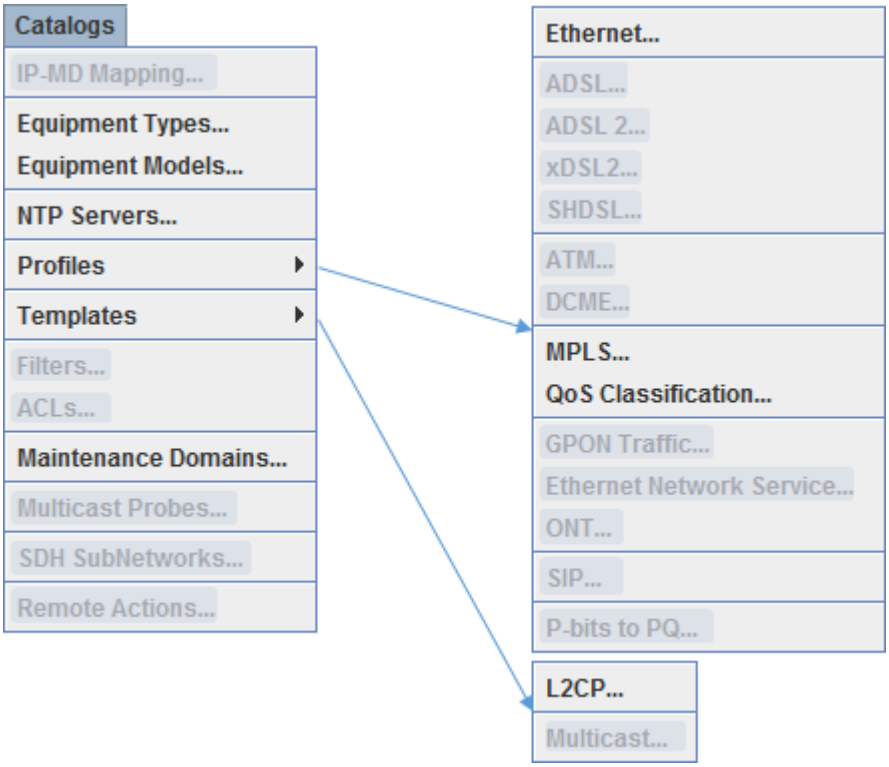


Figure 42. SDH catalogs menu (not available)

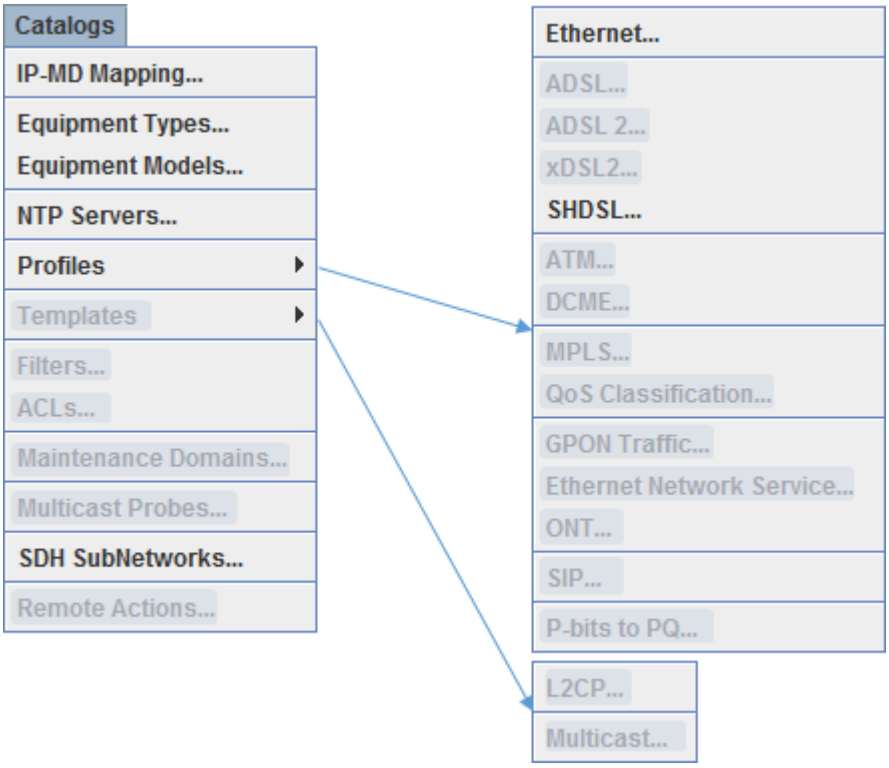
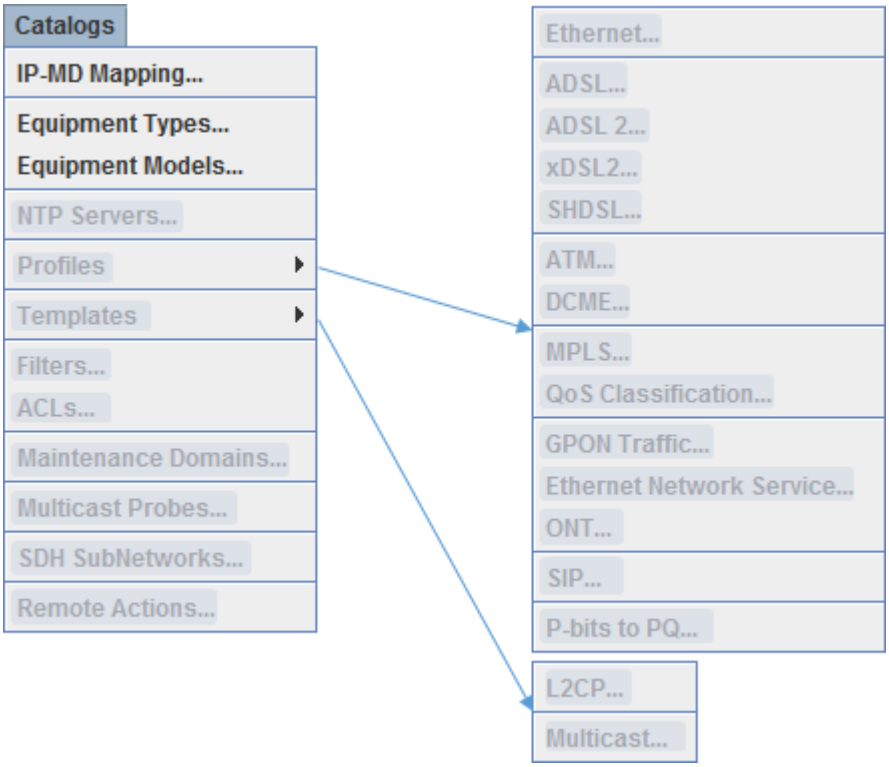


Figure 43. Nx64K catalogs menu (not available)



Tools menu

This menu provides some utility items for generic application. It is possible to view the conversion tables between n*64K bit and ATM cells, select various options to view maps and test both the connectivity between the management system and the equipment, as well as between the client and the management system.

Figure 44. General tools menu

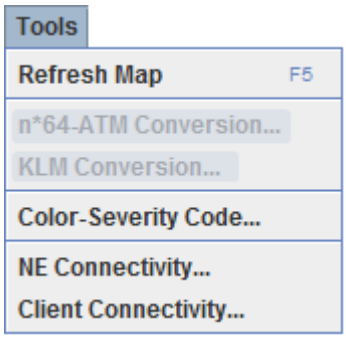
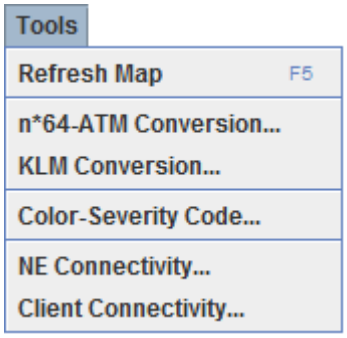


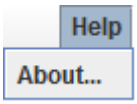
Figure 45. Technology specific tools menu



Help menu

This menu allows the identification of the application version and some related technical data.

Figure 46. Help menu



Status Bar

Status bar is located in the application main window lower side.

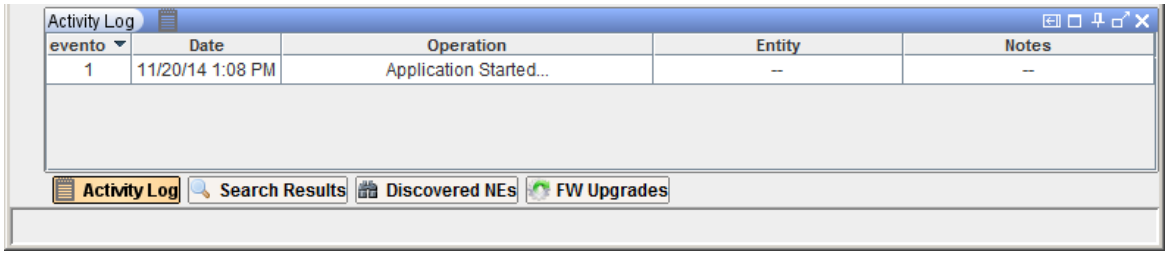
Status bar may show:

- That the user is executing background tasks, through the icon at bar right side;
- The application synchronization process status.

Background Tasks

Background tasks bar icon denotes that background tasks have been executed, otherwise it does not show up.

Figure 47. Status Bar



Application Synchronization Process Status

The synchronization process is triggered when the server starts up, depending on the network size this process may take a long time. During this process the application graphic elements colors will be updated, according to network elements operational status.

Through icons that are shown on the left side of the status bar (Figure 28), the user may check the synchronization process status, thus:

- The icon indicates that the synchronization process is ongoing, which means that application graphic elements colors may not indicate their actual status;
- The icon indicates that no notifications are being received from the server which means that operational status changes notifications are not being received, and thus the graphic elements colors cannot be trusted. This problem may occur due to communication problems between the client and the server;
- In case there is no icon represented in this status bar zone this means that the system is synchronous, i.e., the colors indicate the operational status of network elements.

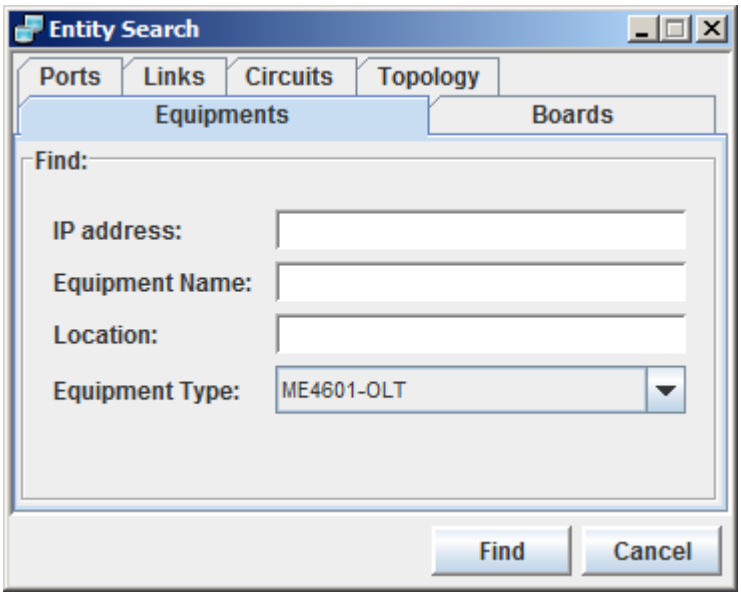
Entity Search

It is possible to search for equipment, boards and ports in the window accessed by selecting View → Topology → Entities, or selecting the icon at the top of the main window, or using Ctrl+F key sequence.

The user may perform several searches filtered by equipment, boards, ports, links, circuits and topology. For each entity type the required fields may vary.

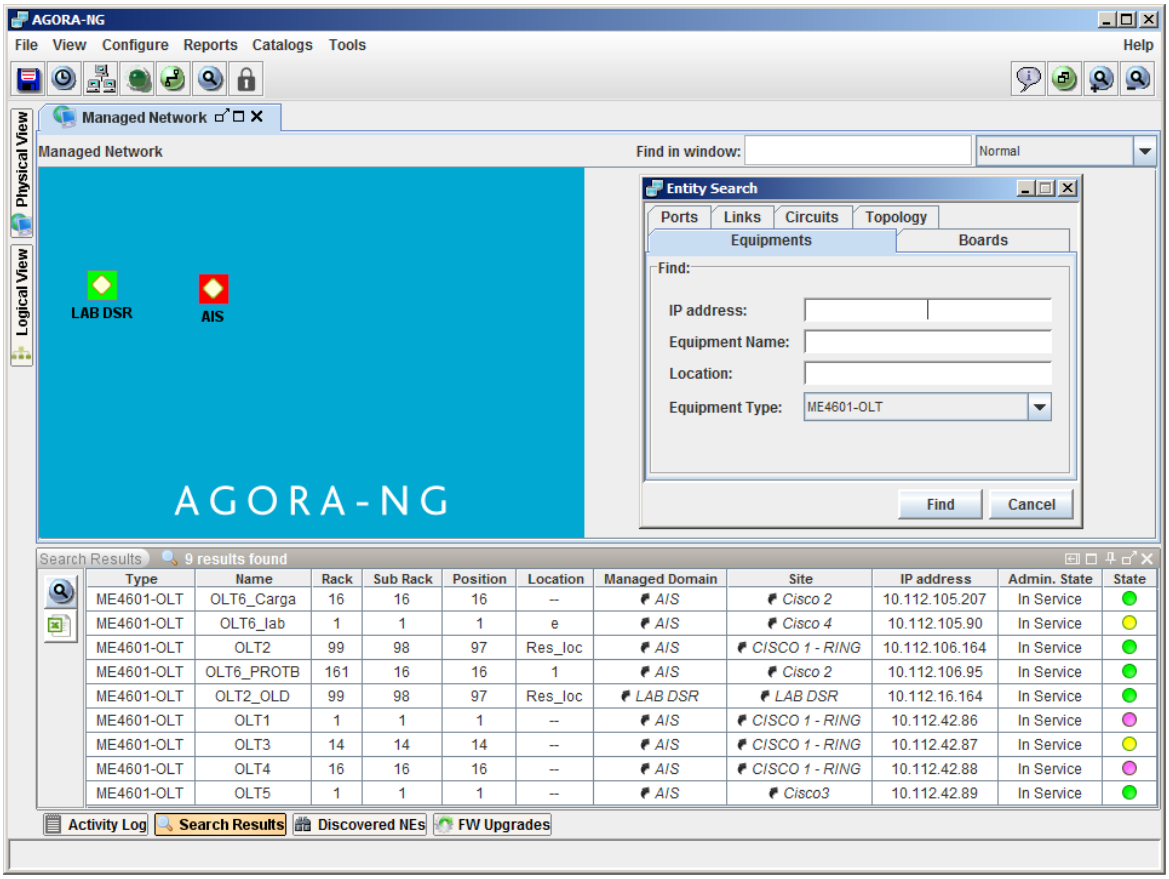
The result of the search is available in the "Search Results" panel in the main window status bar. Select "Search Results" in Figure 28 to show or hide the search results panel.

Figure 48. Entity search



For example, an equipment may be searched by IP address, name (or part of the name, by using the '%' wildcard in the 'Equipment Name' field), location and/or equipment type.

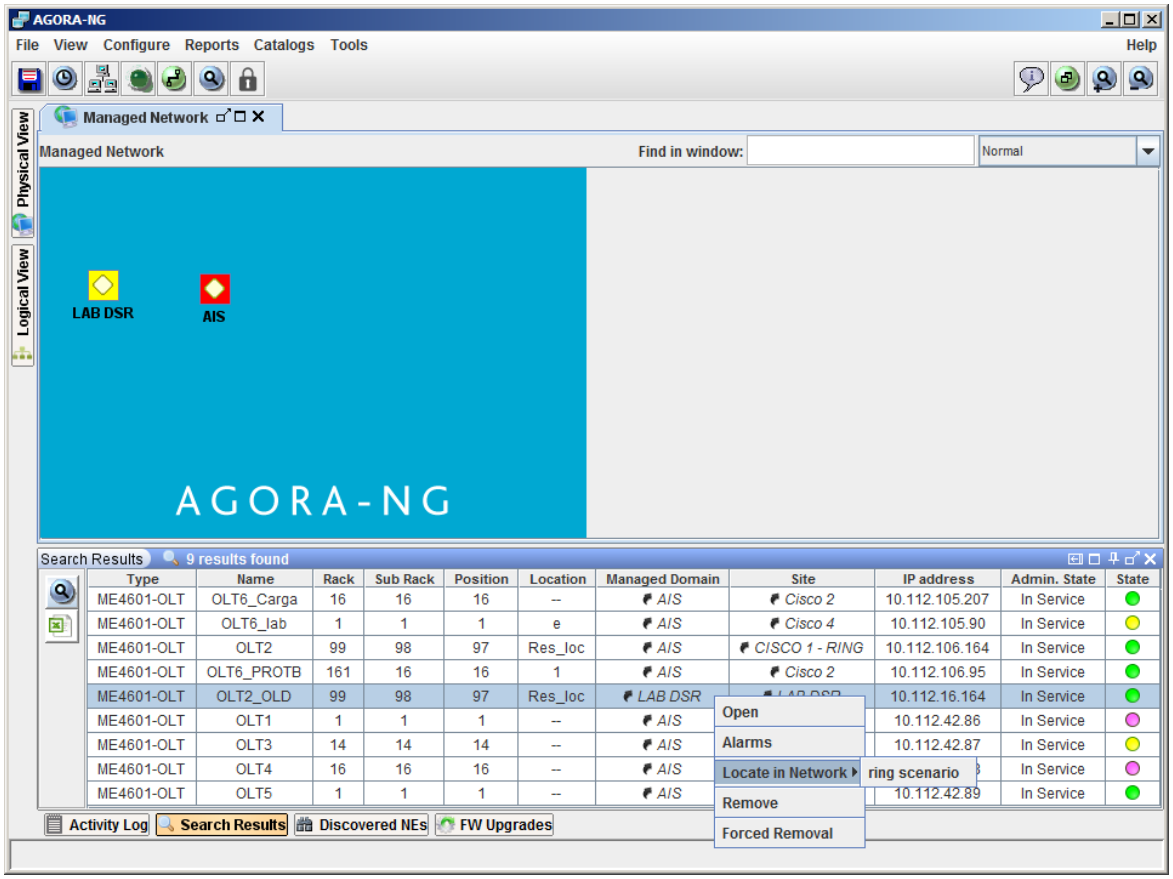
Figure 49. Equipment search results



Type	Name	Rack	Sub Rack	Position	Location	Managed Domain	Site	IP address	Admin. State	State
ME4601-OLT	OLT6_Carga	16	16	16	--	AIS	Cisco 2	10.112.105.207	In Service	
ME4601-OLT	OLT6_lab	1	1	1	e	AIS	Cisco 4	10.112.105.90	In Service	
ME4601-OLT	OLT2	99	98	97	Res_loc	AIS	CISCO 1 - RING	10.112.106.164	In Service	
ME4601-OLT	OLT6_PROTB	161	16	16	1	AIS	Cisco 2	10.112.106.95	In Service	
ME4601-OLT	OLT2_OLD	99	98	97	Res_loc	LAB DSR	LAB DSR	10.112.16.164	In Service	
ME4601-OLT	OLT1	1	1	1	--	AIS	CISCO 1 - RING	10.112.42.86	In Service	
ME4601-OLT	OLT3	14	14	14	--	AIS	CISCO 1 - RING	10.112.42.87	In Service	
ME4601-OLT	OLT4	16	16	16	--	AIS	CISCO 1 - RING	10.112.42.88	In Service	
ME4601-OLT	OLT5	1	1	1	--	AIS	Cisco3	10.112.42.89	In Service	

In the Search Result pane the user will be presented with the result of the previous search query. A right mouse click on a result will allow the user to go directly to the logical view (Locate in Network) or to the Alarm Monitor window (Alarms).

Figure 50. Network equipment location



Double-clicking the equipment icon, in the network logical view, it is possible to view its physical structure (Figure 51).

Figure 51. Equipment physical view

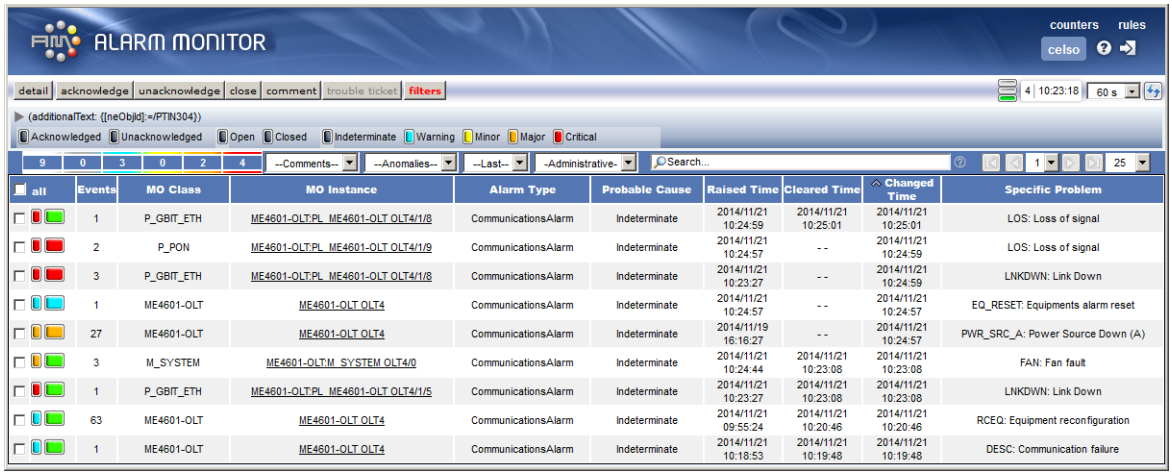
Alarm Management

Alarm management is handled by AGORA-NG Alarm Monitor module.

Alarms window may be accessed in two ways:

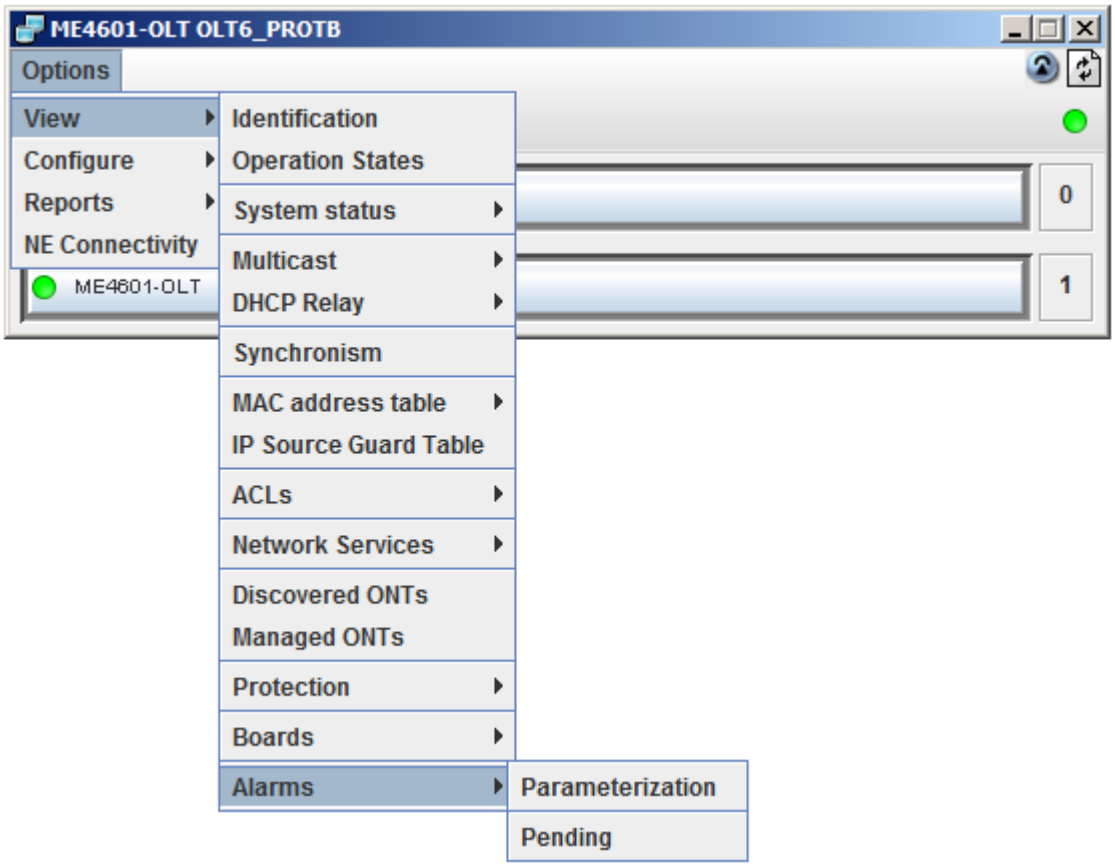
- Accessing the general option View → Alarms, in the main menu or selecting the quick access button in the application's toolbar, a new window (Figure 52) will appear with alarmed managed elements, boards and ports;
- Or in a managed element context, by selecting Options → View → Alarms from the equipment menu.

Figure 52. General alarms window



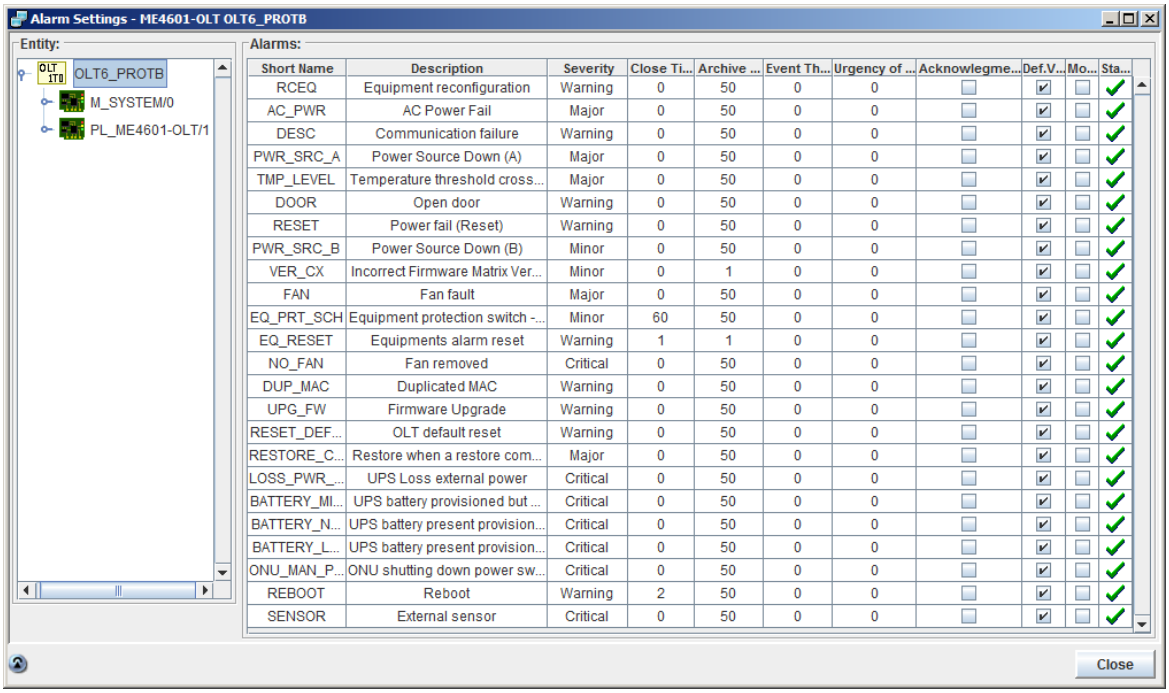
all	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem
	1	P_GBIT_ETH	ME4601-OLT:PL_ME4601-OLT OLT4/1/8	CommunicationsAlarm	Indeterminate	2014/11/21 10:24:59	2014/11/21 10:25:01	2014/11/21 10:25:01	LOS: Loss of signal
	2	P_PON	ME4601-OLT:PL_ME4601-OLT OLT4/1/9	CommunicationsAlarm	Indeterminate	2014/11/21 10:24:57	- -	2014/11/21 10:24:59	LOS: Loss of signal
	3	P_GBIT_ETH	ME4601-OLT:PL_ME4601-OLT OLT4/1/8	CommunicationsAlarm	Indeterminate	2014/11/21 10:23:27	- -	2014/11/21 10:24:59	LNKDWN: Link Down
	1	ME4601-OLT	ME4601-OLT OLT4	CommunicationsAlarm	Indeterminate	2014/11/21 10:24:57	- -	2014/11/21 10:24:57	EQ_RESET: Equipments alarm reset
	27	ME4601-OLT	ME4601-OLT OLT4	CommunicationsAlarm	Indeterminate	2014/11/19 16:16:27	- -	2014/11/21 10:24:57	PWR_SRC_A: Power Source Down (A)
	3	M_SYSTEM	ME4601-OLT:M_SYSTEM OLT4/0	CommunicationsAlarm	Indeterminate	2014/11/21 10:24:44	2014/11/21 10:23:08	2014/11/21 10:23:08	FAN: Fan fault
	1	P_GBIT_ETH	ME4601-OLT:PL_ME4601-OLT OLT4/1/5	CommunicationsAlarm	Indeterminate	2014/11/21 10:23:27	2014/11/21 10:23:08	2014/11/21 10:23:08	LNKDWN: Link Down
	63	ME4601-OLT	ME4601-OLT OLT4	CommunicationsAlarm	Indeterminate	2014/11/21 09:55:24	2014/11/21 10:20:46	2014/11/21 10:20:46	RCEQ: Equipment reconfiguration
	1	ME4601-OLT	ME4601-OLT OLT4	CommunicationsAlarm	Indeterminate	2014/11/21 10:18:53	2014/11/21 10:19:48	2014/11/21 10:19:48	DESC: Communication failure

Figure 53. Example of how to access the alarms window from a unit environment



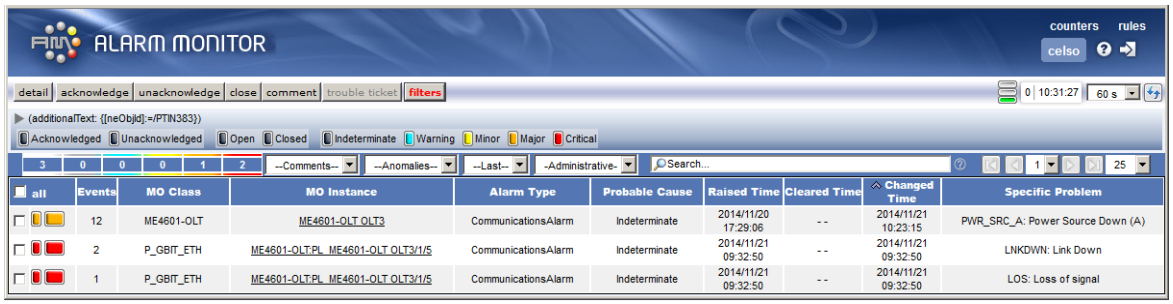
The different types of alarms associated with a managed element can be parameterized.

Figure 54. Alarm settings parameterization



Short Name	Description	Severity	Close Ti...	Archive ...	Event Th...	Urgency of ...	Acknowlegme...	Def.V...	Mo...	Sta...
RCEQ	Equipment reconfiguration	Warning	0	50	0	0		✔		✔
AC_PWR	AC Power Fail	Major	0	50	0	0		✔		✔
DESC	Communication failure	Warning	0	50	0	0		✔		✔
PWR_SRC_A	Power Source Down (A)	Major	0	50	0	0		✔		✔
TMP_LEVEL	Temperature threshold cross...	Major	0	50	0	0		✔		✔
DOOR	Open door	Warning	0	50	0	0		✔		✔
RESET	Power fail (Reset)	Warning	0	50	0	0		✔		✔
PWR_SRC_B	Power Source Down (B)	Minor	0	50	0	0		✔		✔
VER_CX	Incorrect Firmware Matrix Ver...	Minor	0	1	0	0		✔		✔
FAN	Fan fault	Major	0	50	0	0		✔		✔
EQ_PRT_SCH	Equipment protection switch -...	Minor	60	50	0	0		✔		✔
EQ_RESET	Equipments alarm reset	Warning	1	1	0	0		✔		✔
NO_FAN	Fan removed	Critical	0	50	0	0		✔		✔
DUP_MAC	Duplicated MAC	Warning	0	50	0	0		✔		✔
UPG_FW	Firmware Upgrade	Warning	0	50	0	0		✔		✔
RESET_DEF...	OLT default reset	Warning	0	50	0	0		✔		✔
RESTORE_C...	Restore when a restore com...	Major	0	50	0	0		✔		✔
LOSS_PWR_...	UPS Loss external power	Critical	0	50	0	0		✔		✔
BATTERY_MI...	UPS battery provisioned but ...	Critical	0	50	0	0		✔		✔
BATTERY_N...	UPS battery present provision...	Critical	0	50	0	0		✔		✔
BATTERY_L...	UPS battery present provision...	Critical	0	50	0	0		✔		✔
ONU_MAN_P...	ONU shutting down power sw...	Critical	0	50	0	0		✔		✔
REBOOT	Reboot	Warning	2	50	0	0		✔		✔
SENSOR	External sensor	Critical	0	50	0	0		✔		✔

Figure 55. Device environment alarms

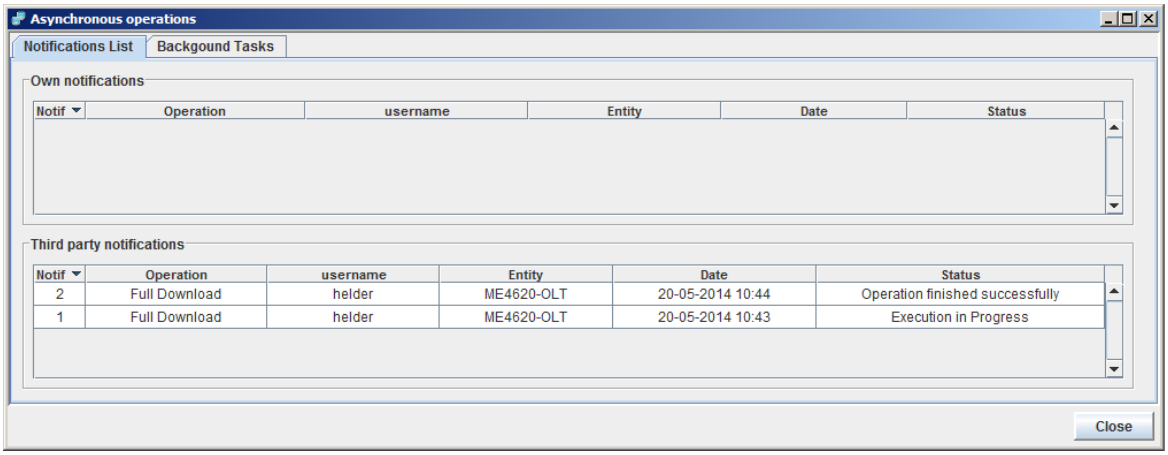


all	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem
	12	ME4601-OLT	ME4601-OLT OLT3	CommunicationsAlarm	Indeterminate	2014/11/20 17:29:06	- -	2014/11/21 10:23:15	PWR_SRC_A: Power Source Down (A)
	2	P_GBIT_ETH	ME4601-OLT:PL_ME4601-OLT OLT3/1/5	CommunicationsAlarm	Indeterminate	2014/11/21 09:32:50	- -	2014/11/21 09:32:50	LNKDWN: Link Down
	1	P_GBIT_ETH	ME4601-OLT:PL_ME4601-OLT OLT3/1/5	CommunicationsAlarm	Indeterminate	2014/11/21 09:32:50	- -	2014/11/21 09:32:50	LOS: Loss of signal

Notifications List

Notifications received in the user's session are available for consultation through the icon.

Figure 56. Notifications list



Graphic Objects

In the next table is shown the graphic symbols list used in this application which represent the network entities (managed domains, sites and aggregators).

Table 43. Graphic Objects

Entity	Symbol
Managed Domain	
Site	
Technology Aggregator	
Geographic Aggregator	
Sub-Network Aggregator	

Visual Status

All entities represented in the application (managed domains, sites, aggregators and managed elements) have an associated status. Each graphic symbol color represents the associated entity (e.g., equipment) or their entities worst status (remaining cases).

Table 44. Color coding map

Color	Meaning
Blue	Equipment or Entity Equipment in Maintenance
Beige	Equipment or Entity Equipment is Blocked
Brown	Equipment or Entity Equipment is Registered
Red	Equipment or Entity Equipment has a Critical Alarm
Garnet	Equipment or Entity Equipment has a Severe Alarm
Orange	Equipment or Entity Equipment has a Severe or Critical, Known Alarm
Yellow	Equipment or Entity Equipment Unknown Alarm
Green	Equipment or Entity Equipment is Operational

If several entities with different status exist under another entity, the most severe one predominates. The decreasing severity level of an alarm is measured in the following order: Red, Garnet, Orange, Yellow, Green, Blue, Beige and Brown.

Application Configuration

Access and permissions for Configuration Operations depend on the user profile.

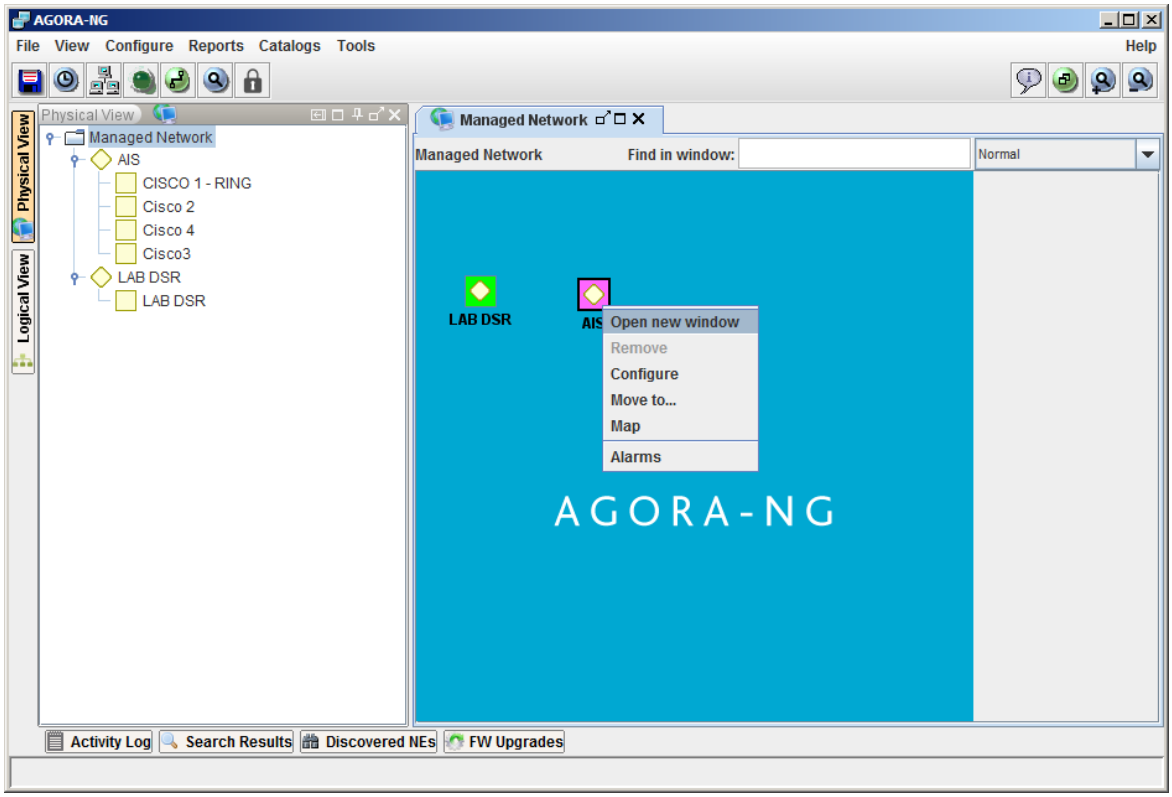
Topology

Managed Domain

Managed Domains can contain other Managed Domains.

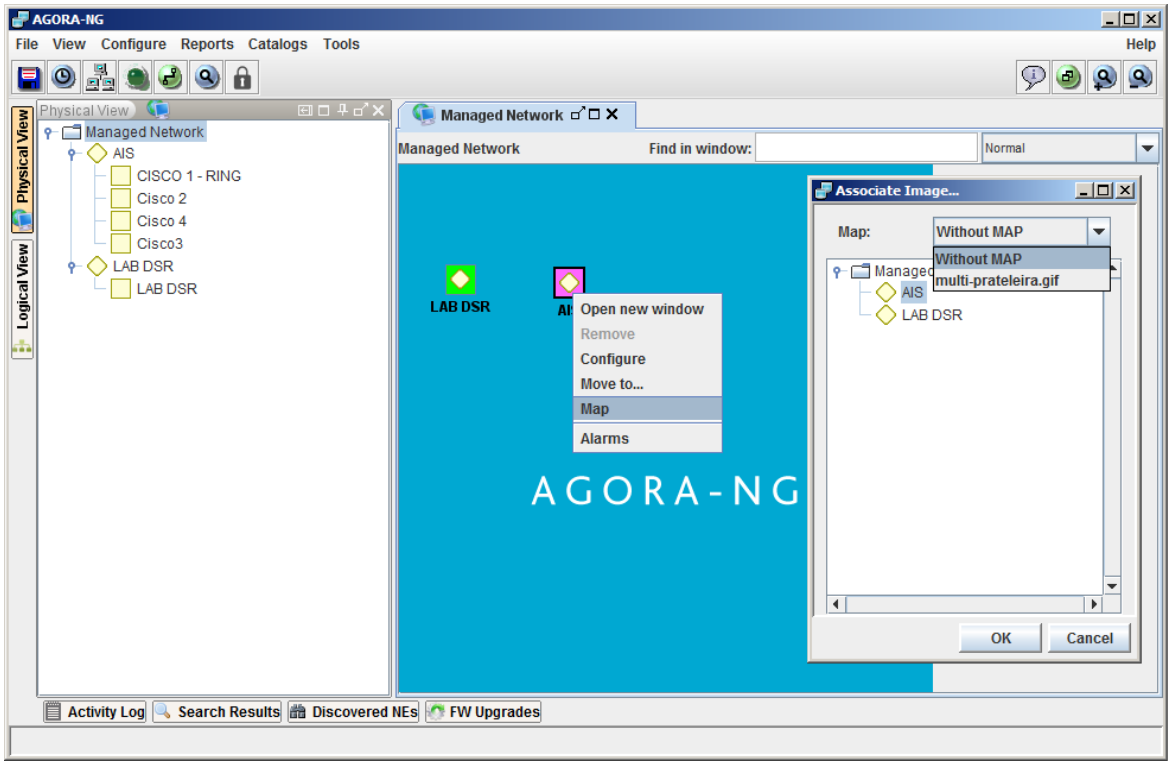
If the user selects a Managed Domain that contains other Managed Domain(s), inner domains will be presented selecting (and “drilling down”) the magnifying glass, next to the Managed Domain on the tree list, or right-selecting the item and selecting ‘Open new window’ (Figure 57). A Managed Domain window with the entities that it contains (Sites and/or managed domains) will be presented (Figure 57).

Figure 57. Looking up managed domains



Right-selecting over the Managed Domain and selecting 'Map', it is possible to associate a custom map (background image) to the Managed Domain entity window (Figure 58).

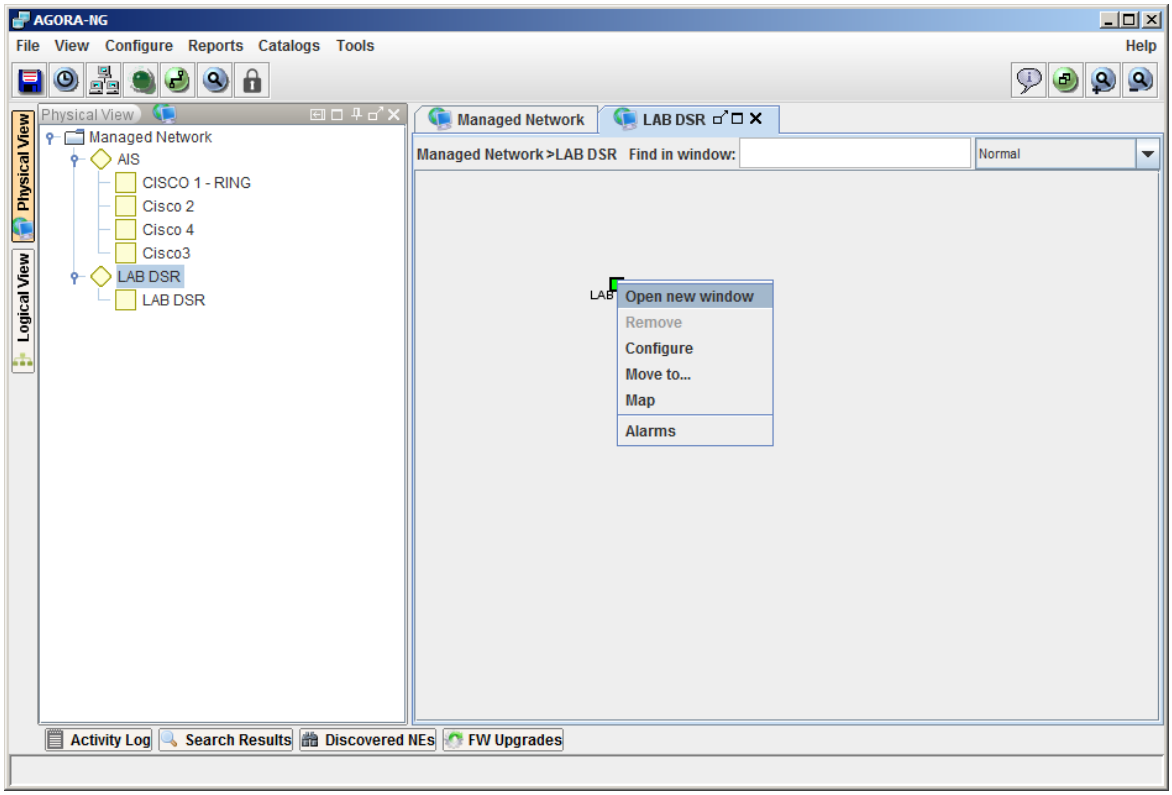
Figure 58. Entity window map insertion example



Site

If the user selects a managed domain that contains sites or other managed domains, the system will display them in the domain on the right panel (Figure 59). Selecting on the magnifying glass next to the Managed Domain on the tree list, or right-selecting over the item and selecting 'Open new window' (Figure 59), will bring up the corresponding Site window with the entities it contains (Technical Groups and/or Network Elements).

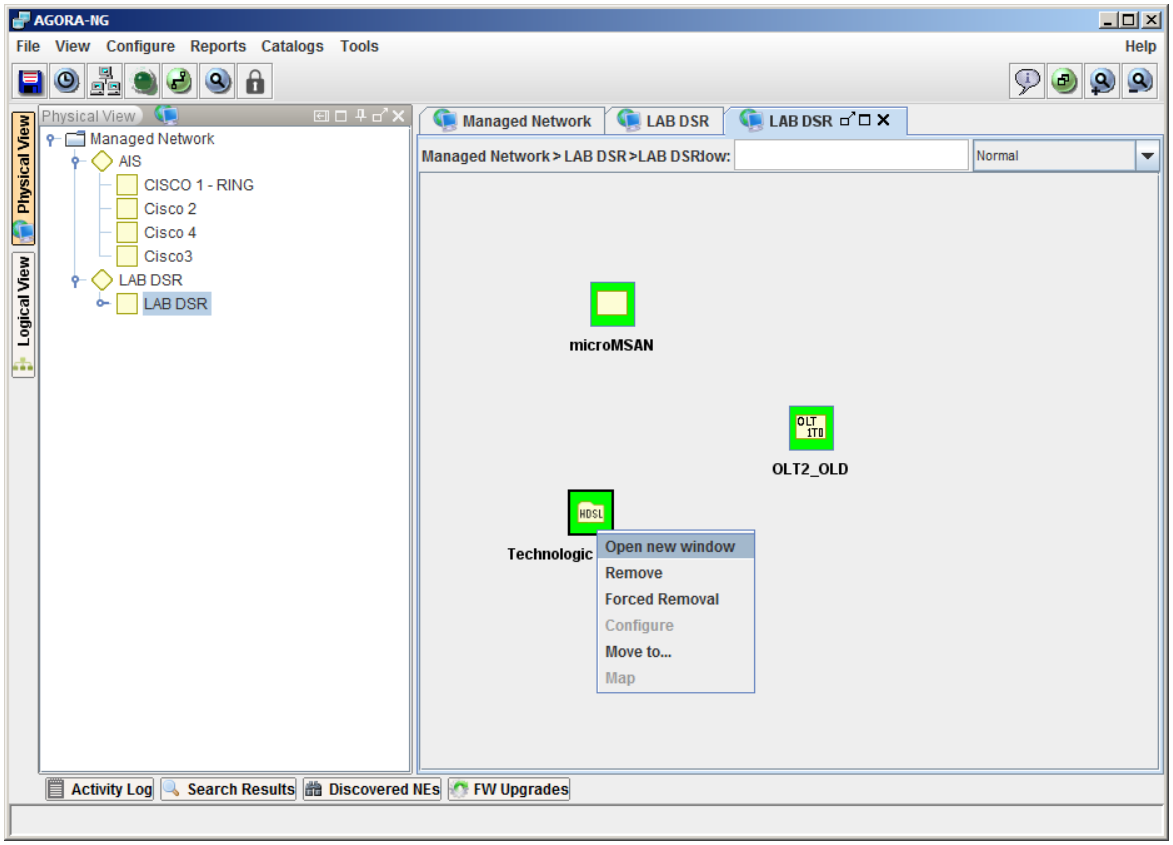
Figure 59. Looking up sites



Technologic Group

If the user selects a site or a Technologic Group that contain Technologic Groups, they will be presented selecting (and "drilling down") the magnifying glass, next to the Managed Domain on the tree list, or right-selecting the item and selecting 'Open new window' (Figure 60). A Technologic window with the entities that it contains (Technical Groups and/or Network Elements) will be presented.

Figure 60. Looking up Technologic Groups



Geographical / Sub-network Group

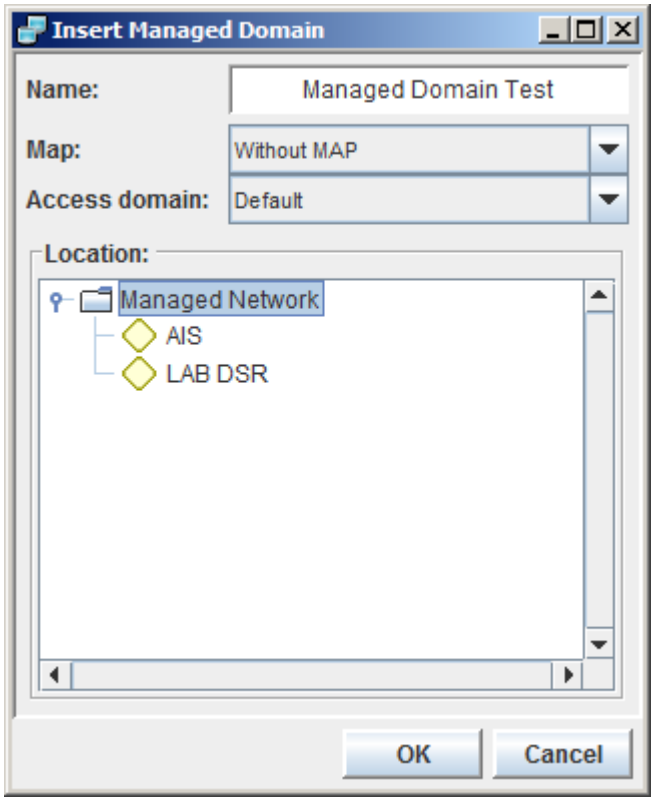
The look up process for Geographical and Sub-network Groups is the same as described for Technologic Group but on the Logical View layer (network representation of the managed elements).

Node Management

Managed Domain

In order to insert a Managed Domain, from the main window select Configure → Topology → Insert → Managed Domain. In the window shown in Figure 61, assign a name to the domain, a map if necessary, a Access domain and choose the partition of the network where to create the Managed Domain. The 'OK' button will bring up a window showing the new created Managed Domain.

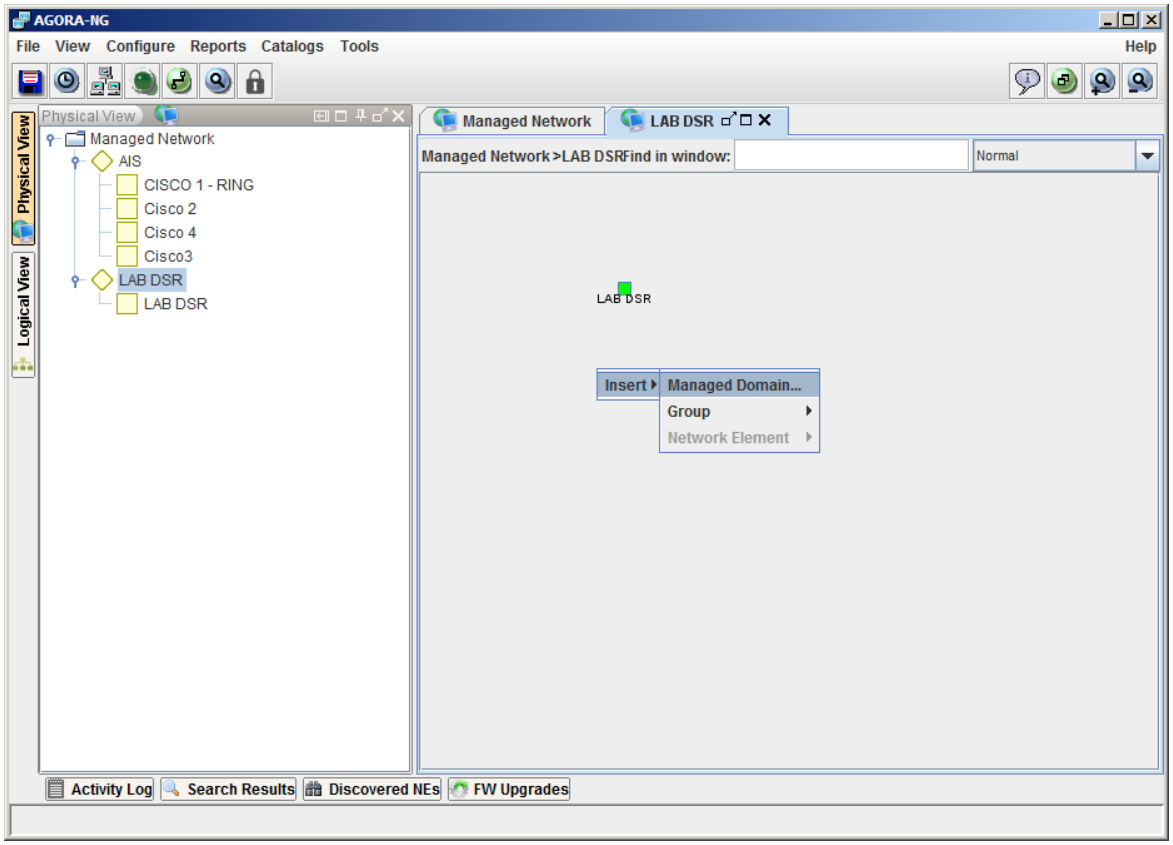
Figure 61. Managed Domain insertion



Each Managed Domain must be associated with an Access Domain. The access domain is a virtual entity related with the access control that allows the aggregation of several physical entities groups (managed domains/equipment) in only one entity, which facilitates access management within Access Control System module.

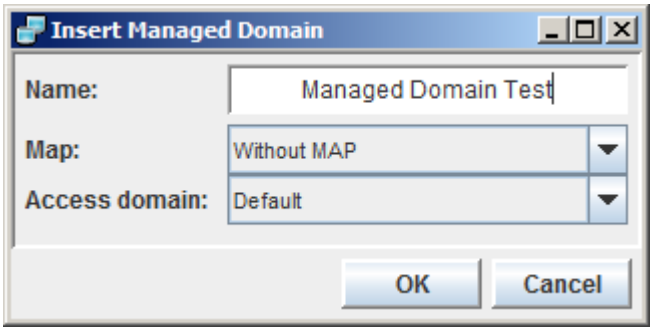
An alternative way to insert a Managed Domain is directly in the window pane where it is intended to be inserted. Select the right mouse button Insert → Managed Domain, as shown in Figure 62.

Figure 62. Direct location Managed Domain insertion



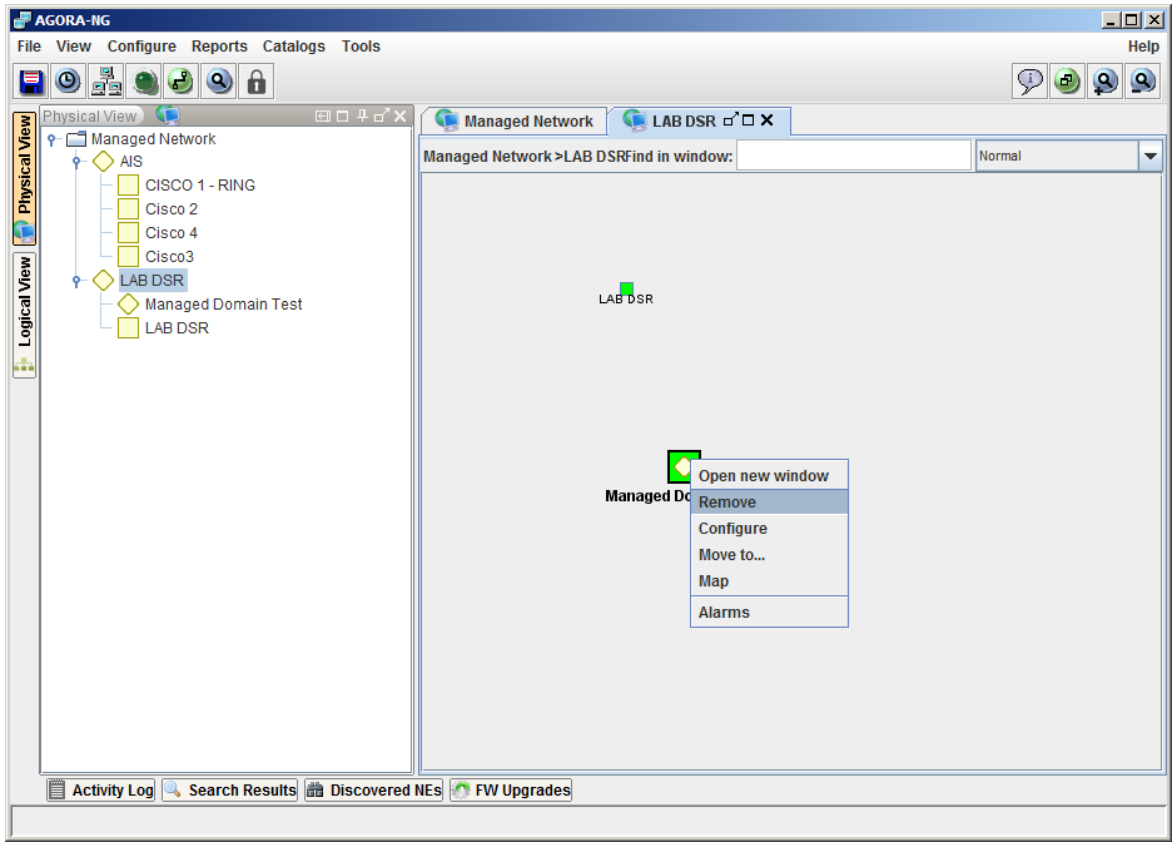
In this case the Managed Domain insertion window is as shown in Figure 63, that is similar with the one in Figure 61, without the choose location component because the Managed Domain will be created in the open window pane.

Figure 63. Direct intended location Managed Domain insertion



In order to remove a Managed Domain, right-select the Managed Domain to be removed and select option 'Remove' (Figure 64).

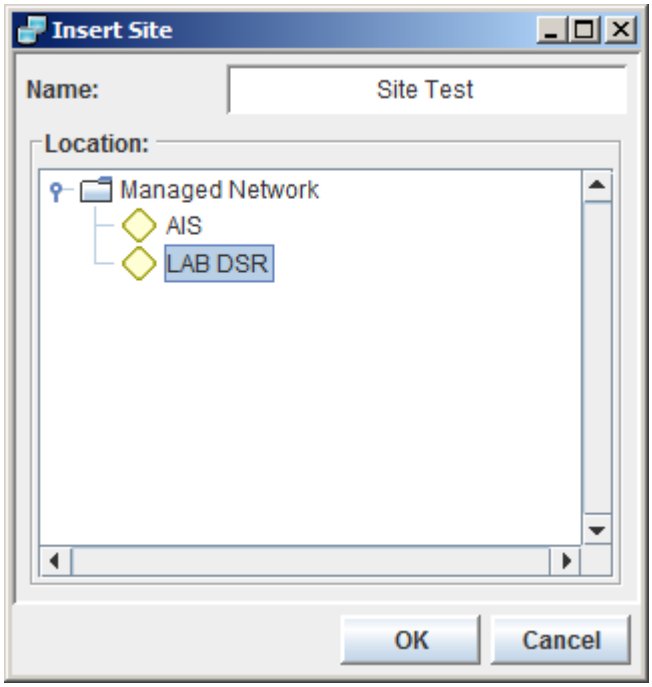
Figure 64. Removing managed domains



Site

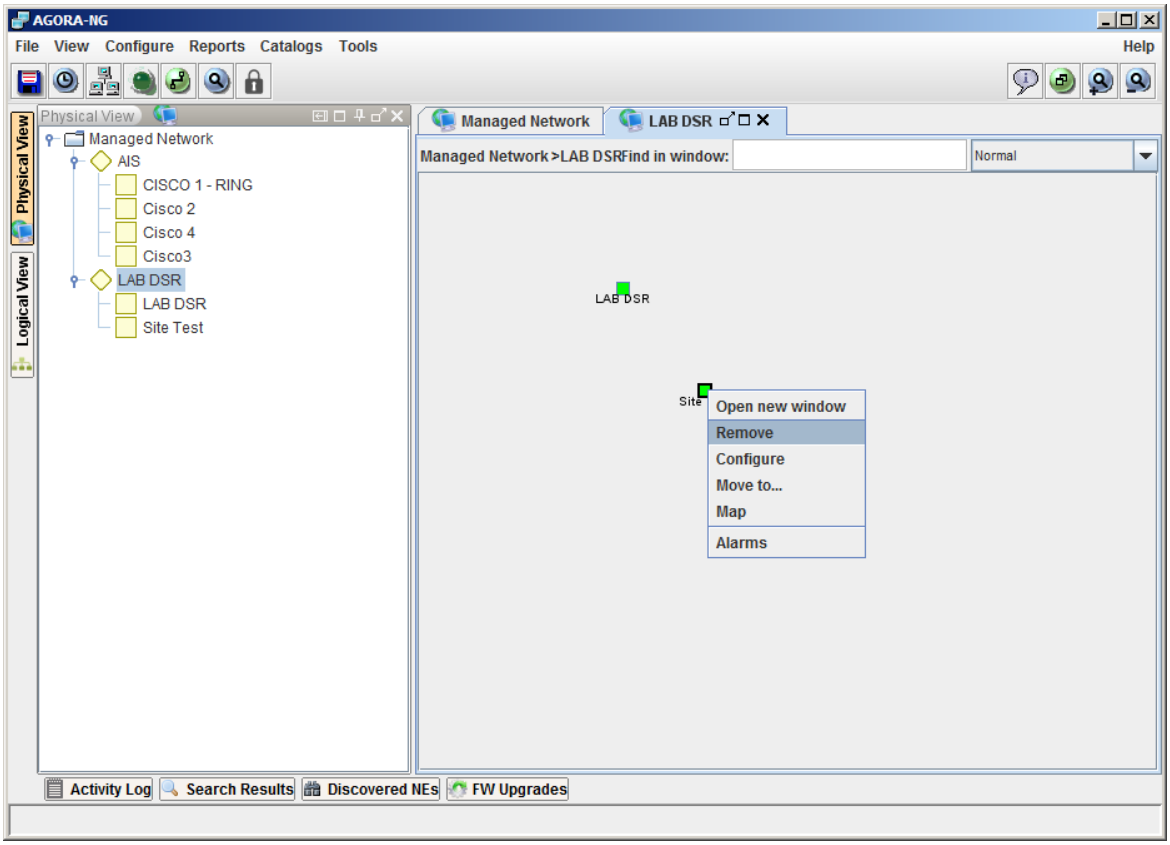
In order to insert a Site, from the main window select Configure → Topology → Insert → Group → Site. In the window shown in Figure 65, assign a name to the Site and choose the managed domain where to create the Site. The 'OK' button will bring up a window showing the new created Site.

Figure 65. Site insertion



In order to remove a Site, right-select the Site to be removed and select option 'Remove' (Figure 66).

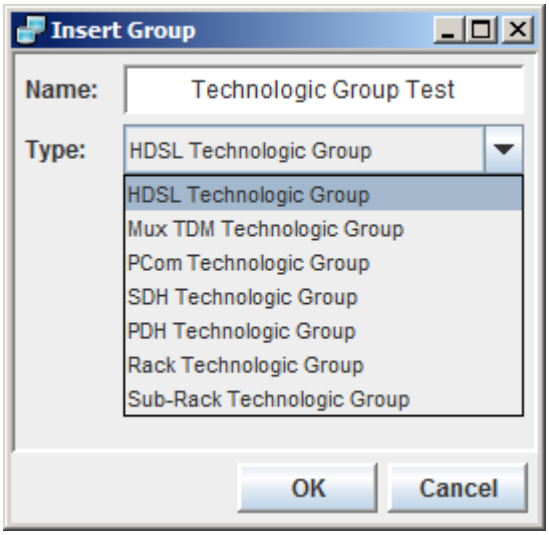
Figure 66. Removing Sites



Technologic Group

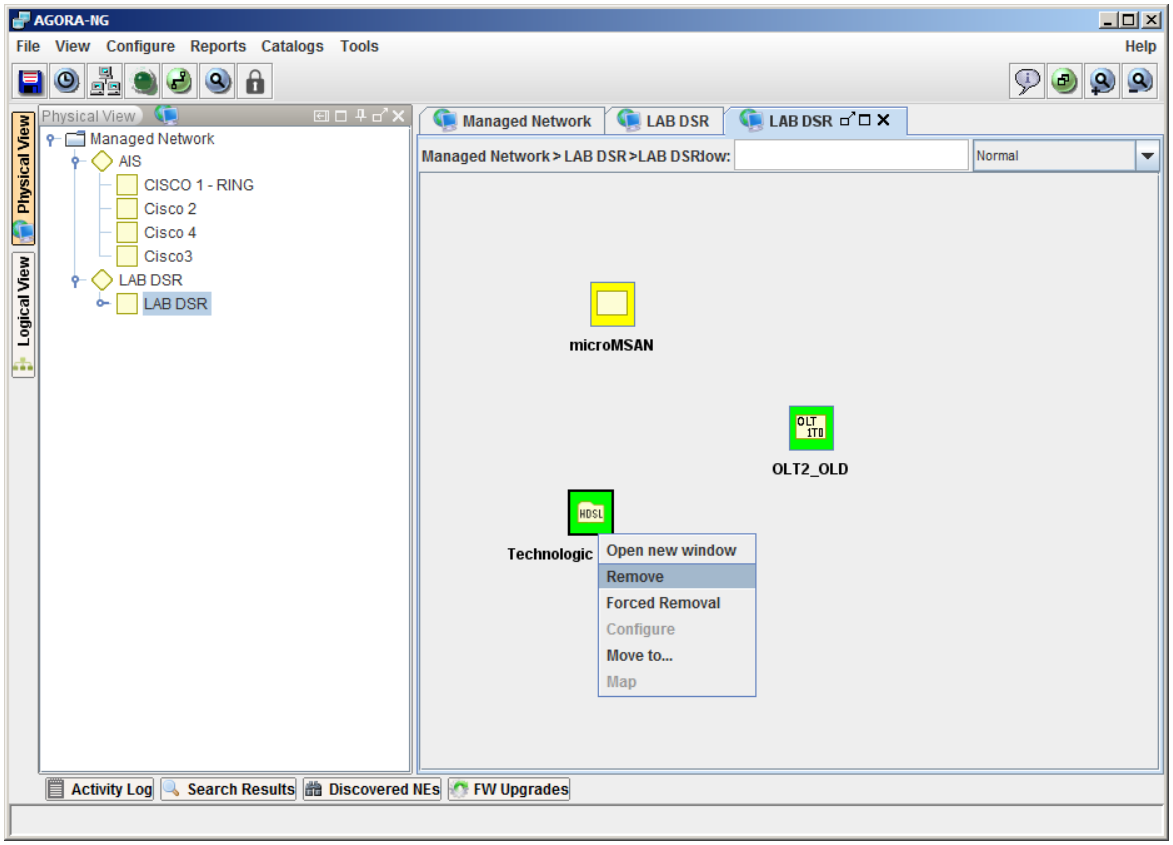
In order to insert a Technologic Group, from the main window select Configure → Topology → Insert → Group → Technologic Group. In the window shown in Figure 67, assign a name and its type to the Technologic Group, and choose the site where to create Technologic Group. The 'OK' button will bring up a window showing the new created Technologic Group.

Figure 67. Inserting a Technologic Group



In order to remove a Technologic Group, right-select the Technologic Group to be removed and select option 'Remove'.

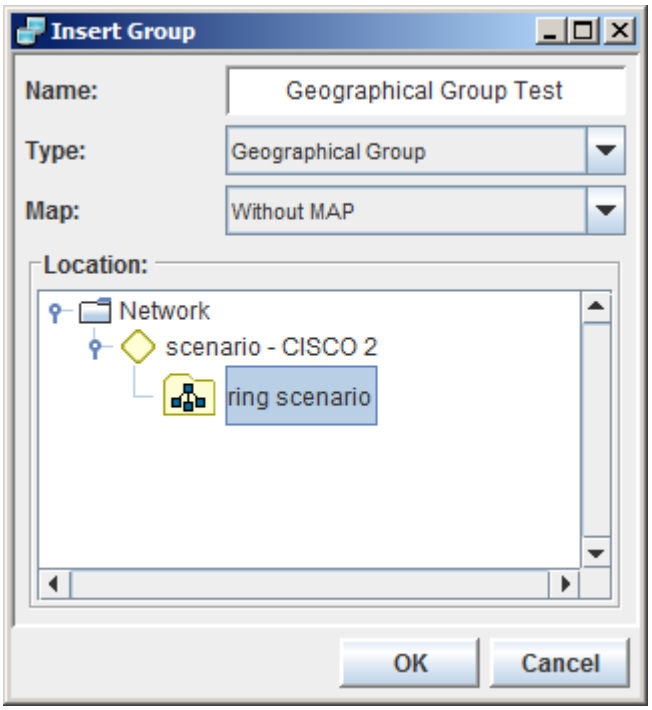
Figure 68. Removing a Technologic Group



Geographical Group

In order to insert a Geographical Group, from the main window select Configure → Topology → Insert → Group → Geographical Group. In the window shown in Figure 69, assign a name and its type, the background Map and choose the parent entity where to create it. The 'OK' button will bring up a window showing the new created Geographical Group.

Figure 69. Inserting a Geographical Group

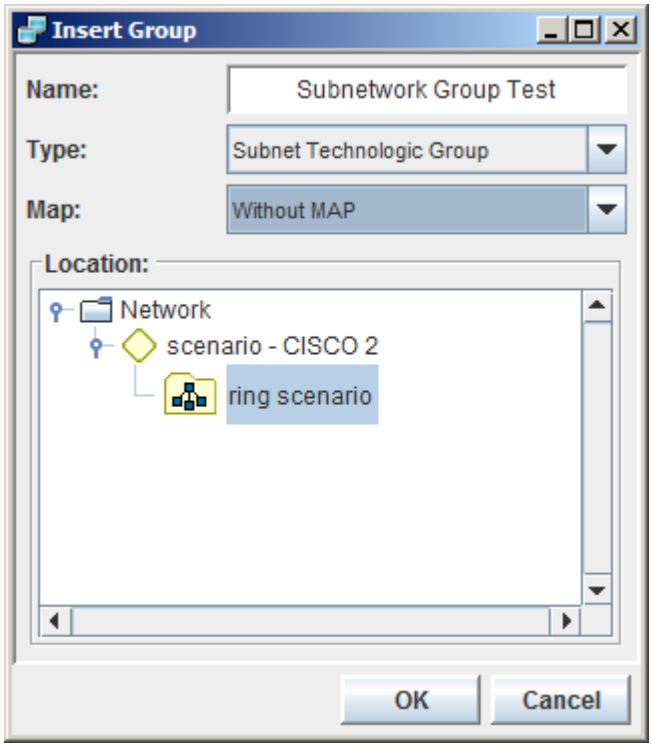


The process of removing a Geographical Group is identical to removing a Technologic Group (Technologic Group section).

SubNetwork Group

In order to insert a Sub Network Group, from the main window select Configure → Topology → Insert → Group → SubNetwork Group. In the window shown in Figure 70, assign a name and its type, the background Map and choose the parent entity where to create it. The 'OK' button will bring up a window showing the new created Sub Network Group.

Figure 70. Insert group



The process of removing a Sub Network Group is identical to removing a Technologic Group (Technologic Group section)

Network Element

The procedures for inserting a Network Element are described in detail, in section Inserting Network Elements.

Links

Depending on the type of technology managed, the application allows the creation of various types of links (PDH, SDH, Ethernet, SHDSL, MPLS, etc). This will vary on the type of element managed by the Assure Pack module and the type of network to be constructed. In many cases, the application even allows the creation of more than one type of link on the same managed element.

For more details on link configuration refer to specific Service Manager Manual.

Parameterization

Alarms

The alarm parameterization function may be accessed from the main application window, by selecting Configure → Parameterization → Alarms.

It is possible to parameterize an alarm by Alarm Type or by Equipment Type (Managed Element Type, Board Type or Port Type).

Alarm Type Parameterization

All alarms of the selected Category Alarm will be presented allowing configuration changes of one or more alarm parameter columns.

It is possible to create a new Alarm Category (new type of alarm) and new alarms.

Figure 71. Create alarm category

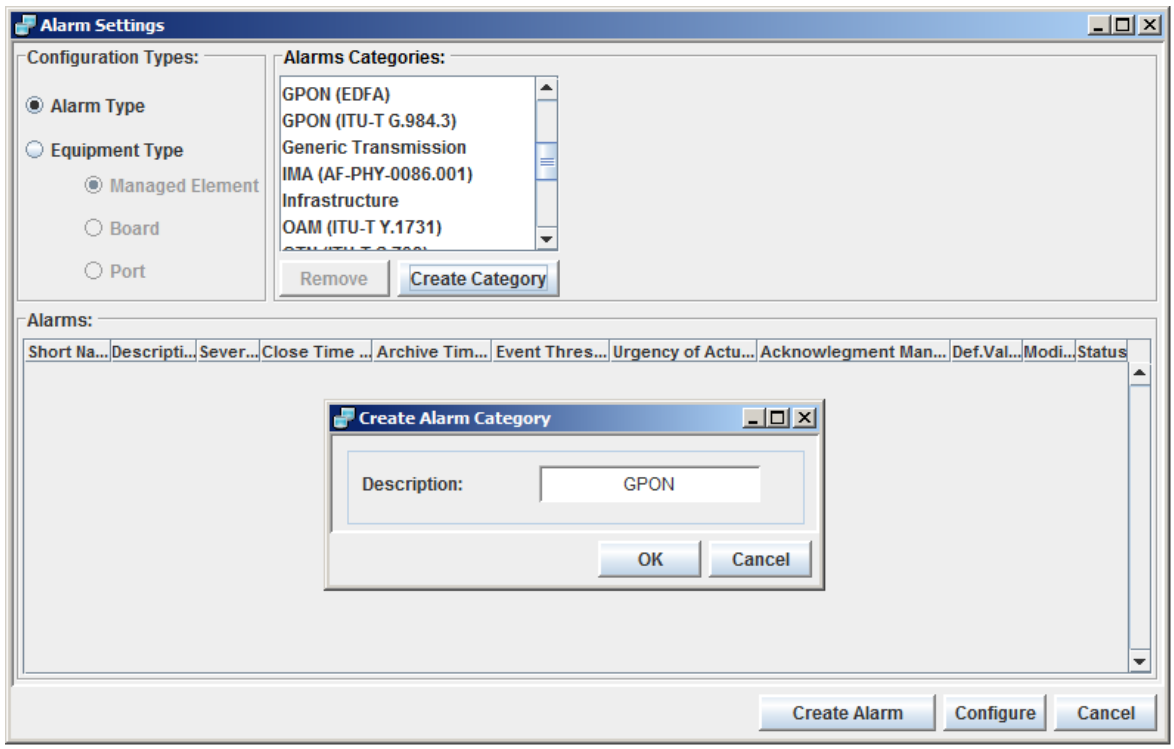
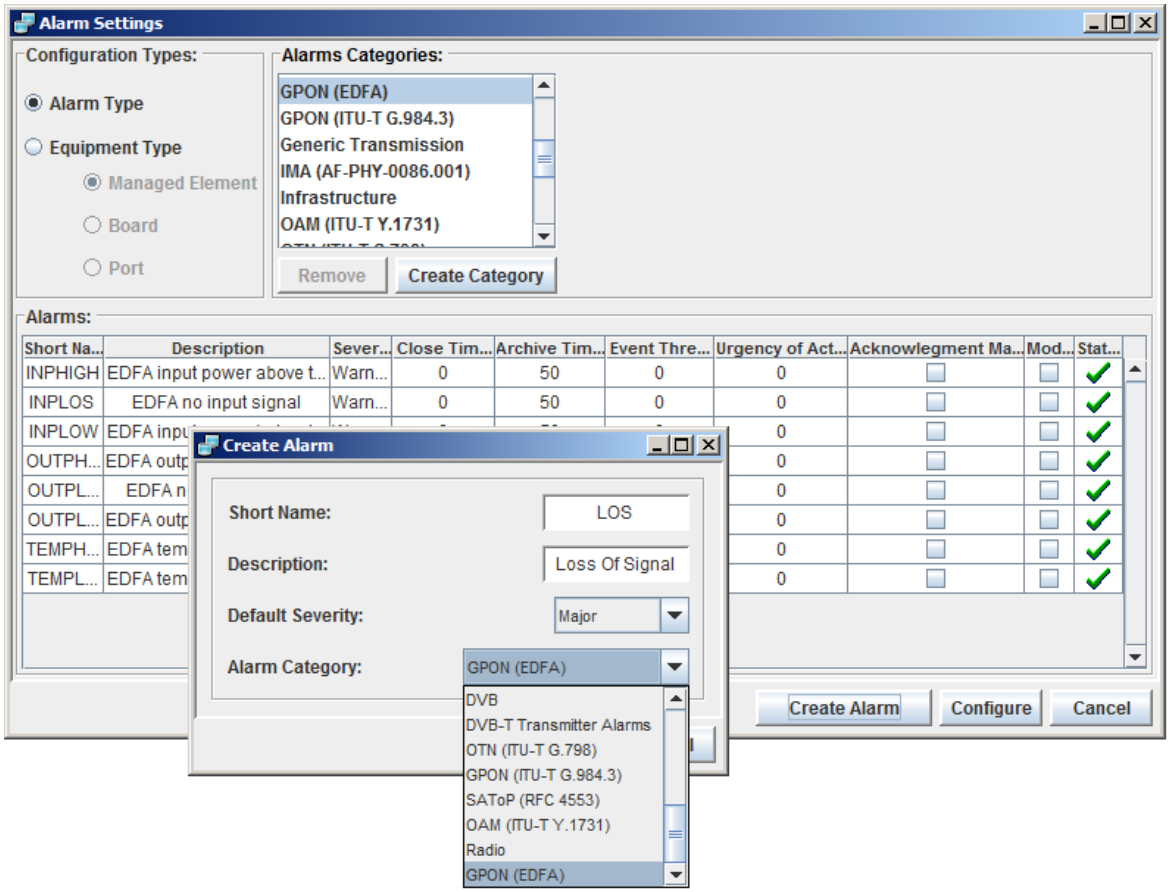


Figure 72. Create Alarm



Equipment Type Parameterization

All alarms of the selected Entity Type (Managed Element, Board or Port) will be presented allowing configuration changes on one or more alarm parameter columns.

Configuration changes will take effect selecting ‘Configure’.

The more significant configurable parameters are:

- Severity: severity level of the event alarm that has been registered;
- Close Time (m): the time after which the alarm will end automatically (when it doesn’t already have an end time);
- Archive Time (s): once the alarm has ended, this is the additional waiting time before the alarm leaves the alarm window (the alarm is archived);
- Event threshold: number of same-seriousness threshold events after which the urgency of action level is automatically increased, even when this has not been reached. If this occurs before the urgency of action is tripped, it automatically resets the urgency of action time;
- Urgency of Actuation: time for which a given seriousness level is maintained before passing to the next seriousness level. If this occurs before the event threshold is reached, the event threshold counter is reset;
- Acknowledgement Mandatory: indicates whether or not the alarm requires acknowledgement.

The configuration parameters can be changed in the following way:

- Severity: Selecting the cell in the 'seriousness' brings up a list from which the value for this parameter may be selected
- Close Time
- Archive Time
- Event threshold
- Urgency of Actuation: Double select on the cell for the parameter that is to be changed and input the required value
- Acknowledgement Mandatory: Select the tick to activate the functionality or clear the tick to deactivate it.

The 'Modify' field indicates which lines in the alarm table are going to be affected when the user confirms the configuration.

An 'X' in the 'Status' field indicates which lines have been changed by the user since the information was first loaded into the window. In other words, it indicates which lines now have a different configuration from that stored in the database. A '√' indicates that the shown configuration of the alarm is the same as in the database.

To execute the configuration changes made in the window, select 'Configure'. If the configuration change is successful the 'Status' icon will change from X' to '√', thus indicating that the information in the table is now consistent with database information.

Performance

The performance parameters configuration function may be accessed:

- From the main application window, selecting Configure → Parameters → Performance;
- It is possible to parameterize an alarm generally by Port Type or by a specific Equipment Type Port.

The more significant configurable parameters are:

- Measurement Interval (min): the time interval between measuring performance data.
- Threshold ES (s): error threshold ('errored seconds') beyond which an alarm warning of the situation will be triggered.
- Threshold SES (s): error threshold ('severe errored seconds') beyond which an alarm warning of the situation will be triggered.
- Threshold UA (s): error threshold ('unavailable seconds') beyond which an alarm warning of the situation will be triggered.

The configuration parameters can be changed in the following way:

- Measurement Interval: Selecting the cell in the 'Measurement Interval' brings up a list from which the value for this parameter may be selected.
- Changes on:
- Threshold ES
- Threshold SES
- Threshold UA

Can be made double selecting the cells to be changed and input the required value.

The ‘Modify’ field indicates which lines in the table are going to be affected when the user confirms the changes.

An ‘X’ in the ‘Status’ field indicates which lines have been changed by the user since the information was first loaded into the window. In other words, it indicates which lines now have a different configuration from that stored in the database. A ‘√’ indicates that the shown configuration of the alarm is the same as in the database.

To add new values (blank lines) to the table, select on ‘Add’ and input the required configuration.

To execute the configuration changes made in the window, select ‘Configure’. If the configuration is successful the ‘Status’ icon will change from X’ to ‘√’, thus indicating that the information in the table is now consistent with that in the database.

To remove lines form the table, select on ‘Remove’.

‘Configure’ must be chosen to effective changes.

Circuits

Depending on the type of technology managed, the application allows the creation of various types of circuits, which will later be associated to ports and cross connections of network managed elements. It is possible to configure a circuit by assigning it with a name, a type, a client and termination and intermediate ports.

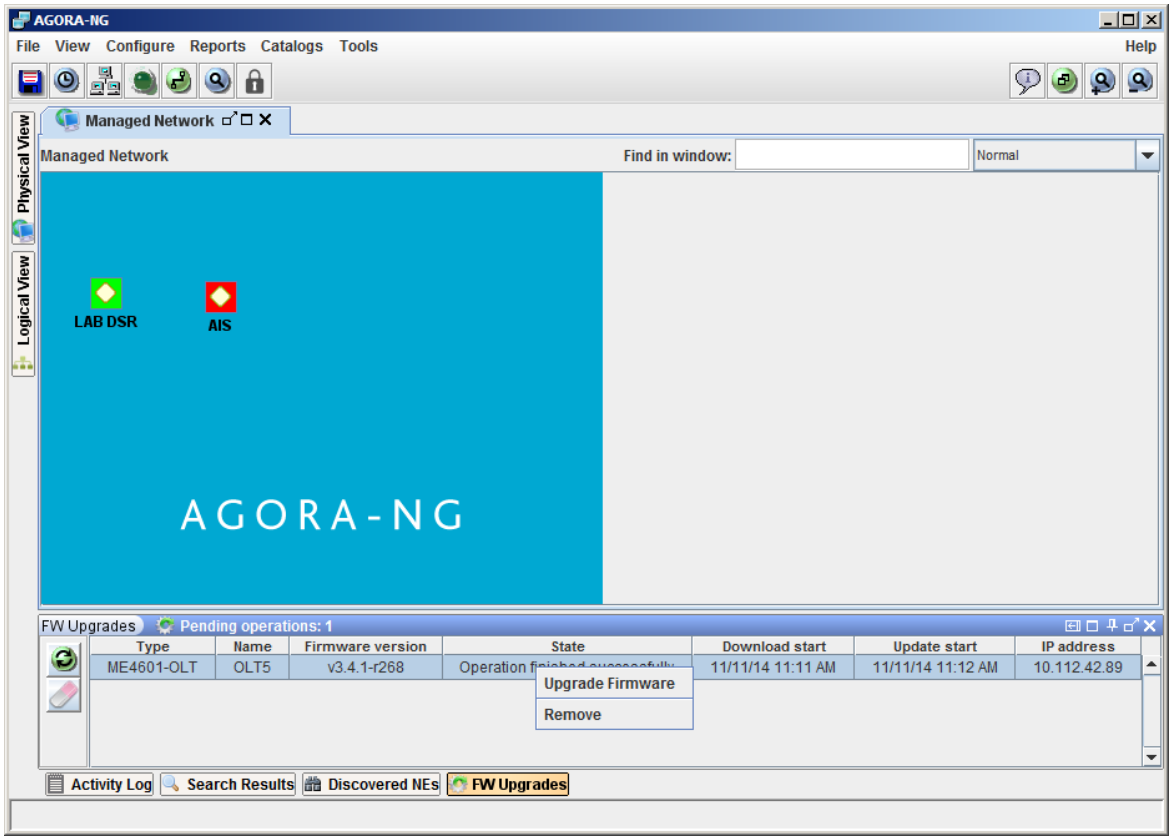
For more details on circuit configuration refer to specific technology Service Manager manual.

Download Firmware

Depending on the type of technology managed, the application allows the download of a specific firmware version file to the network managed element. A firmware download details window will be displayed indicating the state of the operation window (Figure 73).

For more details on Download Firmware refer to specific Service Manager Manual.

Figure 73. Download Firmware



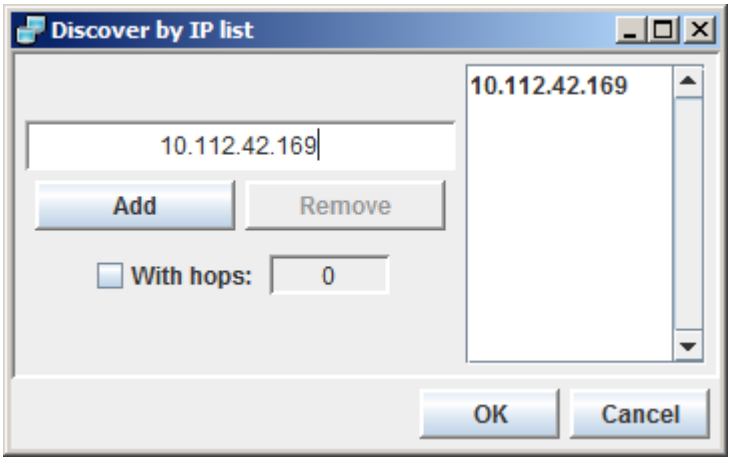
Network Element

Network Elements discovery using SNMP agents

In order to discover a Network Element (NE), from the main application menu, select Configure → NE Discovery or, in the toolbar, select 'Discover NE by IP address' ( ) icon.

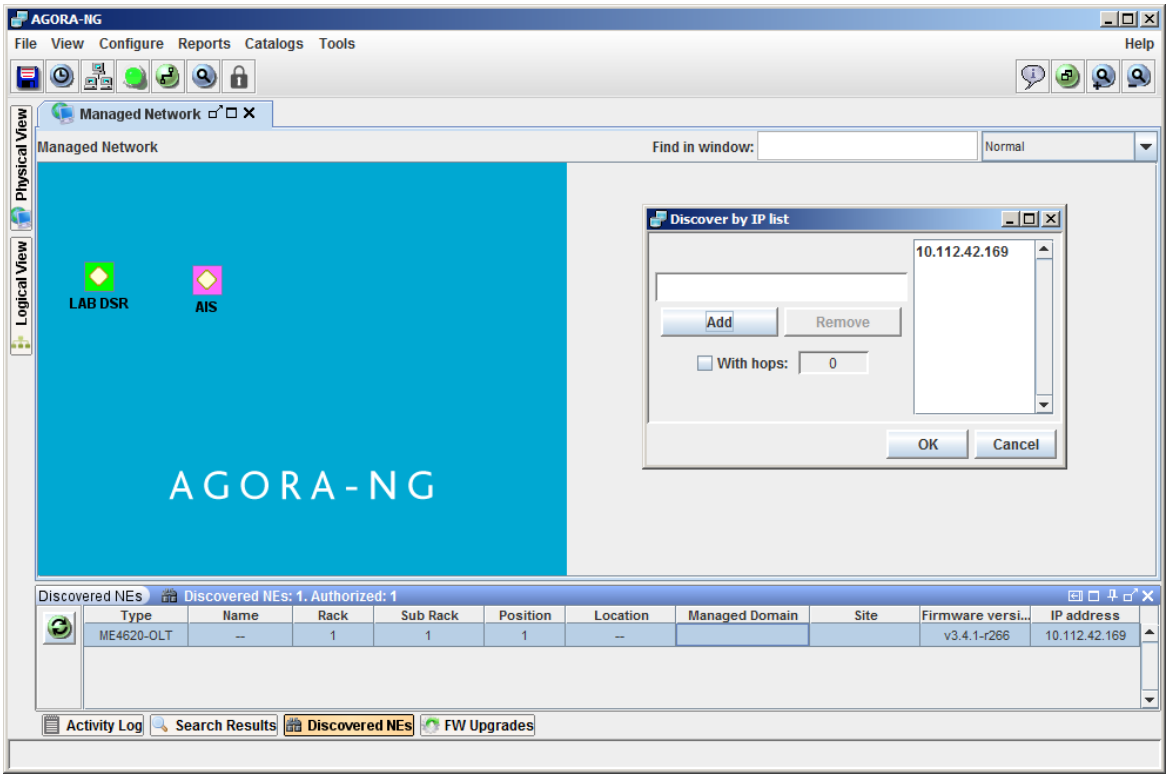
In the 'Discover by IP list' window, shown in the next figure, add IP addresses, to be discovered, to the list. Then select OK to execute the operation.

Figure 74. Discover by IP list



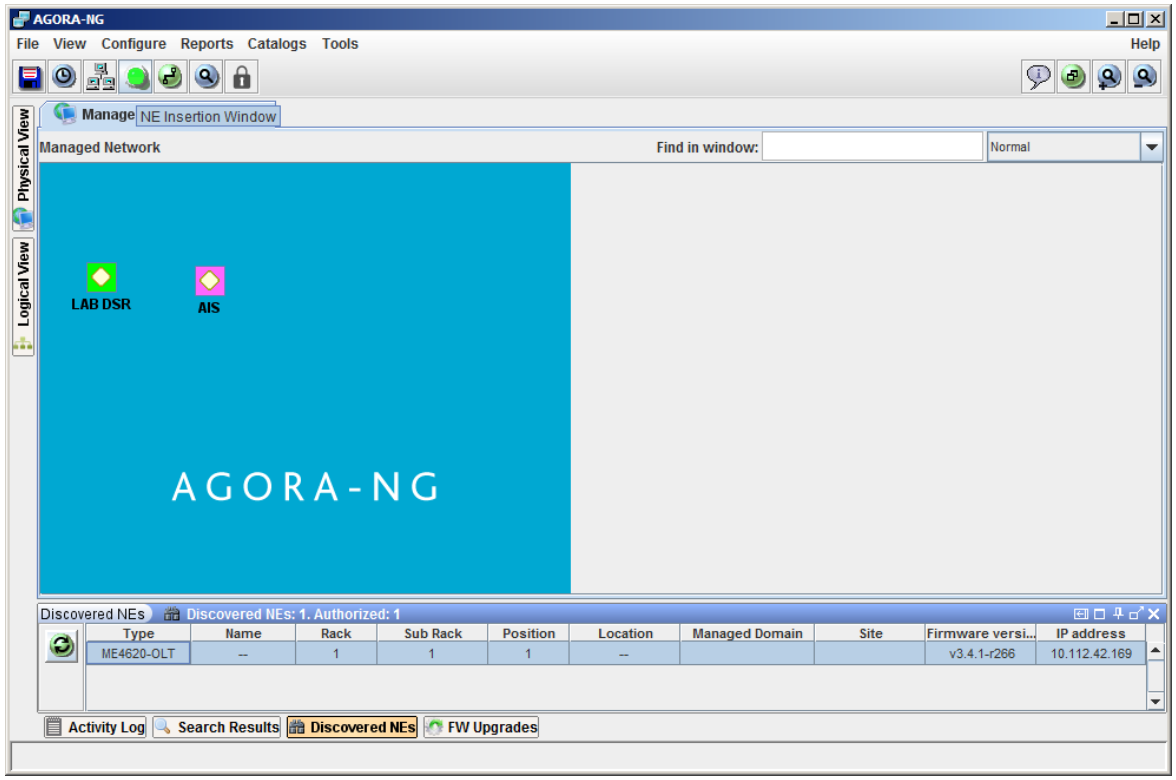
In the window shown in Figure 75, it is possible to discover a list of Network Elements by IP, which will be shown in the 'Status Bar' 'Discovered NEs' panel.

Figure 75. NE Discovery



As Network Elements are discovered, on the network, the relevant data will be added to the 'Discovered NEs' panel window (Figure 76) and the associated icon in the main menu will change to light green ( ), indicating that NEs have been successfully discovered.

Figure 76. Insertion window for discovered NEs



Inserting Network Elements

In order to insert a Network Element, from the main window select Configure → Topology → Insert → Network Element → Discovered. A Network element can be inserted manually or after being automatically discovered.

Manual Insertion

Manual Insertion of a network element is not possible in all technologies. Unlike 'Insertion by discovery' a manually inserted managed element hasn't been discovered on the network yet. This operation only stores network element physical information into database (inventory information), it is not associated with any network resource. Later on, this element will be put on 'service' and actually managed in the network. For more detailed information of this functionality please refer to the Service Manager Manual for the specific technology.

To enter a network element into the database base inventory select from the main menu Configure → Topology → Insert → Network Element → Manual.

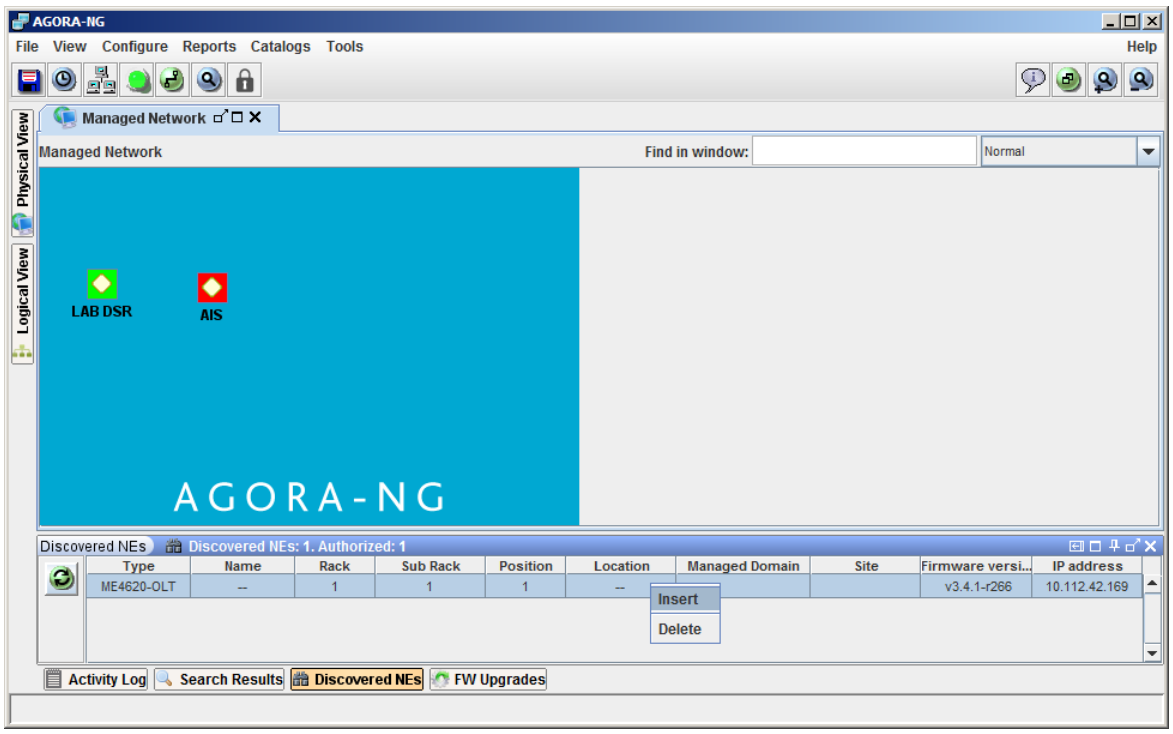
Insertion by Discovery

To insert a network element by discovery the network element must have been previously successfully discovered.

To insert a discovered network element select the 'NE Insertion Window' icon ( ) or on the main menu, Configure → Topology → Insert → Network Element → Discovered. This will bring up the Panel window for Discovered NEs. The network element to be inserted must be on this list.

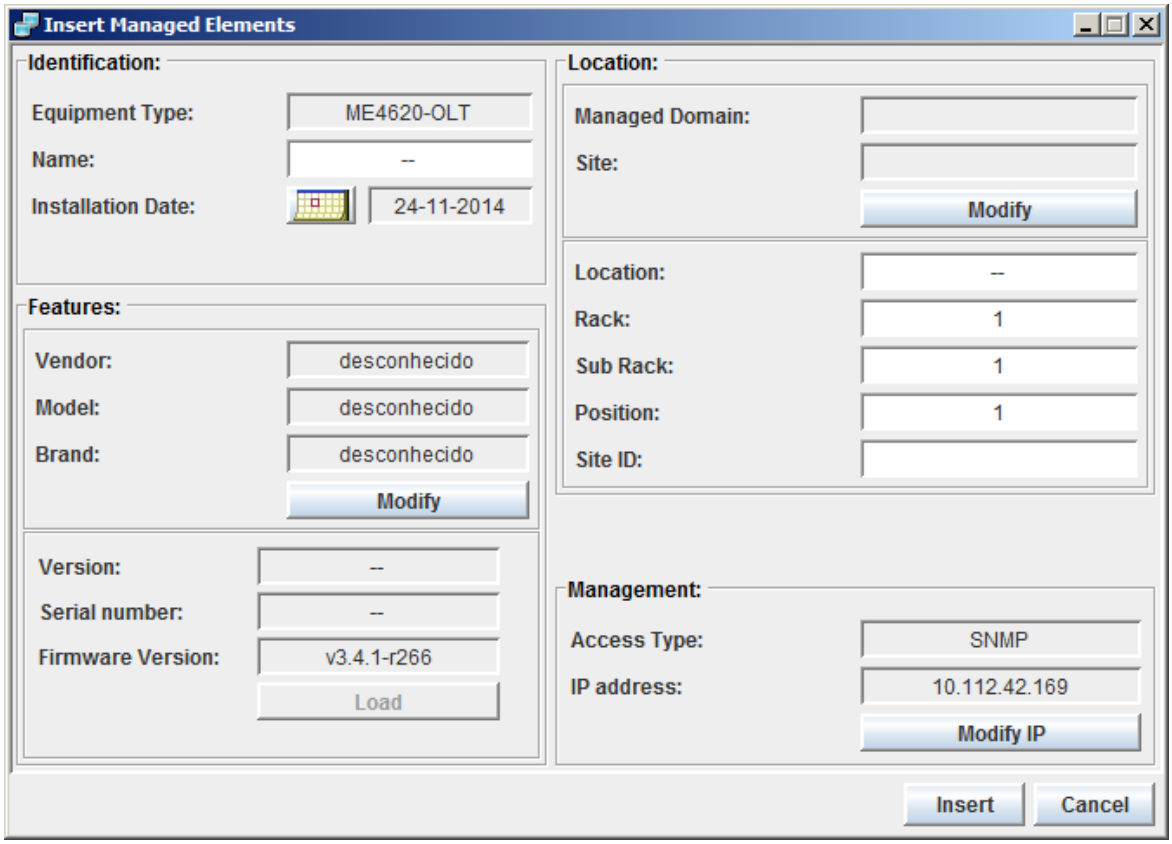
A NE can be selected for insertion or deletion, Figure 77.

Figure 77. Insertion of discovered NEs



From the list that is displayed right-select to select the element to be inserted and select 'Insert'. This will bring up the managed element insertion window, which needs to be filled in with network element physical information.

Figure 78. Insertion window details for discovered NEs



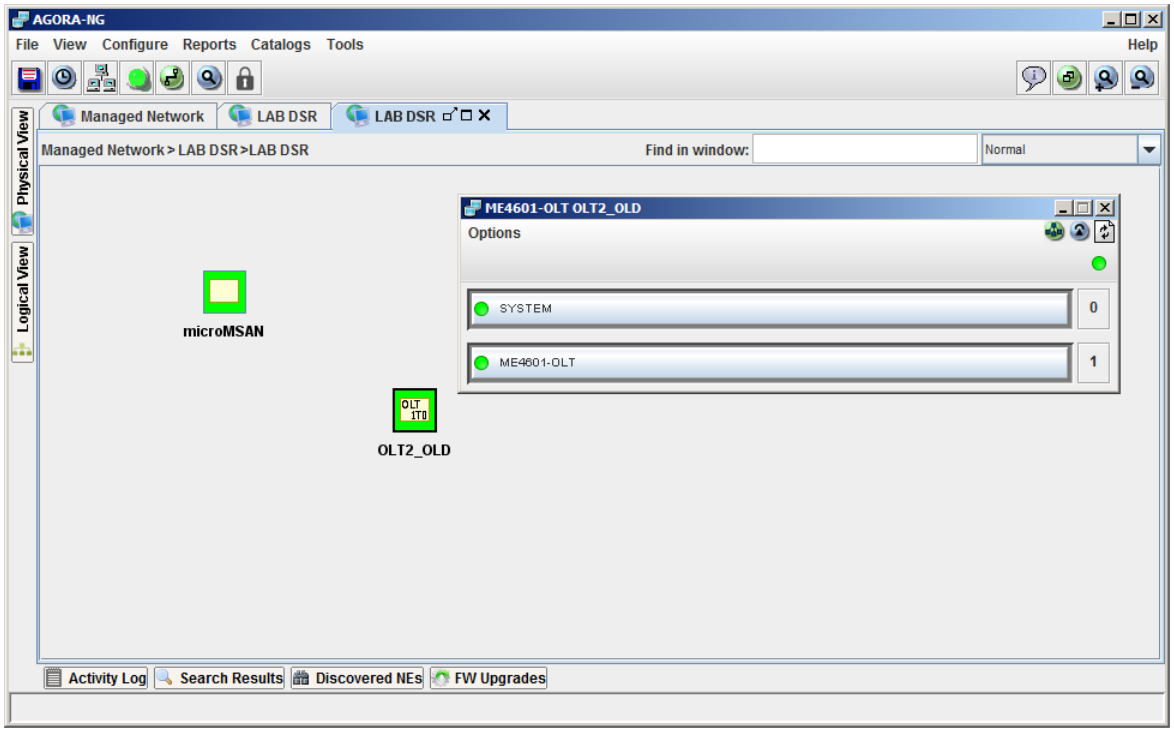
Looking up Network Elements

To look up for a network managed element a View panel (Physical, Logical or Management) must be selected.

In the window shown in Figure 79, navigate through the tree, opening the various levels of Managed Domains, Sites and Groups, until the element is found. Left-select on the network element icon and the application will then bring up the network element window.

Alternatively a short cut can be used to search a network element, selecting the icon at the top of the main window, or using 'Ctrl+F' key sequence.

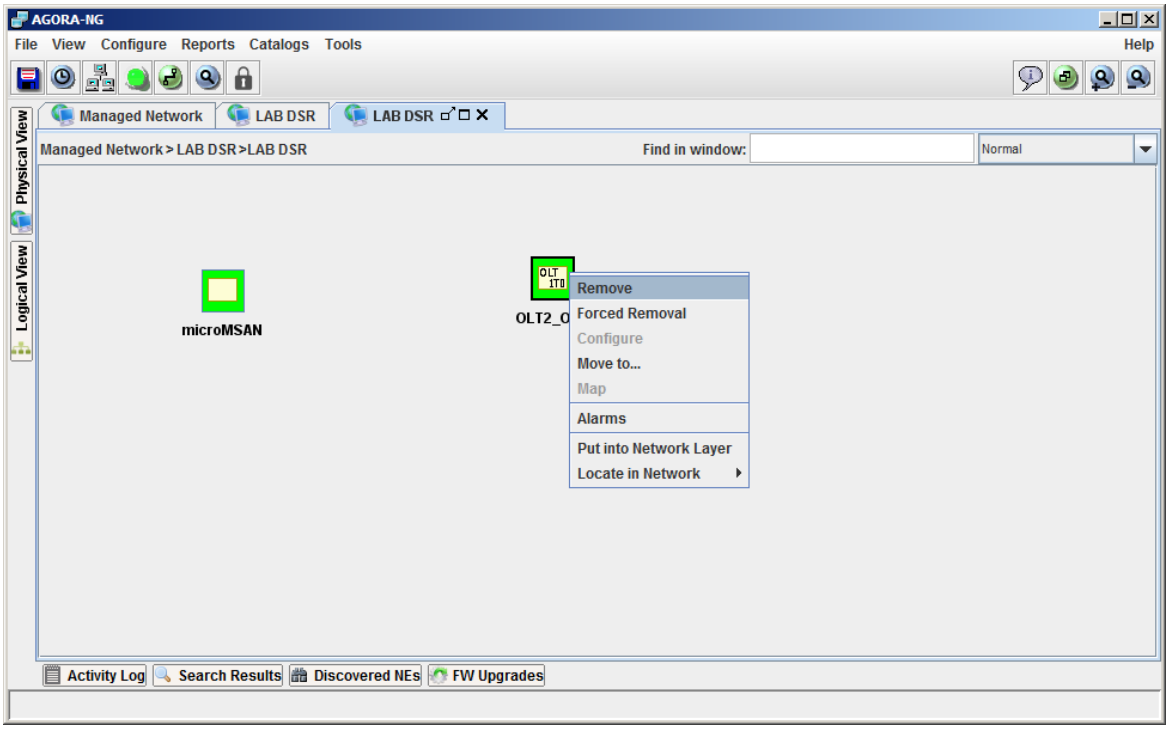
Figure 79. Looking up a network element



Removing Network Elements

A network element can be removed right-selecting the network element icon and choosing ‘Remove’, (Figure 80).

Figure 80. Removing a device



There are some restrictions on removing network elements. For detailed information please refer to specific Service Manager Manual technology.

Network Element removal may also be forced (select 'Force Removal' from the menu) when, for example, the element has been physically removed from the network but it is still registered in the management system database. For more detailed information please refer to specific Service Manager Manual technology.

Moving Network Elements

To move a network element, right-select on the icon representing the element in the map and select 'Move to…' (Figure 81). This will bring up a window displaying the tree of all elements in the network organization (managed domains, Sites and Groups) to which the element can be moved (Figure 82).

Figure 81. Moving a network element

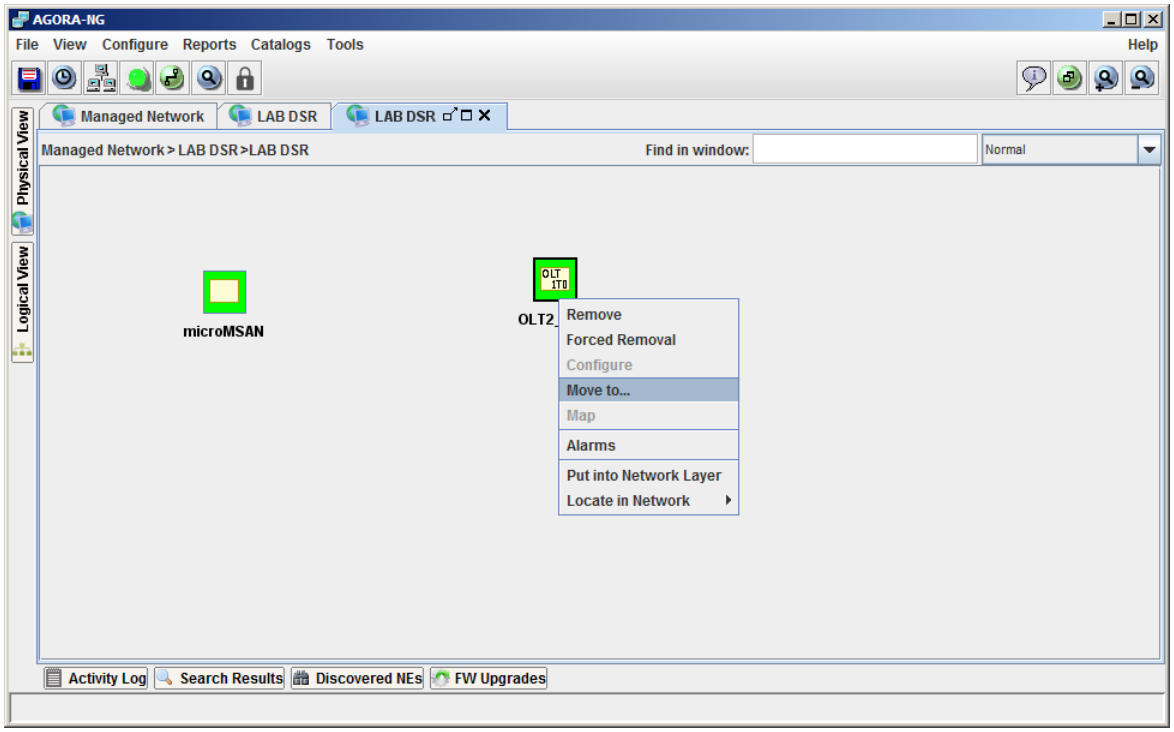
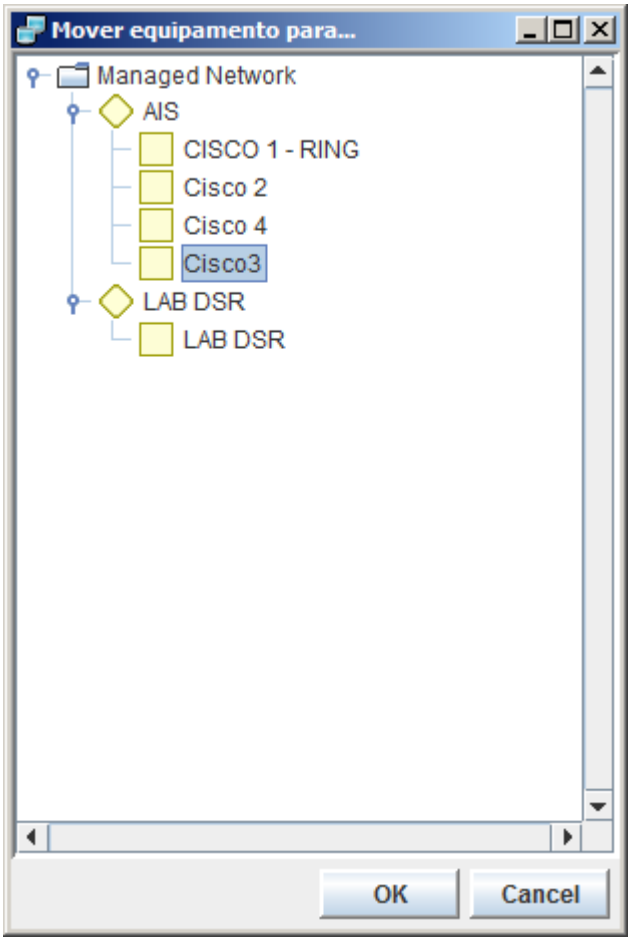


Figure 82. Moving a network element

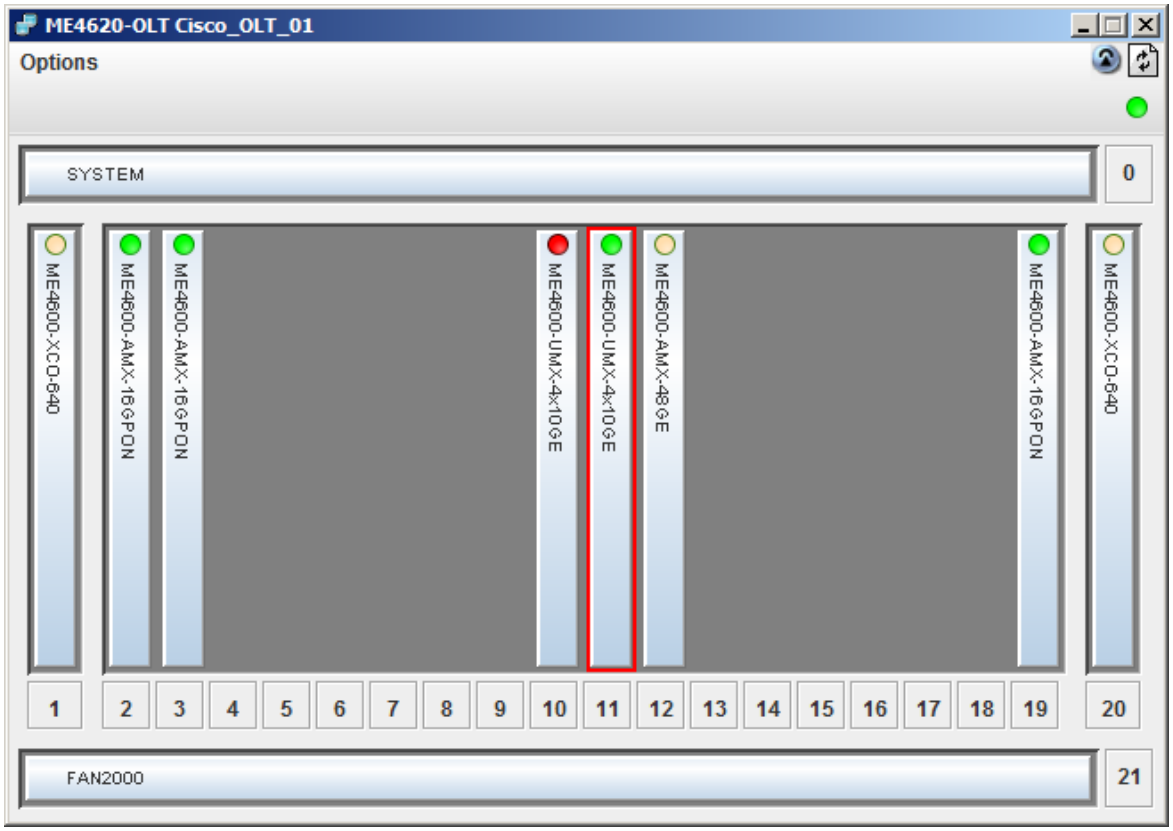


Configuring Network Elements

Network Element Window

The appearance of the network managed element window depends on the network element type, the number of boards it contains, its physical configuration and the configurations that can be applied on it. However, the window will always display the set of boards of which the managed element is composed, as exemplified in Figure 83.

Figure 83. Device window



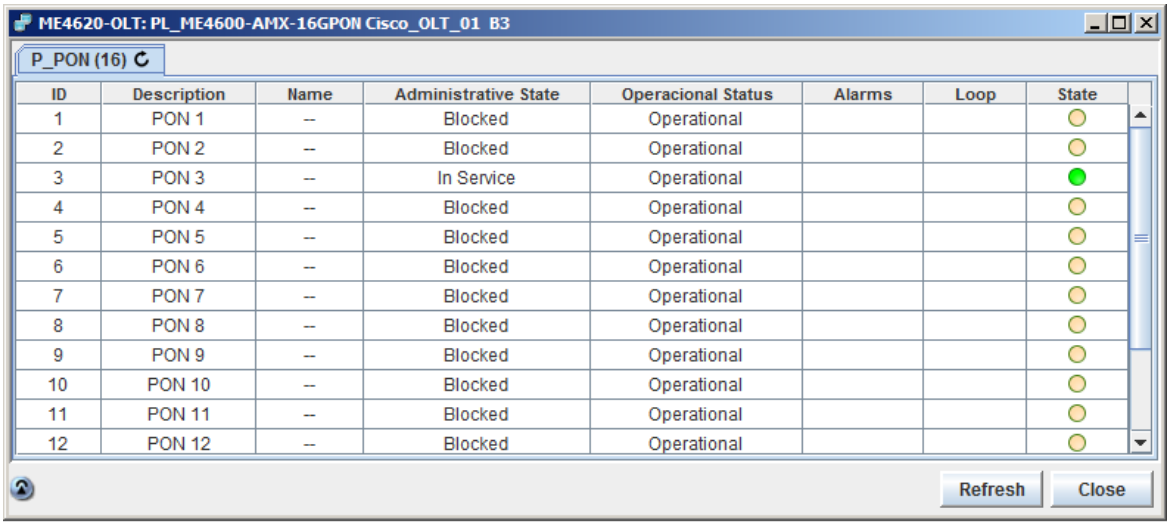
The colored icon ( ) on the upper right-hand corner of the window (**Figure 83**) indicates network element status. The icon on each board indicates the worst state of all the contained ports.

On the upper right-hand corner of the window (**Figure 83**) icon ( ) allow access to the managed element representation on the two physical and logical views.

The "Refresh" ( ) updates network managed element information.

To see the ports on each board, double-click on the board. In each board's ports window, the network element window may be displayed by selecting the button ( ), in the lower left-hand corner. To configure a port right-select it, a pop-up menu with specific configuration options, will appear.

Figure 84. A board's ports window



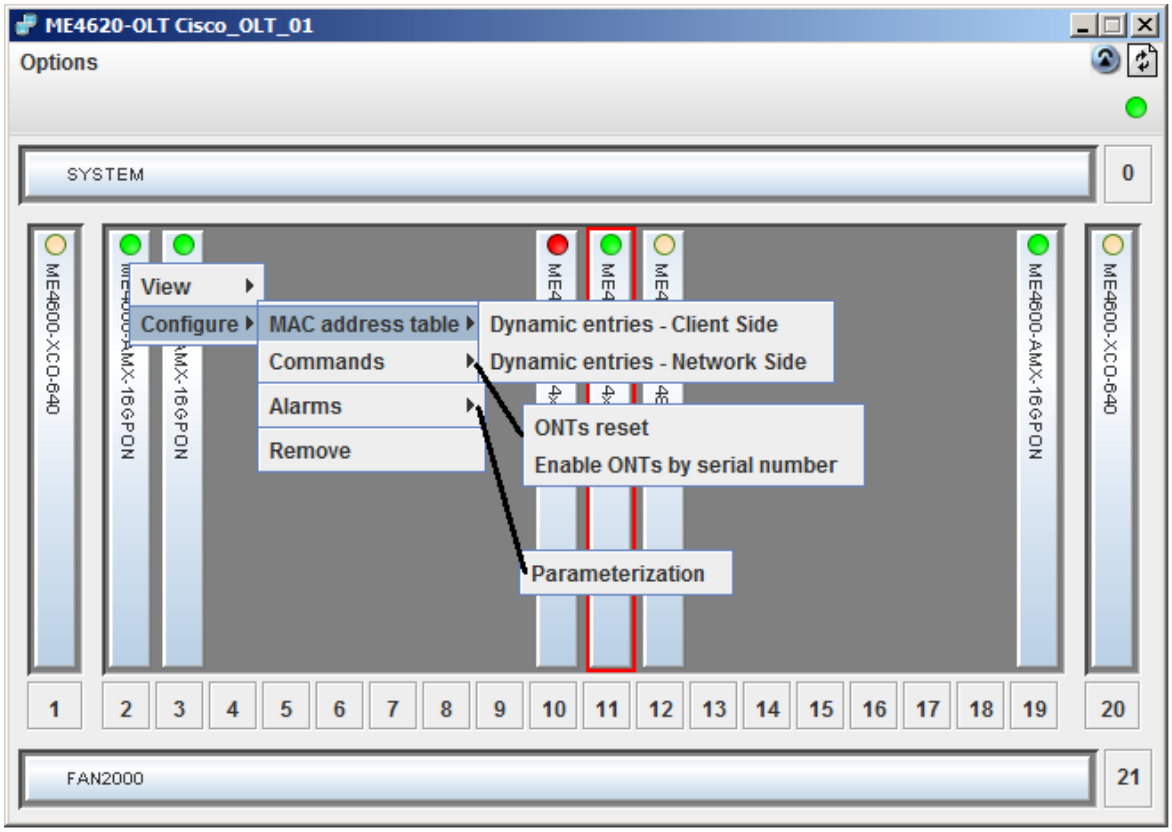
ID	Description	Name	Administrative State	Operacional Status	Alarms	Loop	State
1	PON 1	--	Blocked	Operational			
2	PON 2	--	Blocked	Operational			
3	PON 3	--	In Service	Operational			
4	PON 4	--	Blocked	Operational			
5	PON 5	--	Blocked	Operational			
6	PON 6	--	Blocked	Operational			
7	PON 7	--	Blocked	Operational			
8	PON 8	--	Blocked	Operational			
9	PON 9	--	Blocked	Operational			
10	PON 10	--	Blocked	Operational			
11	PON 11	--	Blocked	Operational			
12	PON 12	--	Blocked	Operational			

The "Refresh" button will update the data in the window, specifically the number of ports and the port data (name, status, alarms and loop status).

Configuration Operations

Network elements may be configured at three levels: managed element, board and port. The possibility of carrying out these operations depends on the type of network element, type of board and type of port. For more detailed information of a port of a specific technology refer to the specific Service Manager Manual technology.

Figure 85. Network element configurations



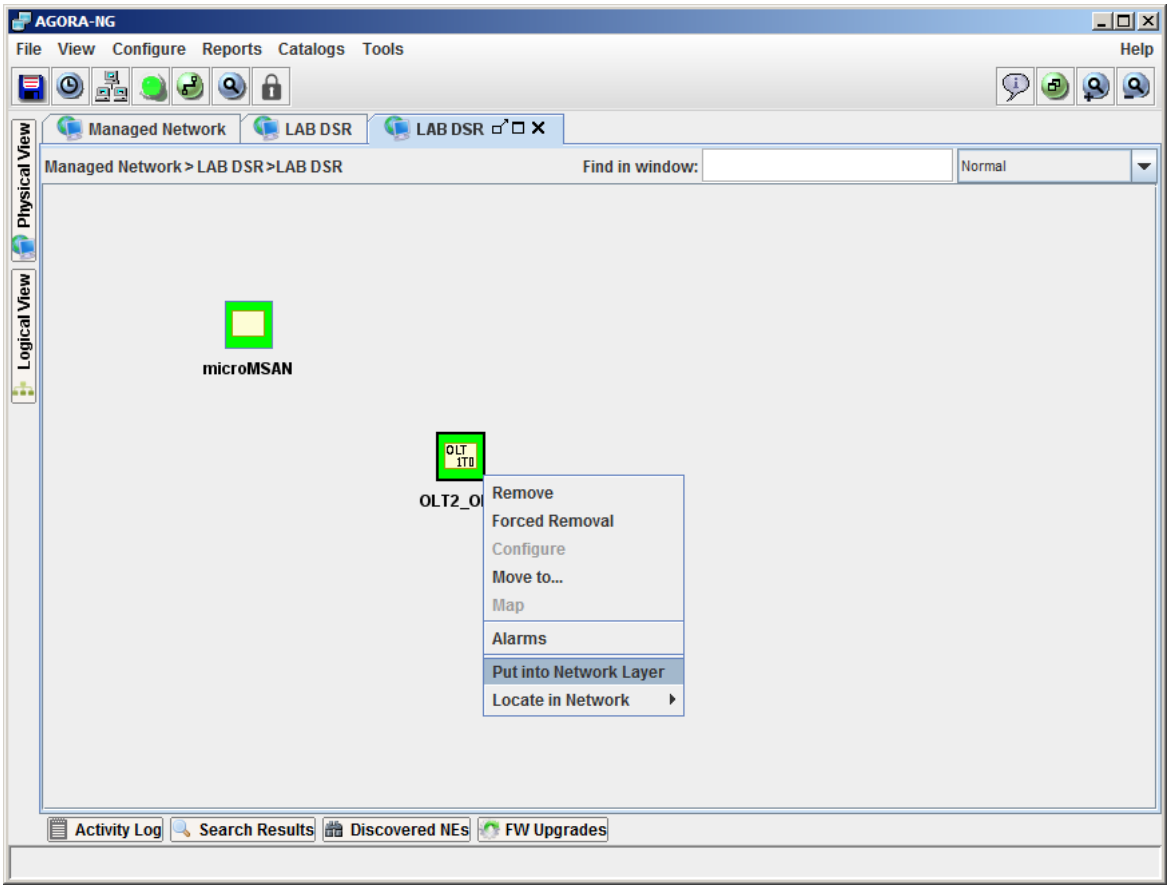
Network level configuration

Placing Network Elements at the Network Level

A network managed element previously inserted in Physical View level can be represented on the network level (Logical view).

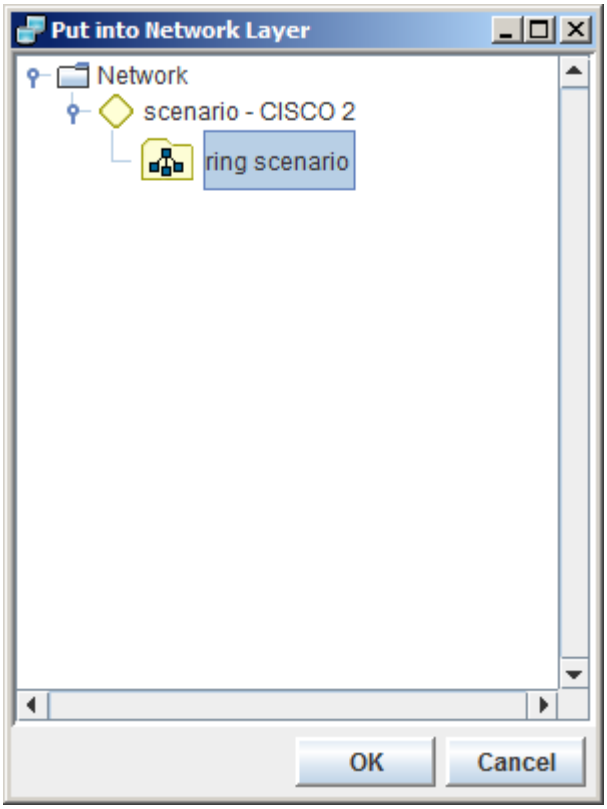
In the Physical View panel right-select the target managed element icon and then select “Put into Network Layer”.

Figure 86. Puting a device on the network



This will bring up the 'Put into Network Layer' window, as shown in **Figure 87**. Select the Managed Domain/Group where to represent the managed element in a network context. Select "OK" to confirm the operation.

Figure 87. Window for selecting the location of the device at the network level



This operation may be repeated as many times as necessary, and the same device may be placed in various locations at the network level.

Note that when a device is placed at the network level, only the graphical representation of this device will be created at the Logical View (network representation).

Reports Management

Reports

The reports platform is common to both Assure Pack and Provision Pack.

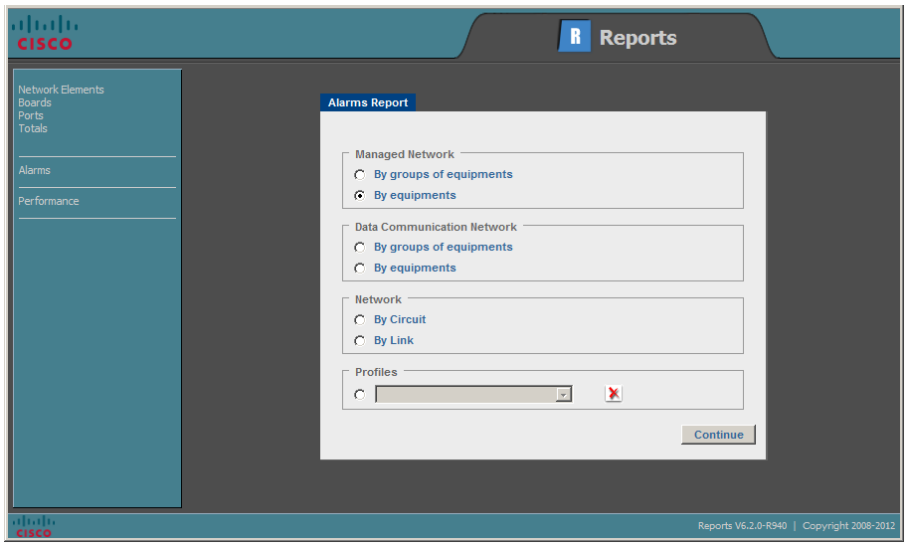
Most of the reports platform's functionalities can be accessed through the Reports menu in the main application window. It takes information stored in AGORA-NG database and presents it in an easy-to-read format, helping to analyze and interpret important information. Generated reports are displayed on the screen or can be exported to PDF and EXCEL format.

Alarms and Performance

Alarm and Performance data of network elements can be viewed by generating a report that can be triggered from each Managed Element option menu or via main application window (Assure Pack Module) or via

Reports Module. The information is presented chronologically for each performance interval collected or each alarm event, reported by the managed element (Figure 88 and Figure 92).

Figure 88. Alarms report window



In order to choose an available equipment (Figure 90) it is necessary to select “Equip” button in Figure 89.

Figure 89. Alarms report window “By equipments” example

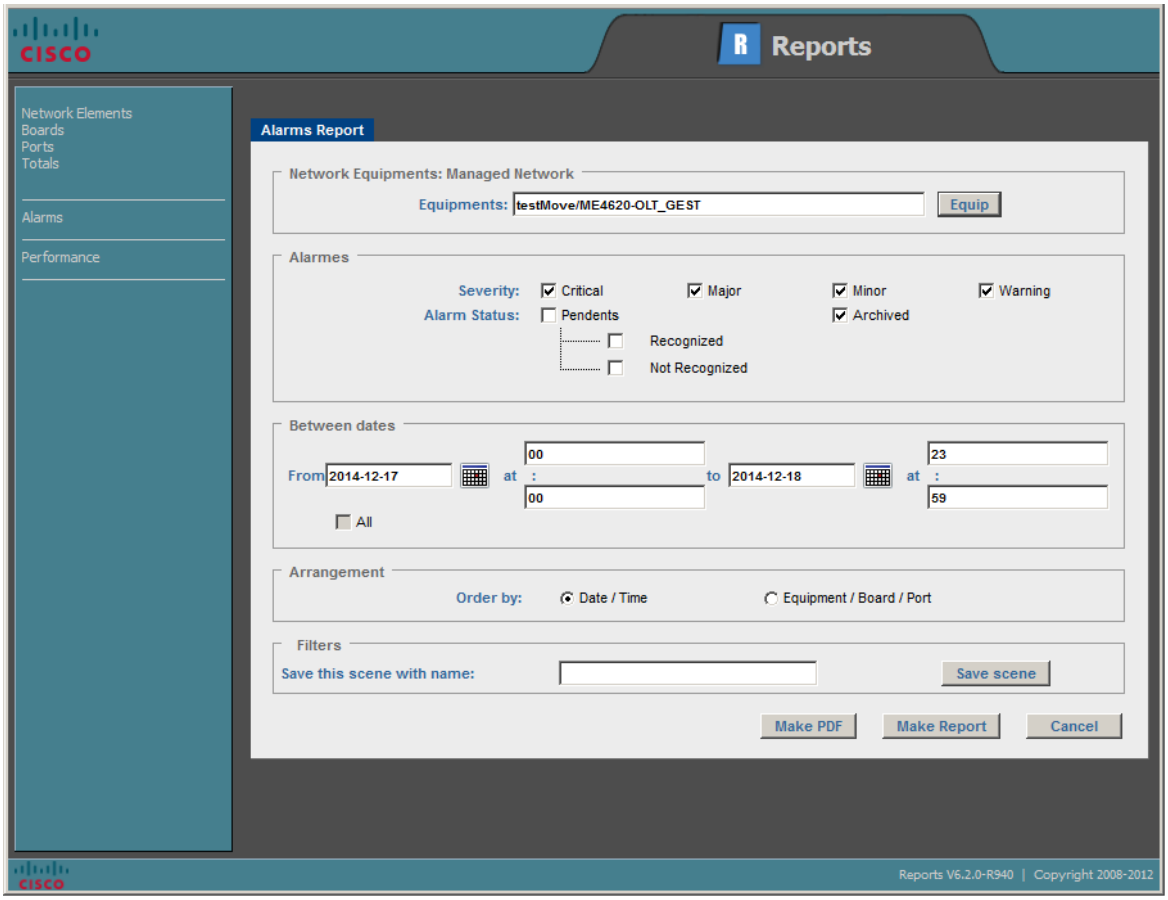
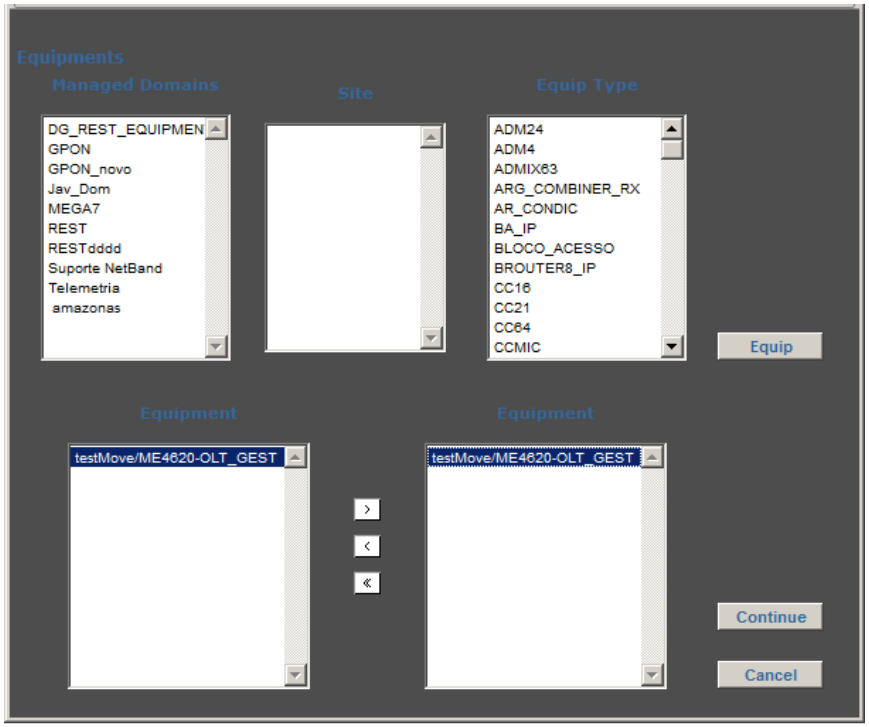
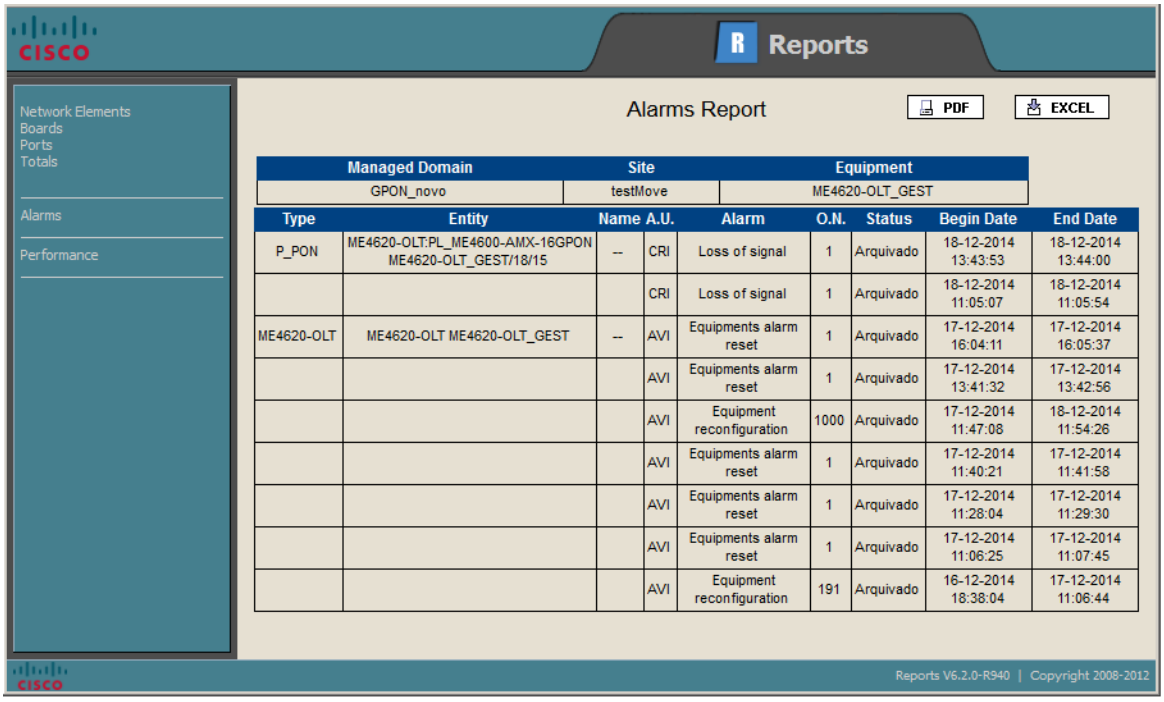


Figure 90. Alarms report window "By equipments" – equipment selection



In order to generate an alarms report (**Figure 91**) it is necessary to select "Make Report" button in **Figure 89**.

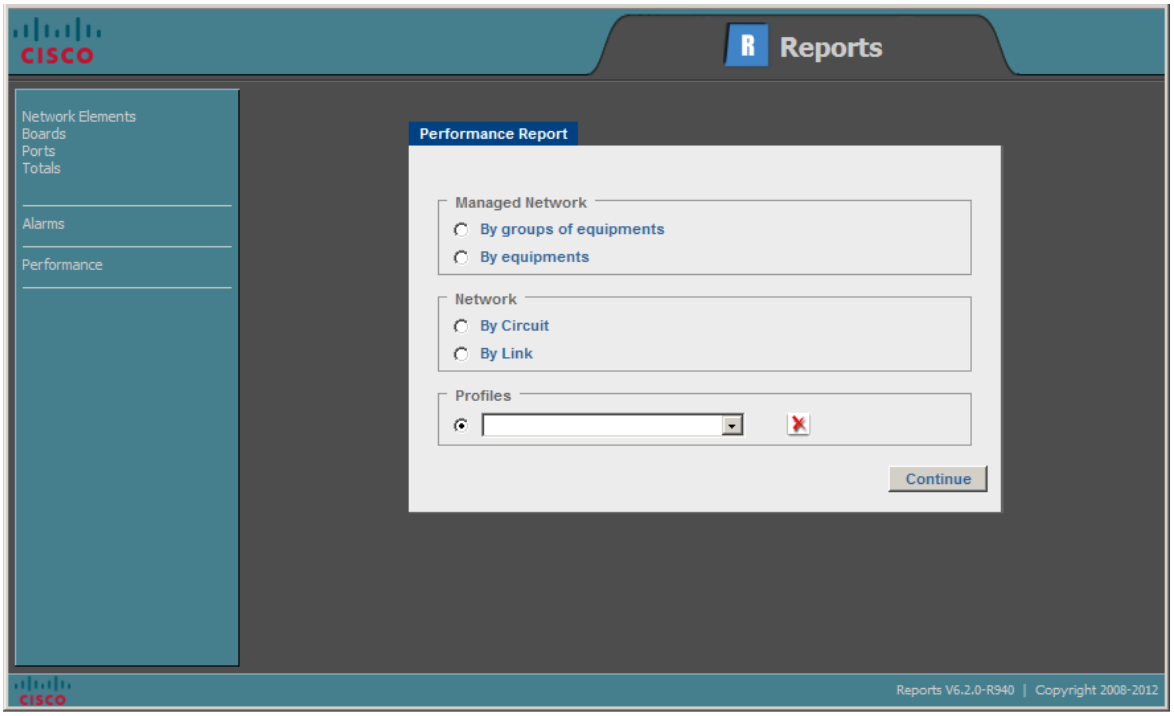
Figure 91. Alarms report window "By equipments" – reports list



Managed Domain	Site	Equipment
GPON_novo	testMove	ME4620-OLT_GEST

Type	Entity	Name	A.U.	Alarm	O.N.	Status	Begin Date	End Date
P_PON	ME4620-OLT:PL_ME4600-AMX-16GPON ME4620-OLT_GEST/18/15	--	CRI	Loss of signal	1	Arquivado	18-12-2014 13:43:53	18-12-2014 13:44:00
			CRI	Loss of signal	1	Arquivado	18-12-2014 11:05:07	18-12-2014 11:05:54
ME4620-OLT	ME4620-OLT ME4620-OLT_GEST	--	AVI	Equipments alarm reset	1	Arquivado	17-12-2014 16:04:11	17-12-2014 16:05:37
			AVI	Equipments alarm reset	1	Arquivado	17-12-2014 13:41:32	17-12-2014 13:42:56
			AVI	Equipment reconfiguration	1000	Arquivado	17-12-2014 11:47:08	18-12-2014 11:54:26
			AVI	Equipments alarm reset	1	Arquivado	17-12-2014 11:40:21	17-12-2014 11:41:58
			AVI	Equipments alarm reset	1	Arquivado	17-12-2014 11:28:04	17-12-2014 11:29:30
			AVI	Equipments alarm reset	1	Arquivado	17-12-2014 11:06:25	17-12-2014 11:07:45
			AVI	Equipment reconfiguration	191	Arquivado	16-12-2014 18:38:04	17-12-2014 11:06:44

Figure 92. Performance report window



Network Elements, Boards, Ports and Totals

To collect a comprehensive report of Network Elements managed (inventory report), their constitution (Boards, Ports) and Totals (total number of equipment), the Report Module provides these options that can be triggered, from main application window menu (Assure Pack Module) or via Reports Module (**Figure 93**, **Figure 94**, **Figure 95** and **Figure 96**). Reports may be generated per managed or data communication network, for equipment, boards and ports. Total Reports can be generated by managed domain or site.

Figure 93. Network Elements report window

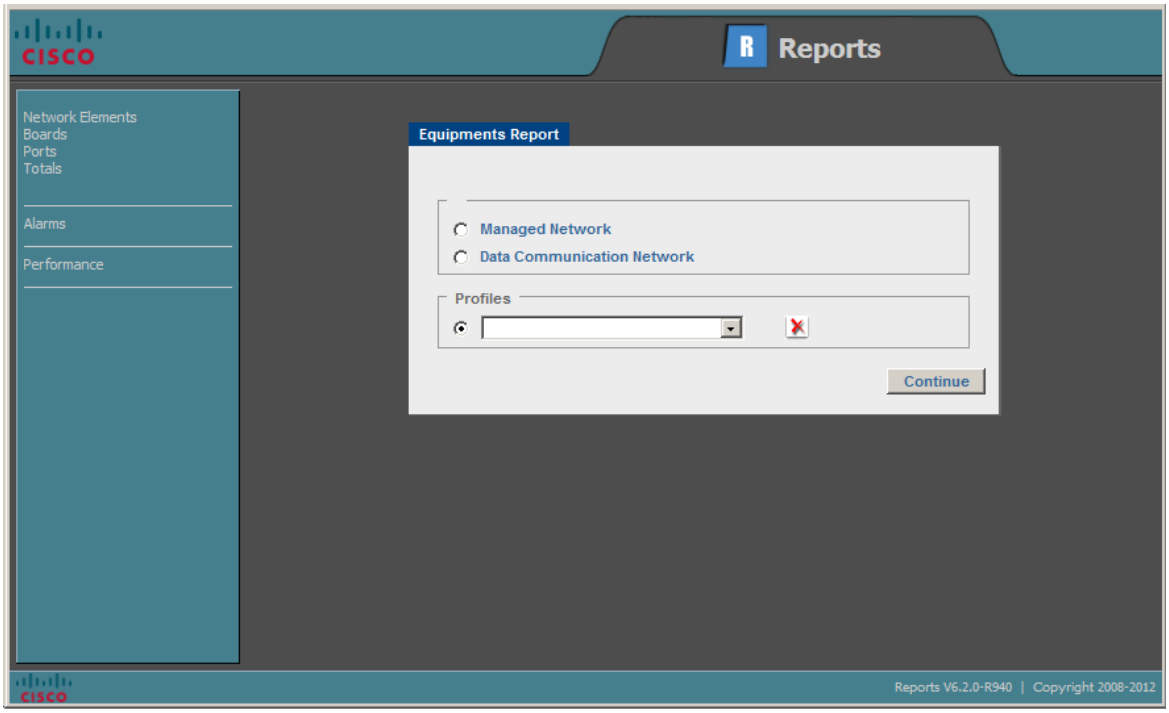


Figure 94. Boards report window

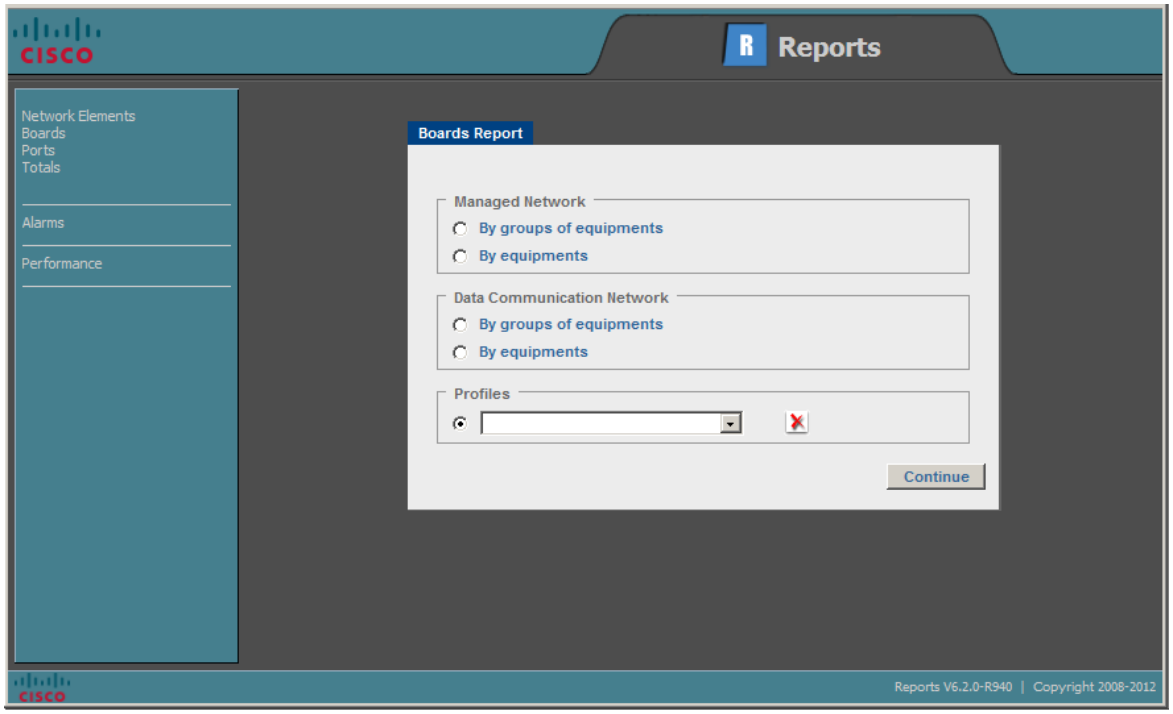


Figure 95. Ports report window

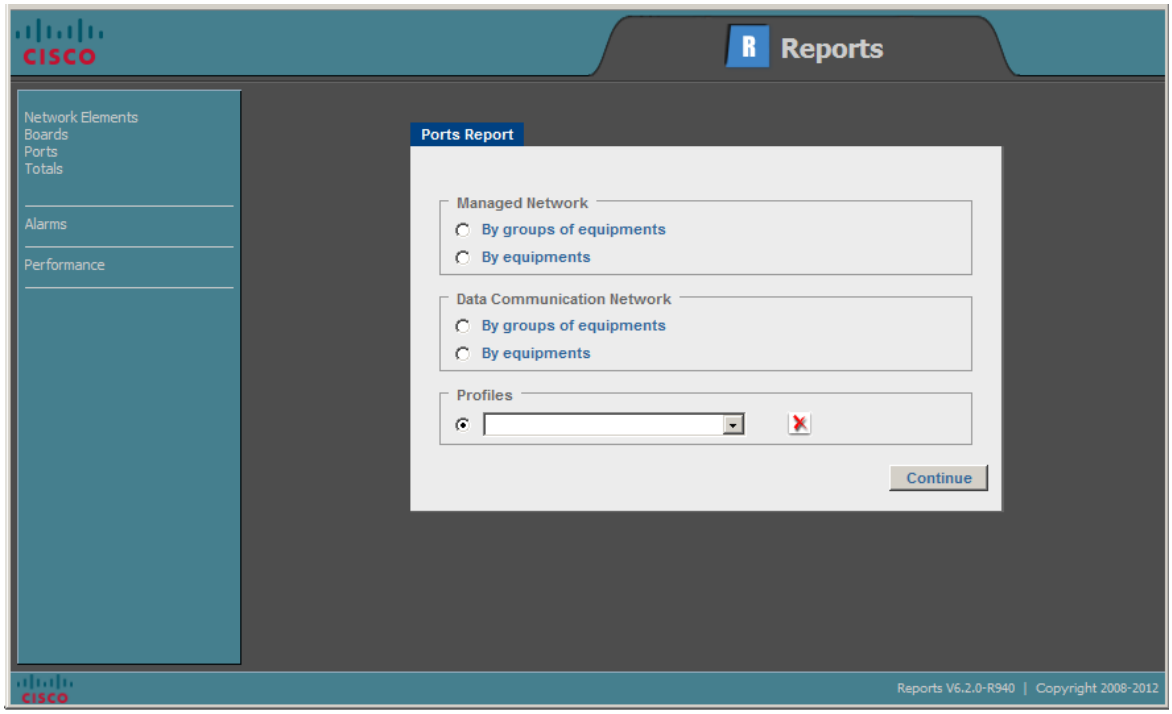
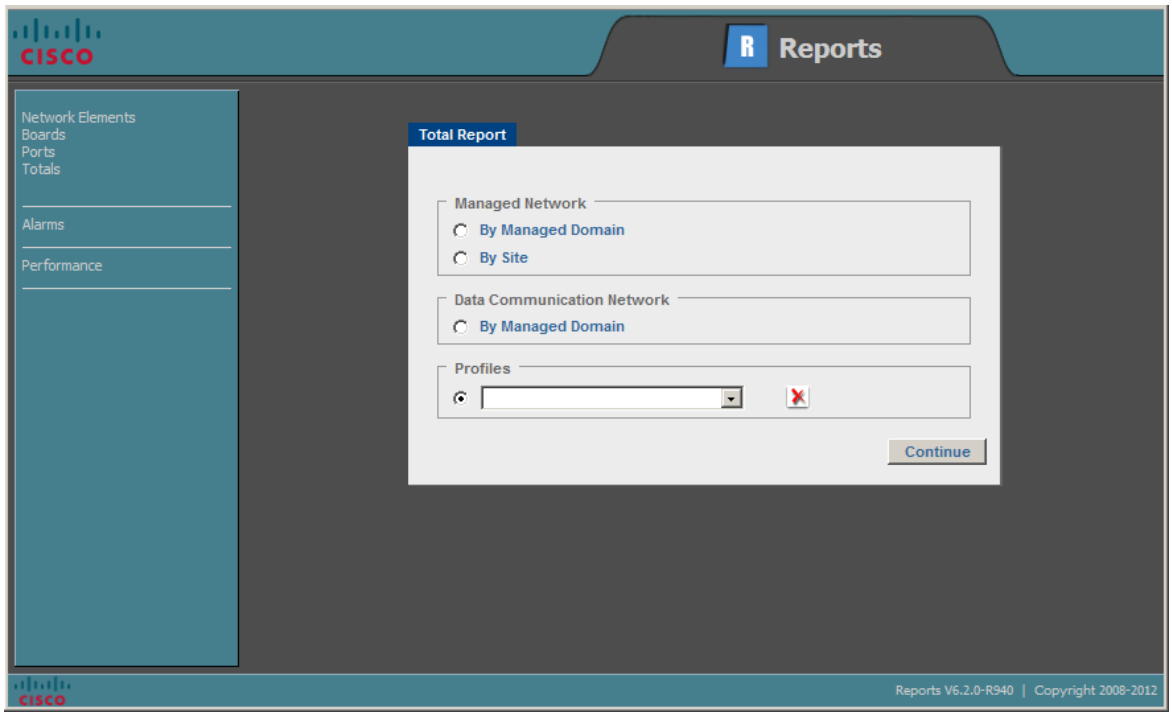


Figure 96. Total number of Network Elements by type report window



Catalog Management

- Cisco Template

The Catalog menu allows the configuration of various types of profiles associated to the different types of supported technologies. These specific technology profiles are applicable throughout the application (it may be Assure or Provision Packs). For more details of specific profile configurations (i.e. GPON traffic profiles, ONT profiles …) refer to the specific Service Manager Technology manual.

AGORA-NG application also allows the management of specific managed network elements types according to the acquired license.

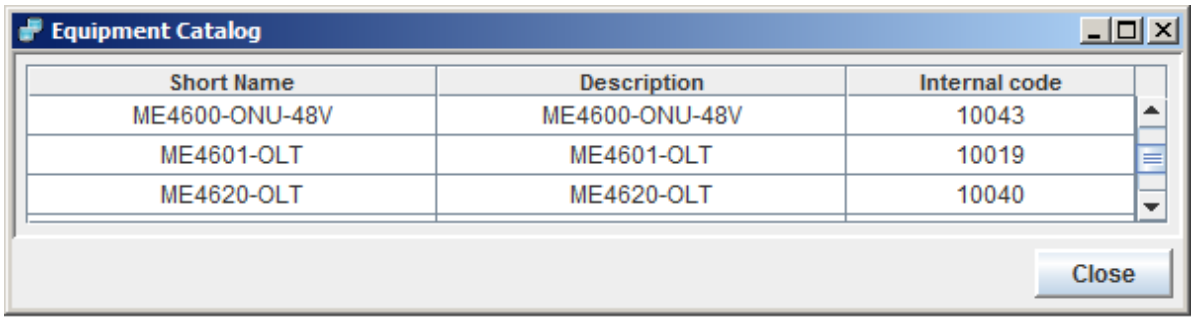
In 'Equipment Types Catalog' only licensed network elements types will be listed.

For specific type of managed network elements, it may be necessary to customize some aspects of its constitution. This is done in the 'Equipment Model Catalog'.

Equipment Types

From the main application menu, select Catalogs → Equipment Types. The table shown in Figure 97 lists existing equipment and some related features.

Figure 97. Equipment types catalog



Equipment Models

From the main application menu, select Catalogs → Equipment Models. The table shown in Figure 98 lists the existing equipment models and some related features.

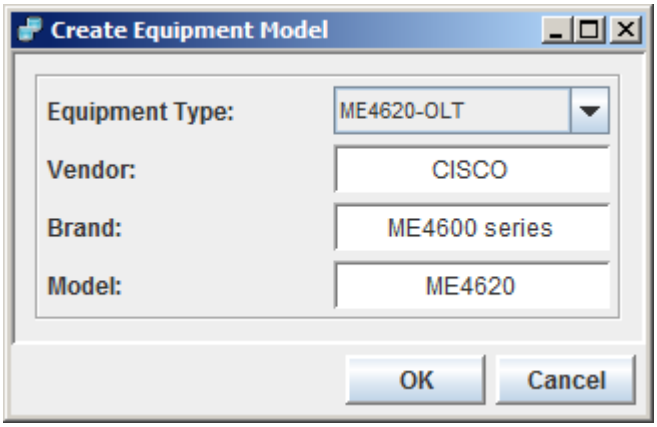
Figure 98. Equipment model catalog

As the previous figure shows, if the user has a profile with configuration access it may create new equipment models, modify and remove existing models and look up the list by equipment list.

Creating Equipment Models

In the figure shown in Figure 98, select 'Create' and, in the window shown in Figure 99, fill out the appropriate fields and select 'OK' to confirm the operation. If the configuration is successful performed, equipment models table will be automatically updated. If the configuration is not successful an error message is shown.

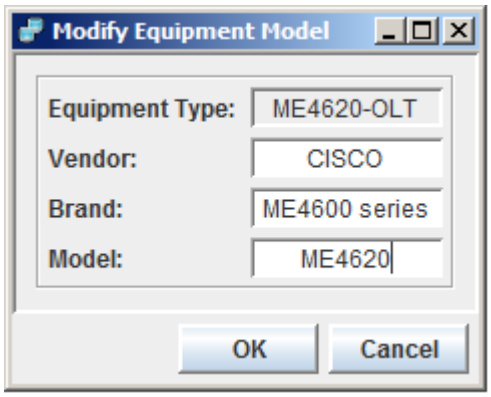
Figure 99. Creating an equipment model



Changing an Equipment Model

In the window shown in Figure 98, right-select on the target equipment model and, from the pop-up menu, select Configure → Modify. In the window shown in Figure 100, fill out the appropriate fields and select 'OK'. If the configuration is successful, the equipment models table will be automatically updated. If the configuration is not successful an error message is shown.

Figure 100. Changing an equipment model

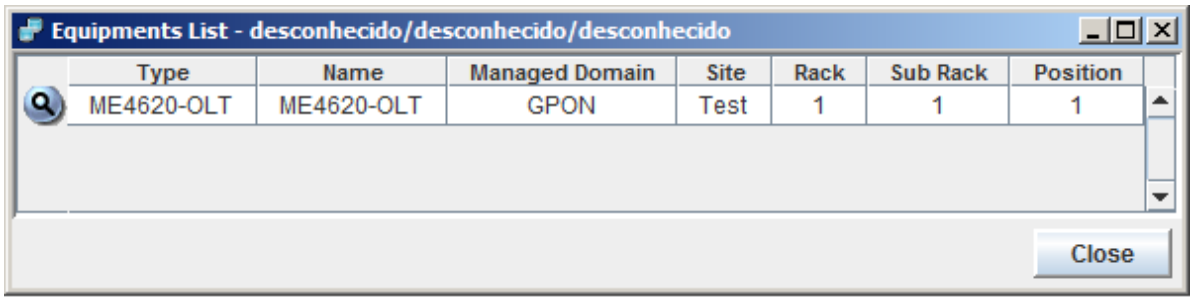


Retrieving an Equipment list

To retrieve the list of equipment inventoried in the management system, for a given equipment model, in the window shown in Figure 98, right-select on the target equipment model and, from the pop-up menu, select

View → Equipments List. This will bring up a window listing equipment using the selected model. Selecting will open the Network Element window.

Figure 101. Retrieving a list of equipment for a given model



Removing Equipment Models

In the figure shown (Figure 98) right-select on the equipment model to be removed and, from the pop-up menu, select Configure → Remove. If the configuration is successful, the equipment models table will be automatically updated. If the configuration is not successful an error message is shown.

Tools

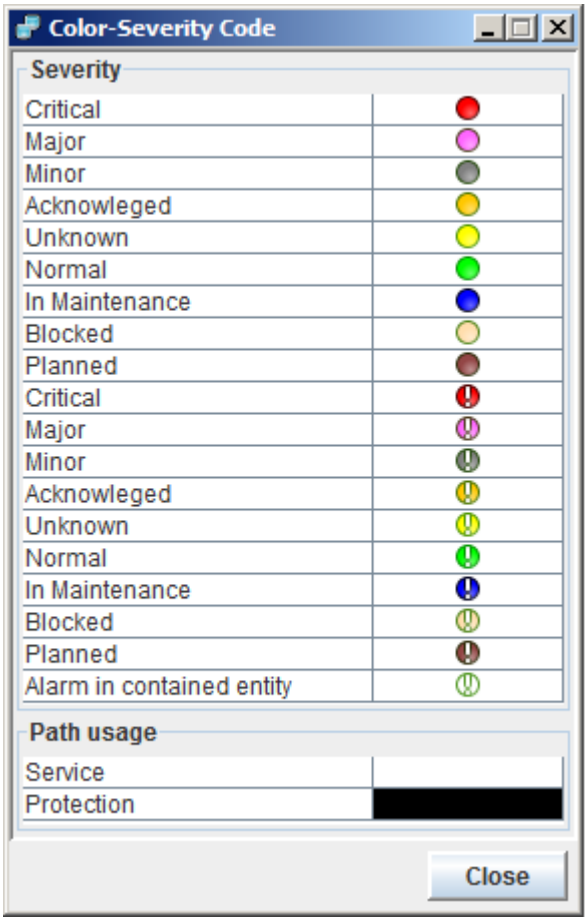
Refresh maps

From the main application menu select Tools → Refresh maps in order to update network map changes.

Color Code

From the main application menu select Tools → Color Code which shows up a color code table with color meanings.

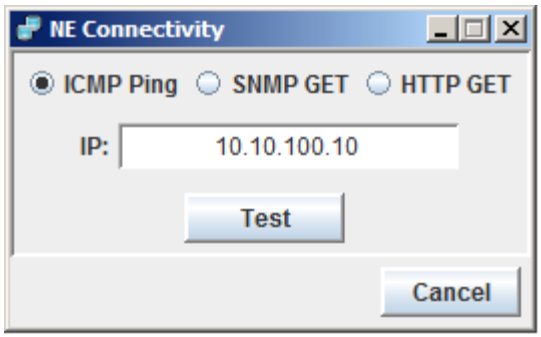
Figure 102. Color Code



NE Connectivity

From the main application menu, select Tools → NE Connectivity. This will bring up the window shown in the next figure. Select the required connectivity desired test (ICMP Ping, SNMP GET or HTTP GET) and the IP address of the managed element to be tested. Once the "Test" button has been selected, the application will run the connectivity test and display the operation result indicating success ( ) or failure ( ).

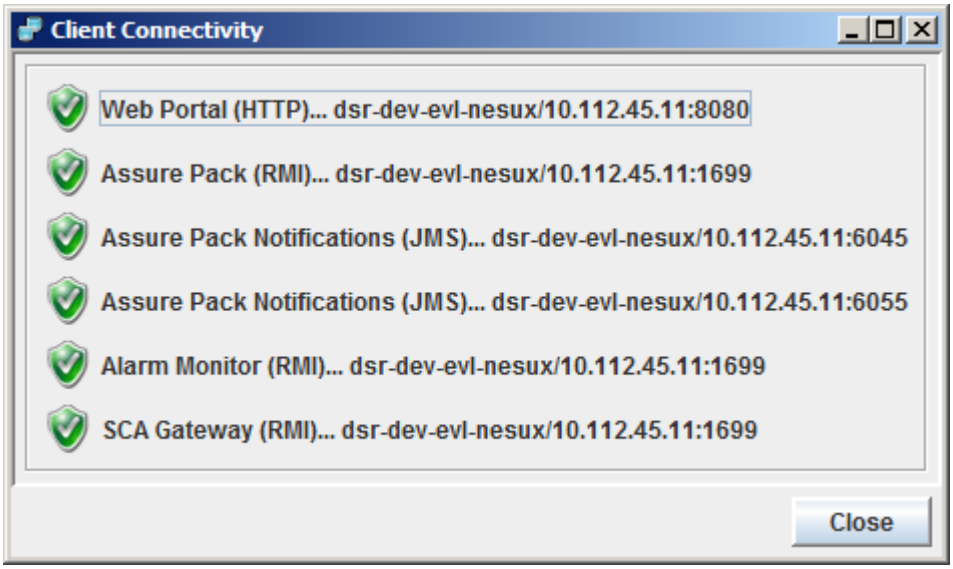
Figure 103. Device connectivity testing window



Client Connectivity

From the main application menu, select Tools → Client Connectivity. This will bring up the window shown in the next figure, which indicates the status of the connection between the customer's application and the some management system services. Icons will indicate if the test was either a success ( ) or a failure ( ).

Figure 104. Window for testing management system customer connections

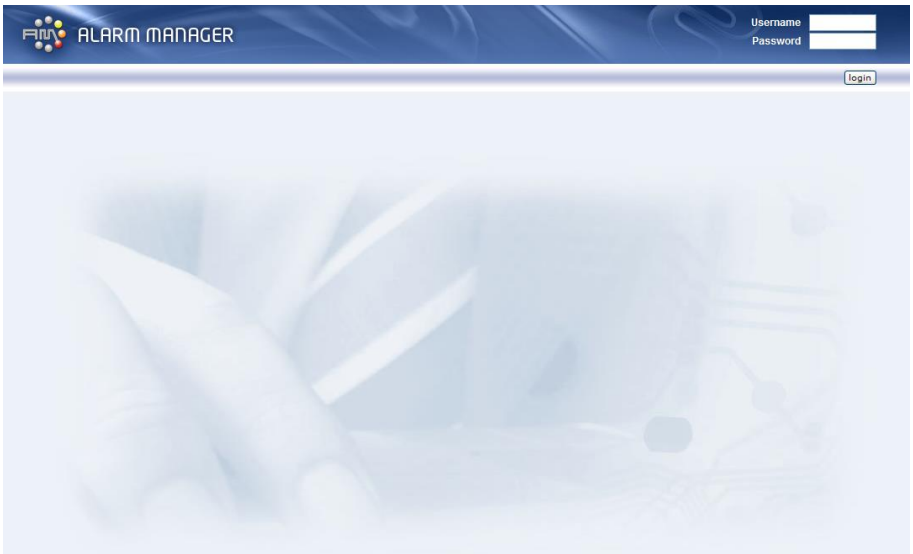


Alarm Manager

Introduction

The purpose of this section is to describe user application interfaces of Alarm Manager Platform fault management solution. Alarm Manager supports real-time monitoring of telecom infrastructures and services.

Figure 105. Main Window



General User Operations

Application Entry

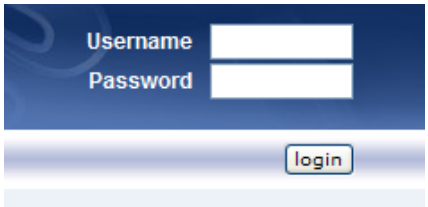
Using one of the supported browsers:

- Internet Explorer 7.0, or above
- Mozilla Firefox 3.6, or above

Type http://<server>:<port>/ejap/ in the address bar, being that <server> is the name of the equipment in which the application is installed and <port> is the number of the listening server port, which is usually 8080 or 8630.

The login page will appear in the system after the user has accessed the application. Type username and password.

Figure 106. System Access



If user information is correct, the pending alarms window will appear.

Application Exit

To exit the application, click on the logout icon or close the main browser page.

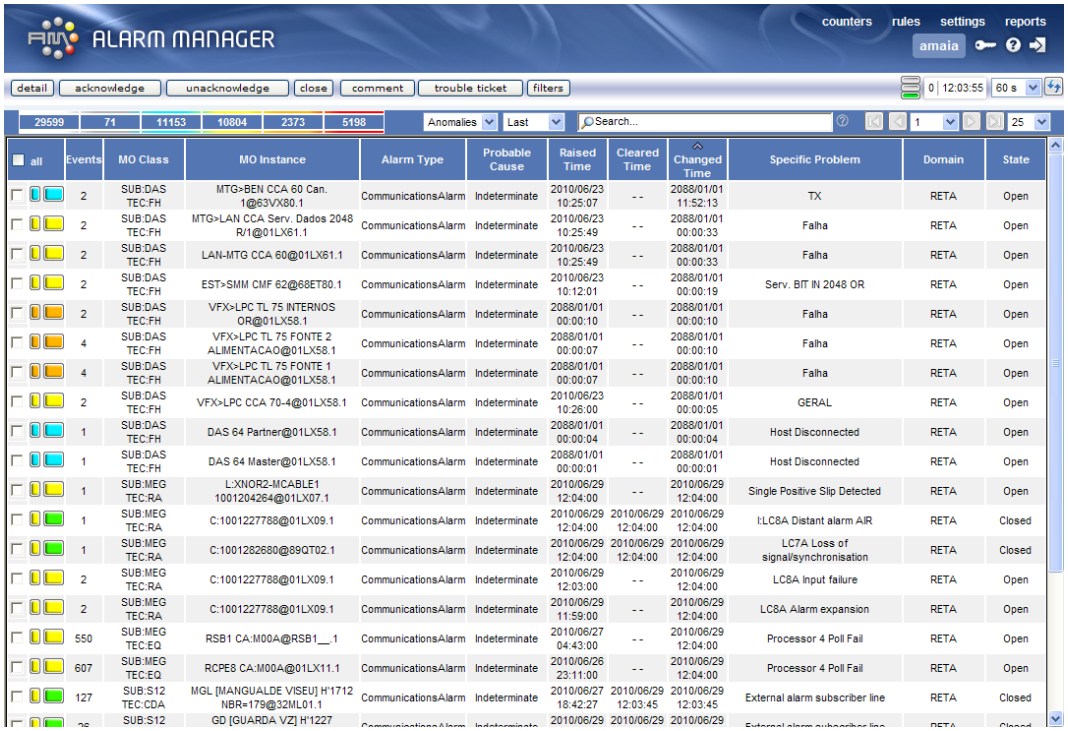
Figure 107. Application Exit

Main Alarms Window

The Main Alarms Window is basically a window divided into three sections:

- List of pending alarms in which displayable fields can be configured;
- Operations toolbar;
- Menu to access the complementary Alarm Manager modules: Access Control (SCA), Rules, Alarms Configuration, Counters and Reports; availability of the above mentioned modules depends on installation.

Figure 108. Main Alarms Window



all	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem	Domain	State
	2	SUB:DAS TEC:FH	MTG>BEN CCA 60 Can. 1@63VX80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:07	- -	2088/01/01 11:52:13	TX	RETA	Open
	2	SUB:DAS TEC:FH	MTG>LAN CCA Serv. Dados 2048 R/1@01LX61.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:49	- -	2088/01/01 00:00:33	Falha	RETA	Open
	2	SUB:DAS TEC:FH	LAN-MTG CCA 60@01LX61.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:49	- -	2088/01/01 00:00:33	Falha	RETA	Open
	2	SUB:DAS TEC:FH	EST>SMM CMF 62@68ET80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:12:01	- -	2088/01/01 00:00:19	Serv. BIT IN 2048 OR	RETA	Open
	2	SUB:DAS TEC:FH	VFX>LPC TL 75 INTERNOS OR@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:10	- -	2088/01/01 00:00:10	Falha	RETA	Open
	4	SUB:DAS TEC:FH	VFX>LPC TL 75 FONTE 2 ALIMENTACAO@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:07	- -	2088/01/01 00:00:10	Falha	RETA	Open
	4	SUB:DAS TEC:FH	VFX>LPC TL 75 FONTE 1 ALIMENTACAO@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:07	- -	2088/01/01 00:00:10	Falha	RETA	Open
	2	SUB:DAS TEC:FH	VFX>LPC CCA 70-4@01LX58.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:26:00	- -	2088/01/01 00:00:05	GERAL	RETA	Open
	1	SUB:DAS TEC:FH	DAS 64 Partner@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:04	- -	2088/01/01 00:00:04	Host Disconnected	RETA	Open
	1	SUB:DAS TEC:FH	DAS 64 Master@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:01	- -	2088/01/01 00:00:01	Host Disconnected	RETA	Open
	1	SUB:MEG TEC:RA	L:XNOR2-MCABLE1 1001204264@01LX07.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:04:00	- -	2010/06/29 12:04:00	Single Positive Slip Detected	RETA	Open
	1	SUB:MEG TEC:RA	C:1001227788@01LX09.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:04:00	2010/06/29 12:04:00	2010/06/29 12:04:00	I:LC8A Distant alarm AIR	RETA	Closed
	1	SUB:MEG TEC:RA	C:1001282680@89QT02.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:04:00	2010/06/29 12:04:00	2010/06/29 12:04:00	LC7A Loss of signal/synchronisation	RETA	Closed
	2	SUB:MEG TEC:RA	C:1001227788@01LX09.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:03:00	- -	2010/06/29 12:04:00	LC8A Input failure	RETA	Open
	2	SUB:MEG TEC:RA	C:1001227788@01LX09.1	CommunicationsAlarm	Indeterminate	2010/06/29 11:59:00	- -	2010/06/29 12:04:00	LC8A Alarm expansion	RETA	Open
	550	SUB:MEG TEC:EQ	RSB1 CA:M00A@RSB1__.1	CommunicationsAlarm	Indeterminate	2010/06/27 04:43:00	- -	2010/06/29 12:04:00	Processor 4 Poll Fail	RETA	Open
	607	SUB:MEG TEC:EQ	RCPE8 CA:M00A@01LX11.1	CommunicationsAlarm	Indeterminate	2010/06/26 23:11:00	- -	2010/06/29 12:04:00	Processor 4 Poll Fail	RETA	Open
	127	SUB:S12 TEC:CDA	MGL [MANGUALDE VISEU] H'1712 NBR=179@32ML01.1	CommunicationsAlarm	Indeterminate	2010/06/27 18:42:27	2010/06/29 12:03:45	2010/06/29 12:03:45	External alarm subscriber line	RETA	Closed
		SUB:S12	GD [GUARDA VZ] H'1227			2010/06/29	2010/06/29	2010/06/29			

Pending Alarms List

A great part of the main window is filled with the list of pending alarms, and its fields. (Figure 109) The fields shown are configurable, and are described below.

Figure 109. Alarms List

all	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem	Domain	State
	2	SUB:DAS TEC:FH	MTG>BEN CCA 60 Can. 1@63VX80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:07	- -	2088/01/01 11:52:13	TX	RETA	Open
	2	SUB:DAS TEC:FH	MTG>LAN CCA Serv. Dados 2048 R/1@01LX61.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:49	- -	2088/01/01 00:00:33	Falha	RETA	Open
	2	SUB:DAS TEC:FH	LAN-MTG CCA 60@01LX61.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:49	- -	2088/01/01 00:00:33	Falha	RETA	Open
	2	SUB:DAS TEC:FH	EST>SMM CMF 62@68ET80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:12:01	- -	2088/01/01 00:00:19	Serv. BIT IN 2048 OR	RETA	Open
	2	SUB:DAS	VFX>LPC TL 75 INTERNOS			2088/01/01		2088/01/01			

Clicking on the blue bar, a new window is open. It's possible to configure the alarm fields to display, as well as the order they appear in the main window. This feature will be discussed in "Alarm Management" section.

The first column is not configurable neither sortable. It always comes in first place. It provides checkboxes to select alarms and then apply some action to them. The checkbox on the header selects/deselects all the listed alarms.

Figure 110. Alarms List

all	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem	Domain	State
	2	SUB:DAS TEC:FH	MTG>BEN CCA 60 Can. 1@63VX80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:07	- -	2088/01/01 11:52:13	TX	RETA	Open

Beyond the aforementioned, the first column also contains two figures. The first one, thinner, signals the alarm perceived severity according to this table:

Table 45. Severity

	Indeterminate
	Warning
	Minor
	Major
	Critical

The wider figure combines color with a tick to provide more information. The color signals both act urgency and alarm state. It may be understood following the table:

Table 46. Act Urgency

	Indeterminate
	Warning
	Minor
	Major
	Critical
	Closed Alarm

If the alarm is acknowledged (and still open), a tick is included in the figure to signal that. (Example:).

It could also appear the icon indicating comments on the alarm. Those may be read in alarm details.

The main window shows a list of alarms with the following default fields:

Figure 111. Alarm Fields

all	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem	Domain	State
	2	SUB:DAS TEC:FH	MTG>BEN CCA 60 Can. 1@63VX80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:07	- -	2088/01/01 11:52:13	TX	RETA	Open
	2	SUB:DAS TEC:FH	MTG>LAN CCA Serv. Dados 2048 R/1@01LX61.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:49	- -	2088/01/01 00:00:33	Falha	RETA	Open

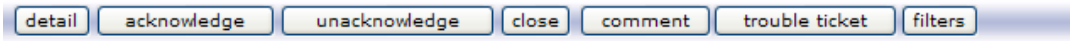
- Events: shows the number of events of an alarm;
- Raised Time: shows the date and time the alarm started;
- Cleared Time: shows the date and time the alarm terminates;

- Changed Time: shows the date and time of the last received event.
- Alarm Type: indicates which alarm type was generated;
- MO Class: shows the type of entity that generated the alarm;
- MO Instance: shows the entity that generated the alarm,
- Specific Problem: shows further details of the problem that generated the alarm;

Operations Toolbar

The Operations Toolbar is a bar located above the pending alarms list, left aligned. Except “filters” button, everyone else assumes that the alarms have been previously selected before it is clicked. All of this actions will be deeply discussed on the next chapter.

Figure 112. Operations Toolbar



Browsing Toolbar

The pending alarms list is displayed per page. On the top-right corner of the pending alarms list there is a browsing toolbar.

Figure 113. Navigation bar

This bar has buttons to jump to the next, previous, first and last page. It also has two select boxes: one to choose the page to be displayed and one to specify the number of alarms per page.

Figure 114. Displayed page

Figure 115. Page browsing

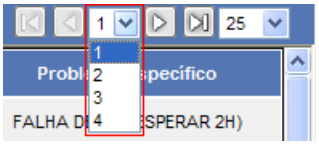


Figure 116. Alarms per page

Figure 117. Selection of alarm numbers per page

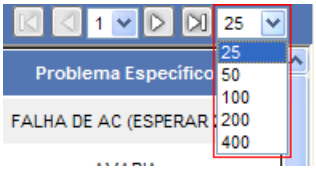


Figure 118. Go to home page

Figure 120. Go to last page

Figure 119. previous page

Figure 121. next page

Status Toolbar

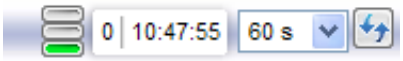
Above of the pending alarms list, but on the right, there is the status toolbar. It starts with a semaphore indicating the alarms list status in the following manner:

Table 47. Window Status

	Error
	Refreshing
	OK

Right after there are two labels. The first one is the number of new alarms minus the alarms that have been dropped from the list whereas the second label has the time of the last refresh.

Figure 122. Status bar



On the selection box that comes next, one may set the time period between refreshes and/or freeze the list by stopping refreshes. To force a refresh, one may click on the manual refresh button. Doing so, the timer is reset and starts counting from zero to the next refresh. As a safety measure, manual refresh won't be available for the next 5 seconds.

Setup, Counters and Reports Menu

On the top right corner of the page, there are links for access to: system access control (SCA), public filter alarm report, setup of rules to send e-mail and sms, received alarms configuration (setup), report creation and online help.

Figure 123. Setup, Counters and Reports Menu

Statistics

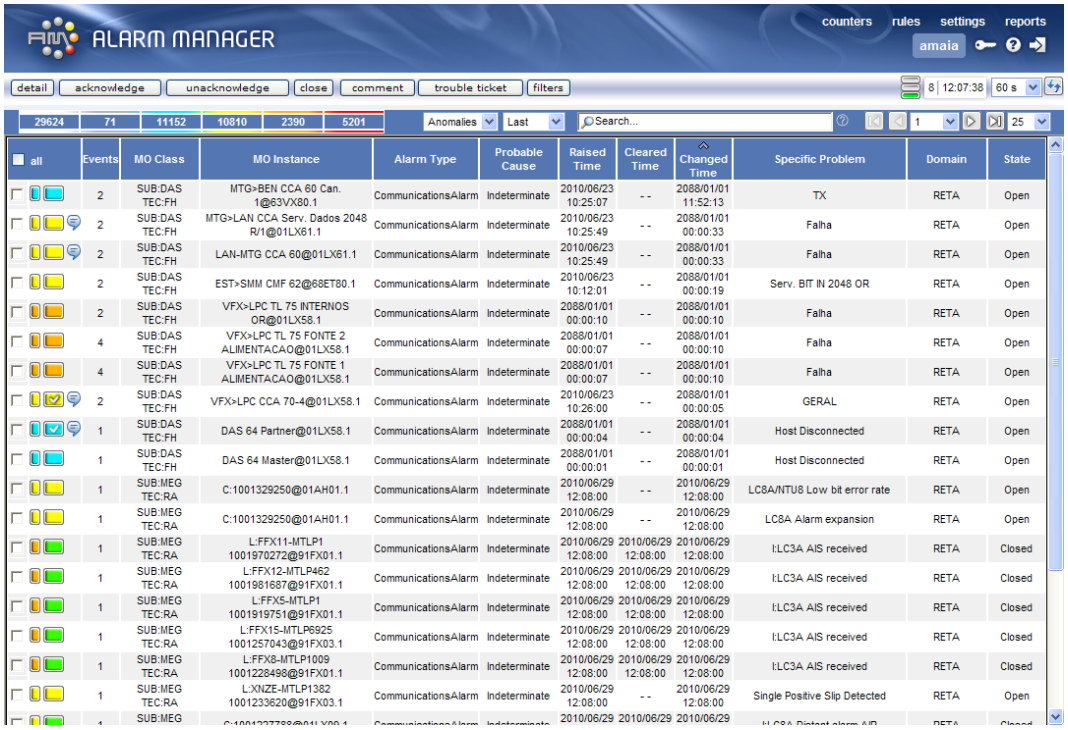
Pending alarms counters/reports bar is at pending alarms list top-left corner. This bar shows the number of urgent corrective action alarms present at any given time. In the case of a filtering condition, these counters show post-filtering results.

Figure 124. Alarm Statistics

Alarm Management

Alarm operations are performed in the Main Alarms Window, see Figure 125.

Figure 125. Alarms List

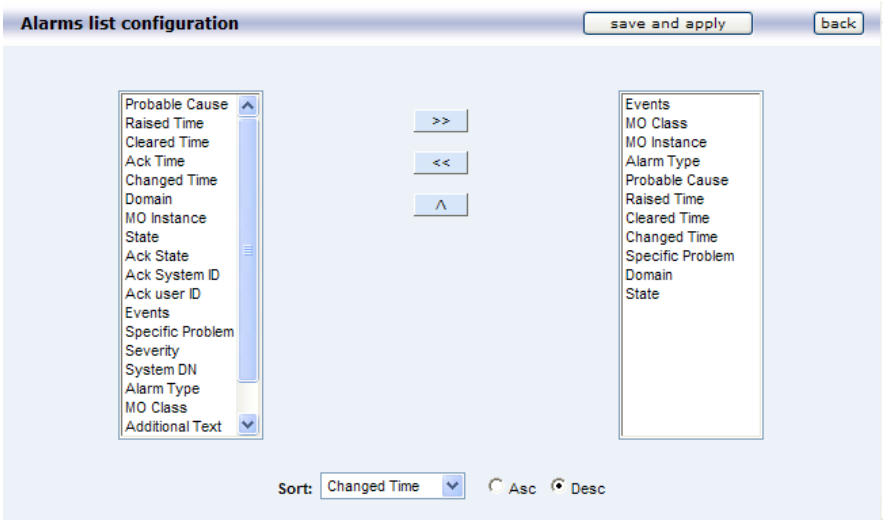


all	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem	Domain	State
	2	SUB:DAS TEC:FH	MTG>BEN CCA 60 Can. 1@63VX80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:07	- -	2088/01/01 11:52:13	TX	RETA	Open
	2	SUB:DAS TEC:FH	MTG>LAN CCA Serv. Dados 2048 R/1@01LX61.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:49	- -	2088/01/01 00:00:33	Falha	RETA	Open
	2	SUB:DAS TEC:FH	LAN-MTG CCA 60@01LX61.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:25:49	- -	2088/01/01 00:00:33	Falha	RETA	Open
	2	SUB:DAS TEC:FH	EST>SMM CMF 62@68ET80.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:12:01	- -	2088/01/01 00:00:19	Serv. BIT IN 2048 OR	RETA	Open
	2	SUB:DAS TEC:FH	VFX>LPC TL 75 INTERNOS OR@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:10	- -	2088/01/01 00:00:10	Falha	RETA	Open
	4	SUB:DAS TEC:FH	VFX>LPC TL 75 FONTE 2 ALIMENTACAO@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:07	- -	2088/01/01 00:00:10	Falha	RETA	Open
	4	SUB:DAS TEC:FH	VFX>LPC TL 75 FONTE 1 ALIMENTACAO@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:07	- -	2088/01/01 00:00:10	Falha	RETA	Open
	2	SUB:DAS TEC:FH	VFX>LPC CCA 70-4@01LX58.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:26:00	- -	2088/01/01 00:00:05	GERAL	RETA	Open
	1	SUB:DAS TEC:FH	DAS 64 Partner@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:04	- -	2088/01/01 00:00:04	Host Disconnected	RETA	Open
	1	SUB:DAS TEC:FH	DAS 64 Master@01LX58.1	CommunicationsAlarm	Indeterminate	2088/01/01 00:00:01	- -	2088/01/01 00:00:01	Host Disconnected	RETA	Open
	1	SUB:MEG TEC:RA	C:1001329250@01AH01.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	- -	2010/06/29 12:08:00	LC8A/NTU8 Low bit error rate	RETA	Open
	1	SUB:MEG TEC:RA	C:1001329250@01AH01.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	- -	2010/06/29 12:08:00	LC8A Alarm expansion	RETA	Open
	1	SUB:MEG TEC:RA	L:FFX11-MTLP1 1001970272@91FX01.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	2010/06/29 12:08:00	2010/06/29 12:08:00	I:LC3A AIS received	RETA	Closed
	1	SUB:MEG TEC:RA	L:FFX12-MTLP462 1001981687@91FX01.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	2010/06/29 12:08:00	2010/06/29 12:08:00	I:LC3A AIS received	RETA	Closed
	1	SUB:MEG TEC:RA	L:FFX5-MTLP1 1001919751@91FX01.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	2010/06/29 12:08:00	2010/06/29 12:08:00	I:LC3A AIS received	RETA	Closed
	1	SUB:MEG TEC:RA	L:FFX15-MTLP6925 1001257043@91FX03.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	2010/06/29 12:08:00	2010/06/29 12:08:00	I:LC3A AIS received	RETA	Closed
	1	SUB:MEG TEC:RA	L:FFX8-MTLP1009 1001228498@91FX01.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	2010/06/29 12:08:00	2010/06/29 12:08:00	I:LC3A AIS received	RETA	Closed
	1	SUB:MEG TEC:RA	L:XNZE-MTLP1382 1001233620@91FX03.1	CommunicationsAlarm	Indeterminate	2010/06/29 12:08:00	- -	2010/06/29 12:08:00	Single Positive Slip Detected	RETA	Open

Display field setup

Visible fields are configured in a menu accessible by clicking on the header of any column, except the first one. A new window will appear.

Figure 126. Alarm fields' setup



It is shown two field lists, side by side. The available fields are on the left whereas the already chosen fields are on the right. The buttons at the middle, throw fields from one list to the other and lift up fields on the right list. At the bottom one may choose the field to order from in an ascending or descending manner.

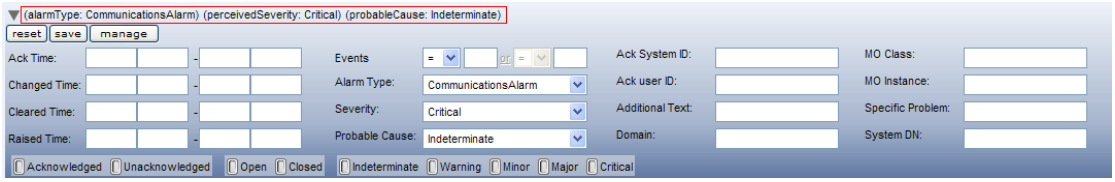
For submit the changes, click on the icon save and apply.

Alarm Filtering

The filters button, on the operations toolbar, shows/hides the filtering panel. Every time filtering is enabled, it turns red. The filtering panel is divided in 4 pieces:

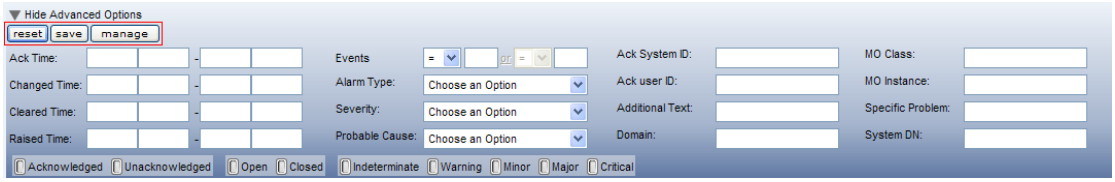
- Current filtering information.
- Operations menu.
- Filtering form.
- Quick filtering.

Figure 127. Filters - Current filtering information



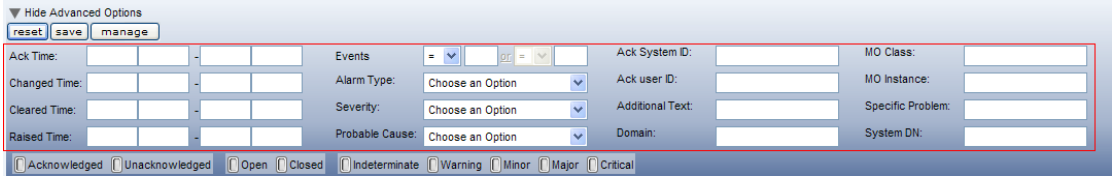
On current filtering information it is shown in a paragraph the current filtering conditions. This information may be split into two lines. The top line is reserved to a small set of attributes, which are noteworthy to startle from the others. This line is only shown when needed to. The second line not only shows the filtering conditions on other attributes but also opens/closes the operations menu and the filtering form. Please note the information does not include filtering conditions provided on the quick filtering, once that it is always shown too.

Figure 128. Filters - Operations Menu



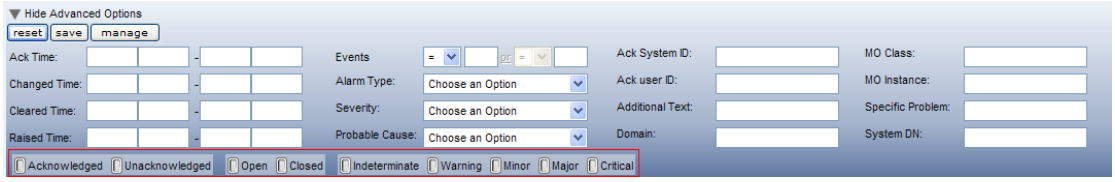
The operations menu has three buttons: reset, save and manage. The first one clears all the filtering conditions form the filtering form and quick filtering as well. The second one lets the user save the current conditions for later use. If saved as public, the conditions will be available to other users and included on counters. The manage button opens a management area where users may load and/or delete conditions.

Figure 129. Filters - Filtering form



The filtering form is a table where each cell provides filtering to a specific attribute. Depending on the type of attribute, different options may be available. There are four kinds of attribute types: date, number, list or text. The date type attributes may be filtered by indicating a time window where the attribute should fit in. To an attribute of number type it should also be provided a range, but it is possible to tell if the attribute should fit in or out. To the attributes of list type are provided a select box with the available options. The user may choose one of them. Last but not least, the text type attributes have a textbox that user may use to indicate what attributes should contain. Notwithstanding, this textboxes allow advanced filtering options, these are explained in “Display field setup” section.

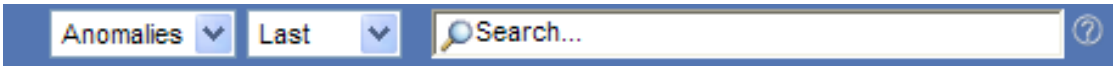
Figure 130. Filters - Quick Filtering



At last, quick filtering is split into two zones. On the left there are sets of toggle buttons to some attributes. For each attribute, if no button is on, then no filtering is applied to that attribute. Thus, no button on is virtually the same has having all buttons on. The attributes shown here is configurable, but the default is acknowledged state, alarm state and acting urgency. On the right of quick filtering is a search box with similar features to the text boxes present on the filtering form. Although, this search box is not targeted to a specific alarm attribute, it filters on any alarm attribute. Anyway, its behavior is also explained on the next section.

Non persistant filtering

Figure 131. Non persistant filtering



The filtering options between the statistics and the navigation bar are always visible and cannot be saved as a filter.

The listboxes are plugins and may vary between installations. The behavior of each one is plugin-dependent.

The search box, on the right, filters within any alarm attribute. The features of this box are discussed on the next chapter.

Text Filtering

Figure 132. Search Box

By filling the search box and pressing enter, the application filter the alarms and show only those that contain the inserted text in the attribute where it has been inserted (or in anyone if inserted on the global searchbox).

Beyond the insertion of a single word, it is possible to build richer filters [10]. For instance, if two or more words are inserted, the attribute being filtered must have all those words (not necessarily respecting the inserted order) .

Example 1: campo pequeno – the attribute should have the words “campo” and “pequeno”.

Users looking for the exact sentence, “campo pequeno” may be surprised with this behavior; but to accomplish such query, it is necessary to bound the sentence with quotes, to get a verbatim query.

Example 2: “campo pequeno” – the attribute should have the sentence “campo pequeno”.

As an exercise, consider the text “Rua do pequeno soldado, campo maior”. The first example would agree with this sentence whereas the latter wouldn’t.

Another common mistake is think that example 1 would be searching for “campo” or “pequeno”. However, if not said nothing against, it is used AND logic operator. To use OR logic operator it should must be said so by writing ‘OR’.

Example 3: campo OR pequeno – the attribute should have the word “campo” or the word “pequeno”.

[10] Special punctuation, separation and text characters must be accepted and presented correctly (see for example HTML Encoding for Special Characters for a list of such characters that must be presented correctly).

It is also allowed to choose text that must not be present on the attribute of the alarm. It is a simple as begin the query with a ”-“.

Example 4: campo –soldado – the attribute must contain the word “campo” but not the word “soldado”.

To assure a case sensitive search exists the “+” operator.

Example 5: +SoLdAdO – the attribute must contain the word “SoLdAdO” respecting the upper and lower letters.

Nonetheless, verbatim search (with quotes) is also case-sensitive.

Last but not least, the “*” wildcard stands for 0 or more characters.

Example 6: so*do – the attribute must contain a word that has the word “so” and “do” but “so” must come first than “do”.

All these features may be used together.

Example 7: rua*soldado OR -“campo maior” – gives the union of the previous example with all alarms that have “campo maior” on the attribute being filtered.

The aforementioned features are present both in the textboxes of the filtering form and on the global search textbox on the quick filtering, but the former filters on any attribute of the alarm.

The usage of the textboxes available on the filtering form is always preferable due to its explicitness and efficiency. Nevertheless, it is also possible to specify the filtering on the global search textbox on the quick filtering to a specific attribute. One just have to use the attribute nickname followed by “:” to indicate that the filtering is just on that attribute.

Example 8: urgAct:critical – it will only be shown alarms with critical act urgency.

This option is not available on the textboxes that belong to the filtering form once that the attribute is already specified on them.

The following table summarizes the features available on text filtering and indicates the precedence from which they are applied.

Table 48. Text filtering features

Precedence	Wildcard	Feature	Availability	Example
1	OR	Or logic	All	Siemens OR Alcatel
2	<field>:	Attribute specification	Global search only	managedObjectClass: sdh
3	-	Not	All	-alcatel

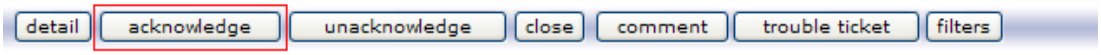
3	+	Case-sensitive	All	+Alcatel
4	“”	Verbatim search	All	“Adapter error”
5	*	0 or more characters	All	Al*el

Alarm Acknowledgement

Acknowledge

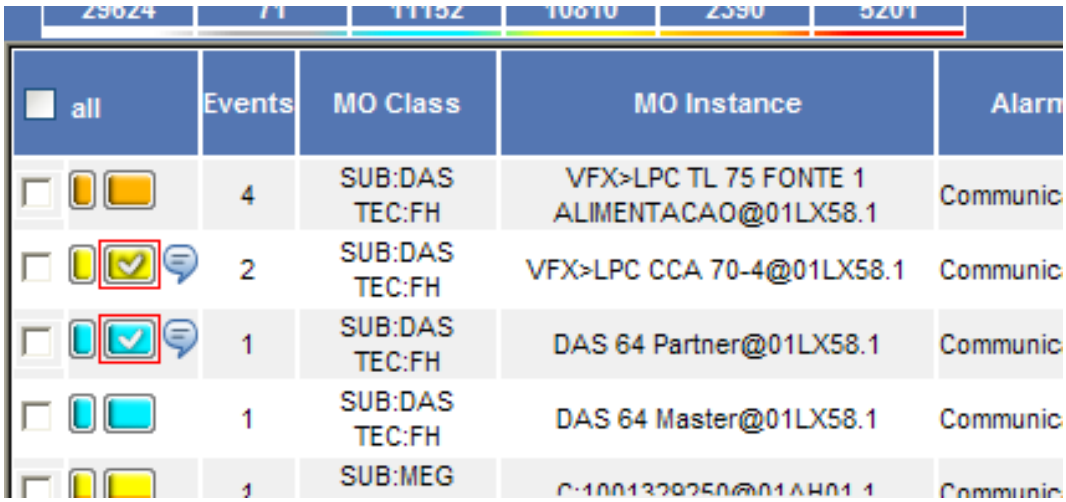
To acknowledge an alarm, select the alarms (Alarms Table) and click on the Acknowledge icon.

Figure 133. Acknowledgement of selected alarm



If the operation is successful, a tick is added to the image signaling act urgency.

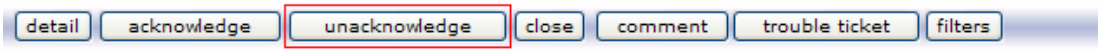
Figure 134. . Indication of acknowledged alarm



Unacknowledge

The unacknowledgement of an alarm can be done selecting the ones to unmark, and clicking on the Unacknowledge button. If the operation is successful the tick is removed from the image that shows the act urgency of the alarm.

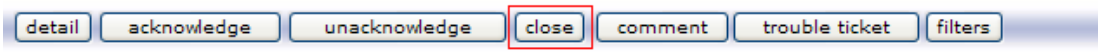
Figure 135. Unacknowledgement of a selected alarm



Manual Closure

To terminate one or more alarms, select the desired ones from the list and click on the Close button. If the operation is successful, the image with information of act urgency turns green. This operation does not close the alarm in the network element: it will only close the alarm in the management platform.

Figure 136. Alarm termination



The alarm will change to ‘Manual Termination’ state (image turns green) and acknowledgement status turns to ‘Ack’ ( ). The data of the user who performed the operation is stored.

Connection to Registration module

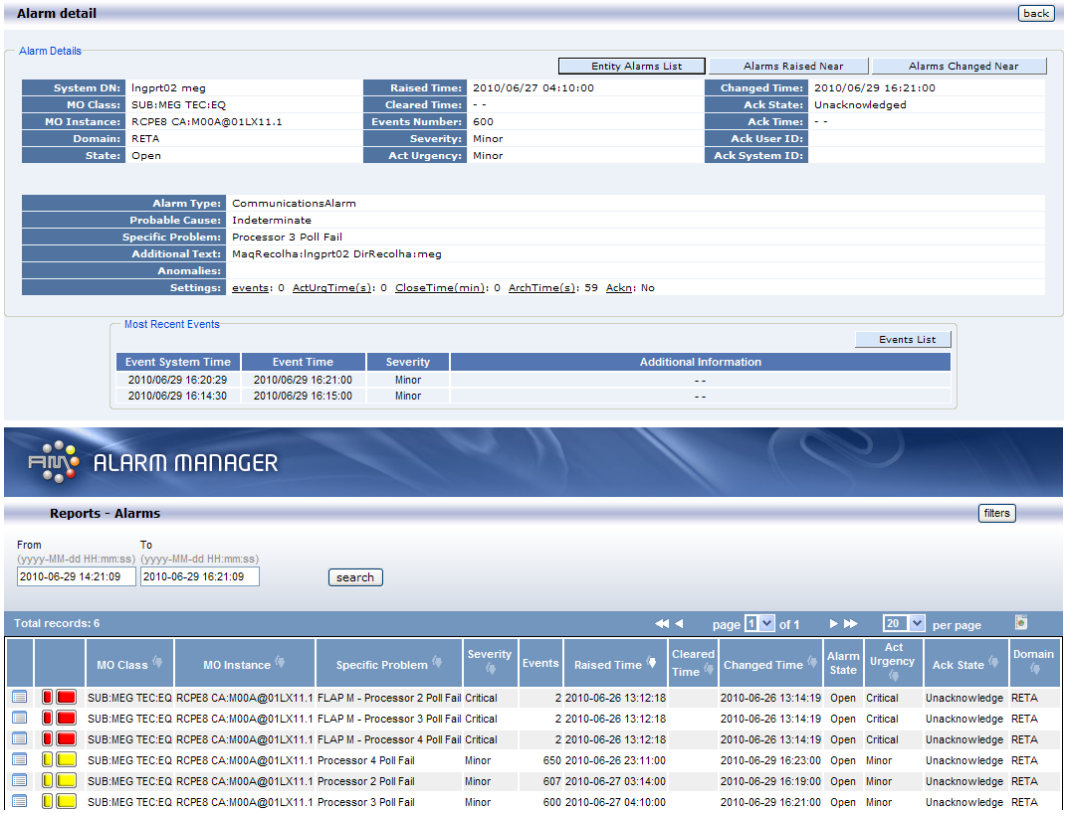
If the registration module is available, it’s possible to see the entity which raised the alarm, in graphic mode, by selecting the attribute 'MO Instance'.

Figure 137. Entity which triggered the alarm

Alarm Detail

To see the Alarm Detail window, select the alarm(s) (in the Alarms Table) and click on Details button. Another option is to click directly on one of the alarm columns and in this case, only details of desired alarm will be displayed. Figure 138 shows the details of a selected alarm, surrounded by a black frame.

Figure 138. Alarm Detail page



All the information of the alarm is shown in this window. The details of the parameterization associated with the alarm are also shown. For more details about the parameterization of alarms, consult “Alarm Configuration” section.

With the information of the context of the alarm serving as basis, it is available direct links to access the following reports:

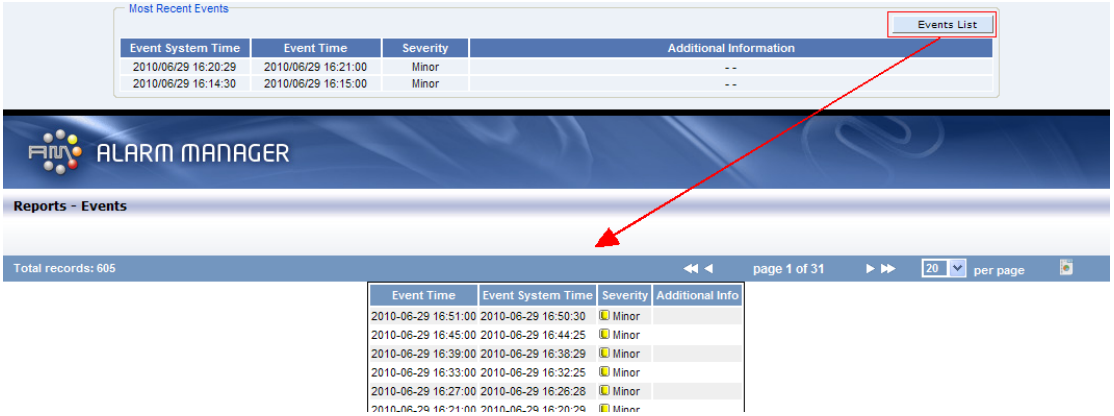
- Alarms list to the entity (filtering by domain, entity and type of entity);
- Alarms list that has begun in the temporal neighborhood (adjustable time window, by default is 2 minutes);
- Alarms list with events occurred in the temporal neighborhood (adjustable time window, by default is 2 minutes);

Events table

Events table is integrated in alarm details window. Figure 139 presents an events table, surrounded by a black frame. In this list it is shown a set of events, pointed out at installation. It is also shown a link to direct access to an event list, with an export to CSV option.

Aside from the indication of the date and time of occurrence, every event list provides information about date and time of registration of the event in the system.

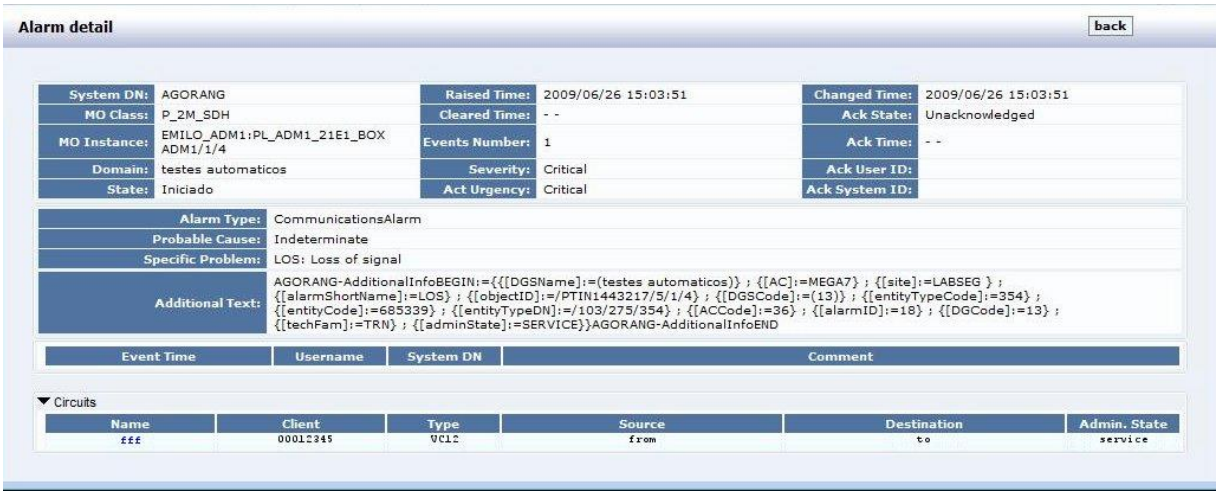
Figure 139. Alarm Detail including events table



Provisioning

If the provision pack is available, the alarm detail window shows information of the circuits affected by the alarm. This feature is possible by selecting '>' on the alarm detail window. There is a link to respective PP for direct access to circuit registration.

Figure 140. Alarm Detail page with Associated Circuits List

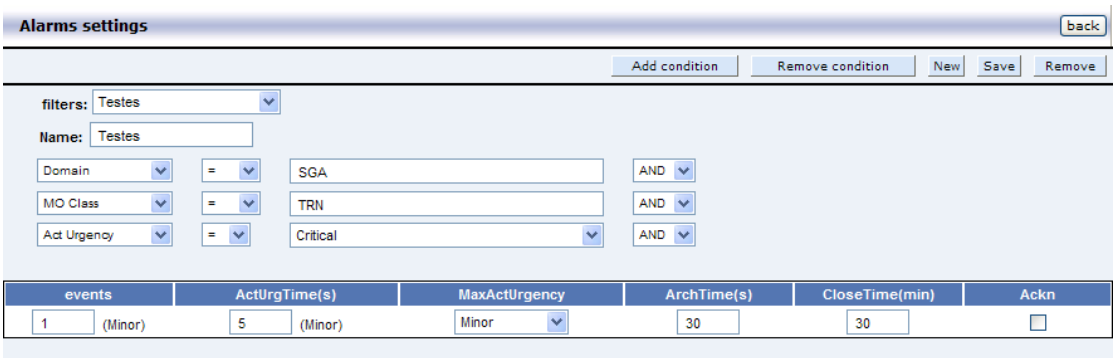


Alarm Configuration

Access to Alarm Settings is possible through the Settings option, in the menu to access the complementary modules. Configuration type can be changed using user defined rules. Figure 141 shows current active configuration rules, the equation which can trigger them, and the values of alarm items. Click on edit for a new window, Figure 142.

Figure 141. Alarm Settings

Figure 142. Editing Alarm Settings



This page allows configuration of the alarm items that follows a specific equation. The equation, as the filters, is a boolean expression in which each condition represents an alarm field. The only possible operation between conditions is AND (&). Configurable items are:

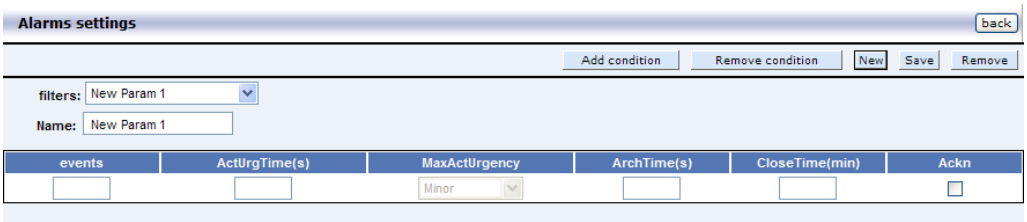
- Events Threshold: if this value is different from zero, after this specific number of events the Urgency of Action is increased to Critical;
- Urgency of Action: if this value is different from zero, after this number of seconds, the Urgency of Action is increased until getting the max configured value;
- Max Urgency of Action: defines the maximum Urgency of Action value that an alarm can assume from result of alarm setting procedure;
- Close Time: if this value is different from zero, it implies the alarm (on absence of other events) will be terminated after this time (value in minutes), and switched to status 'A' (Terminated Automatically);
- Archive Time: if this value is different from zero, after the termination (in absence of other events), the alarm is archived at end of time (value in seconds).
- Mandatory Acknowledgement: if this field is active, it means the alarm is only removed from the list after manual acknowledgement;

Create Configuration Rule

To create a new configuration rule, click on the New button. Data will appear with the default configuration, i.e. name of rule would be New ParamX.

Caution: rules cannot have the same name. Items will be empty but it will only accept data after a new condition has been introduced.

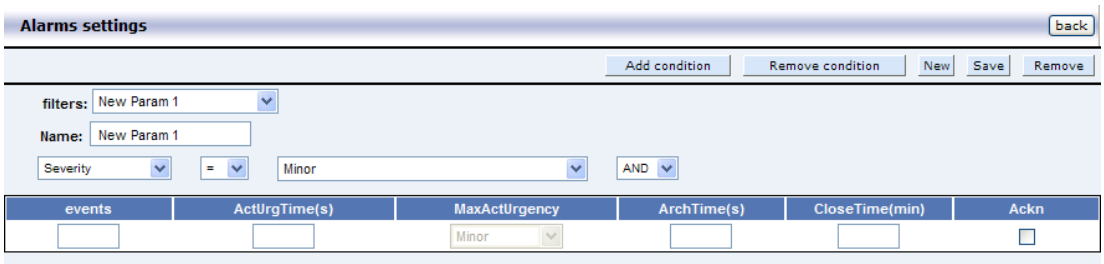
Figure 143. New configuration



Add/Remove Conditions

A configuration rule is a set of one or more conditions (up to five). To add a new condition, click on Add new condition icon, and it will appear right below the name if it is the first one. In case there's already one or more conditions created, it will appear after the last one. Items become editable after a condition has been added.

Figure 144. Adding a Condition



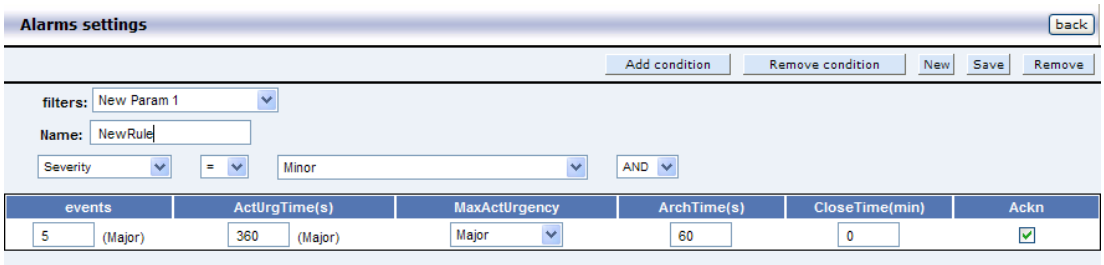
To remove the last condition, click in Remove last condition button.

Save/Remove Configuration Rule

After creating a rule and introducing the configuration field values, the rule must be saved to become available. Click Save.

To remove the selected rule, click Remove.

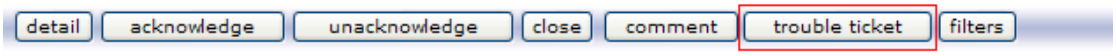
Figure 145. Save Configuration Rule



Anomalies

Creation of Anomalies

Figure 146. Create anomaly for the selected alarms



To create an anomaly, select one or more alarms and click on the Trouble Ticket link - a new window will open (**Figure 147**). Use the radio buttons to select the root cause alarm, and then type some text with remarks and finally select whether to record the anomaly to an external system (eg, TTK SIGO ®) or send an e-mail to a list of recipients (separated by comma or semicolon). The anomaly is created upon the green check button is clicked.

Figure 147. Anomaly management window

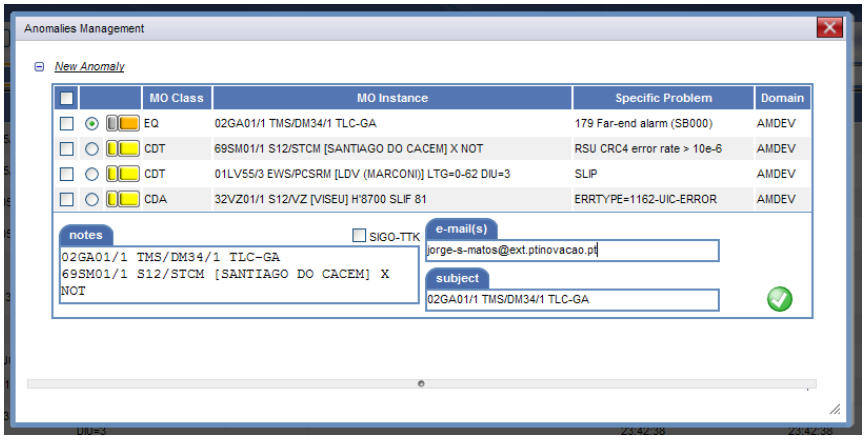
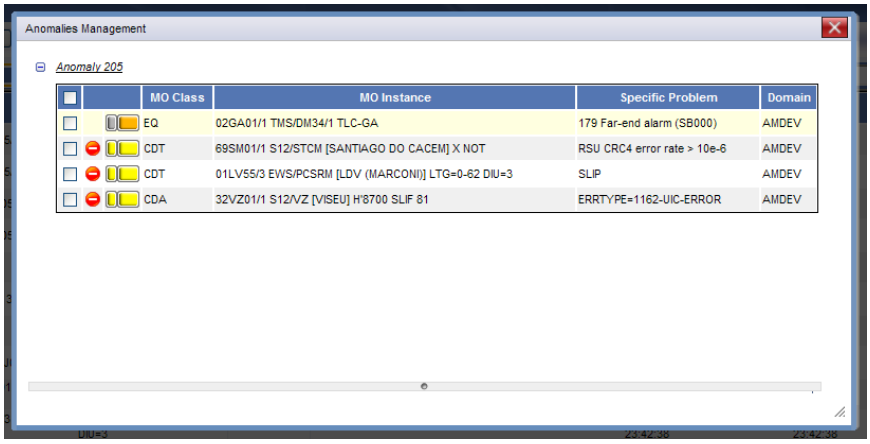


Figure 148. Anomaly management window after creation of an anomaly



Anomaly details

To see the details of an anomaly it is necessary to identify an alarm associated to it. The anomalies column has a shortcut to the details of each anomaly as shown in Figure 149. Another way to see the details is to select an alarm which is linked and click on "trouble ticket".

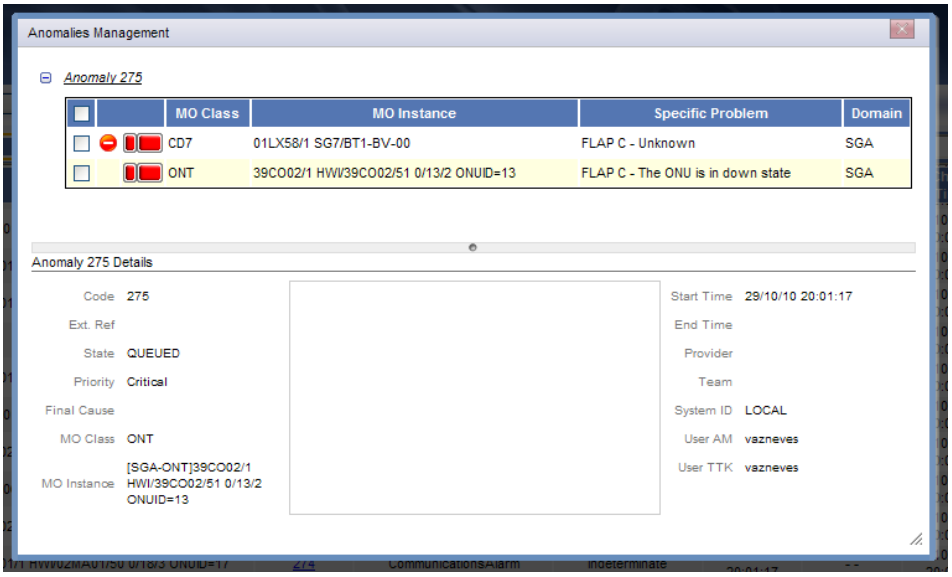
Figure 149. Anomalies column in the alarms window

Figure 150 shows some alarms associated to a couple of anomalies. Clicking on any of it show its details. The information shown on this window may differ depending on the selected alarm. The next images show the difference.

Figure 150. Alarms with anomalies associated

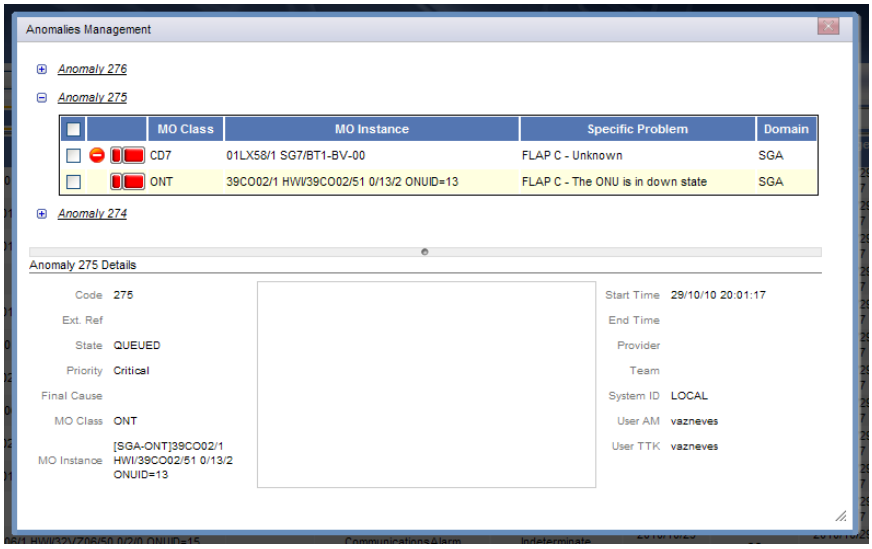
Clicking on the anomaly of the red highlighted alarm shows the information on Figure 151.

Figure 151. Anomalies Management window with only one anomaly



Clicking on the anomaly of the green highlighted alarm shows the information on Figure 152.

Figure 152. Anomalies Management window with multiple anomalies



All the anomalies that the alarm is associated with are shown as pointed by the above images. Clicking the anomaly id, for example Anomaly 276, the details zone is updated.

Figure 153. Anomaly with details visible

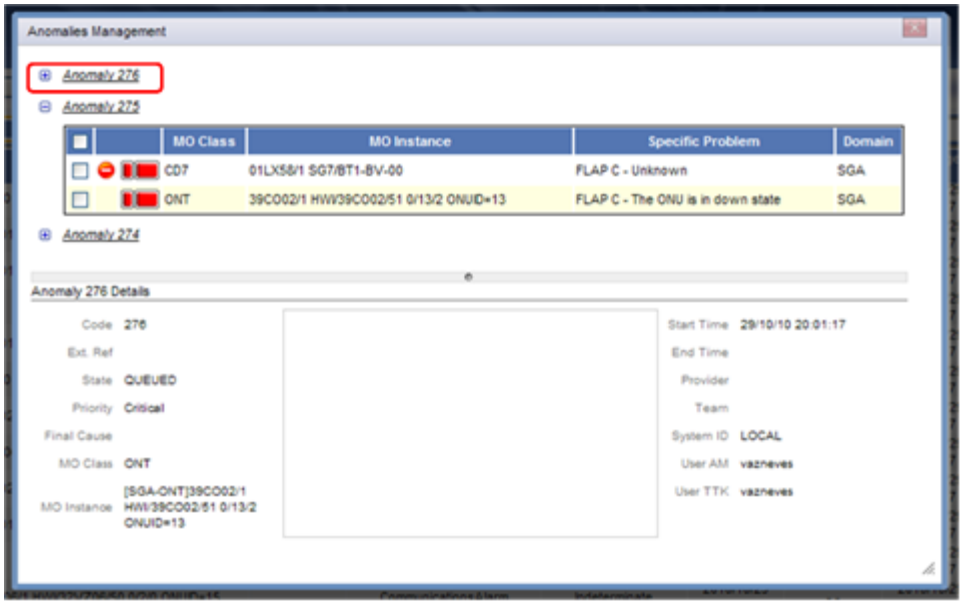
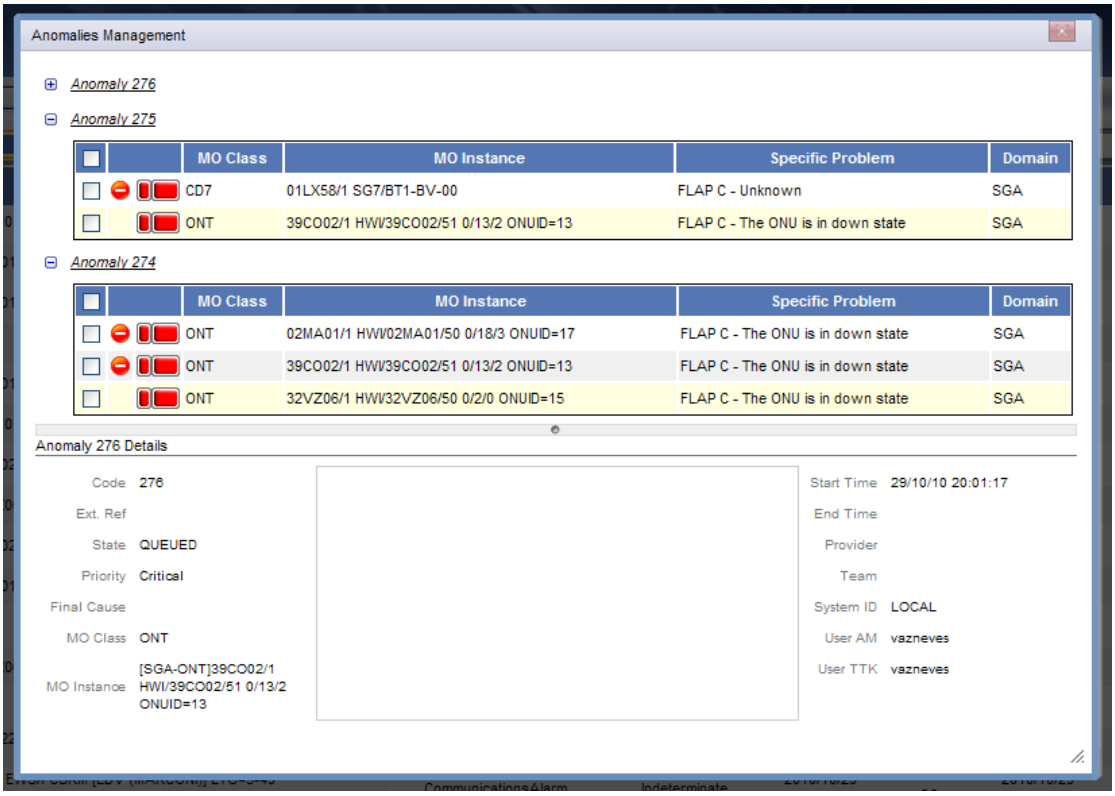


Figure 154. Multiple anomalies with alarms visible



Associating alarms to an existing anomaly

To associate an alarm to an existing anomaly it is necessary to select an alarm previously associated with the given anomaly and the new alarm to be associated with.

Figure 155. Window to associate new alarms with an existing anomaly

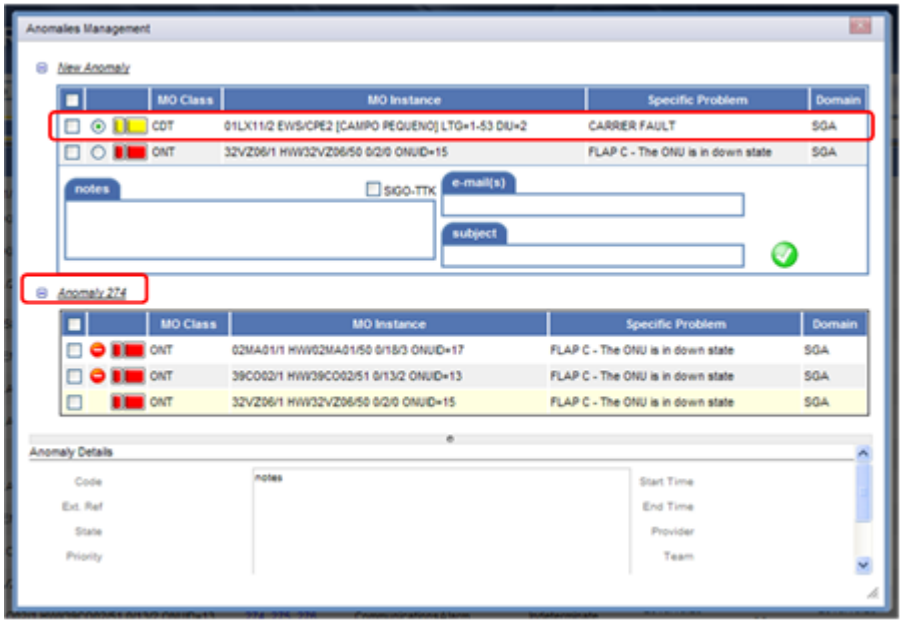
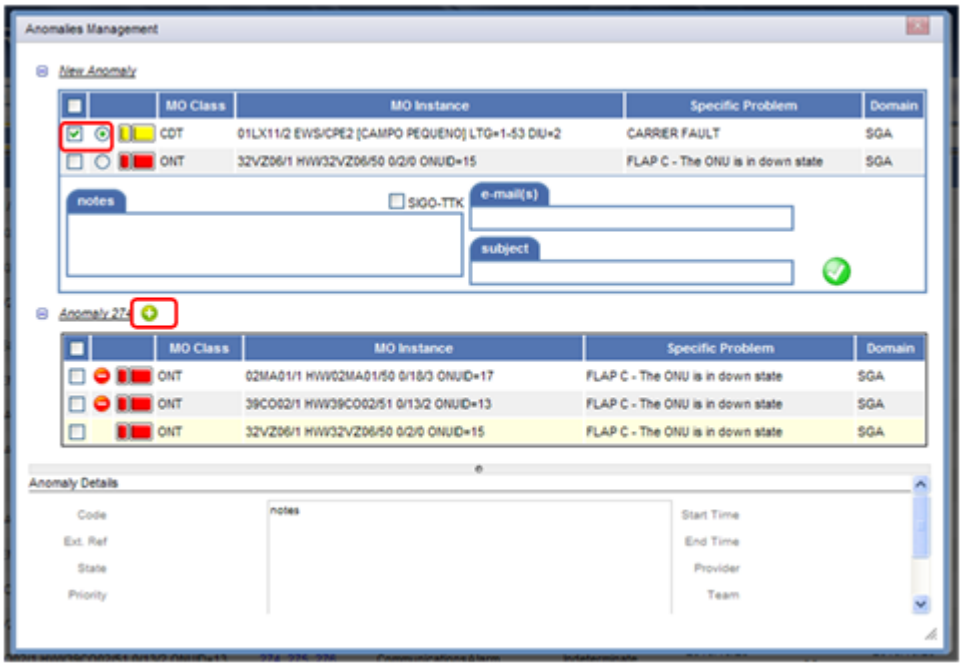


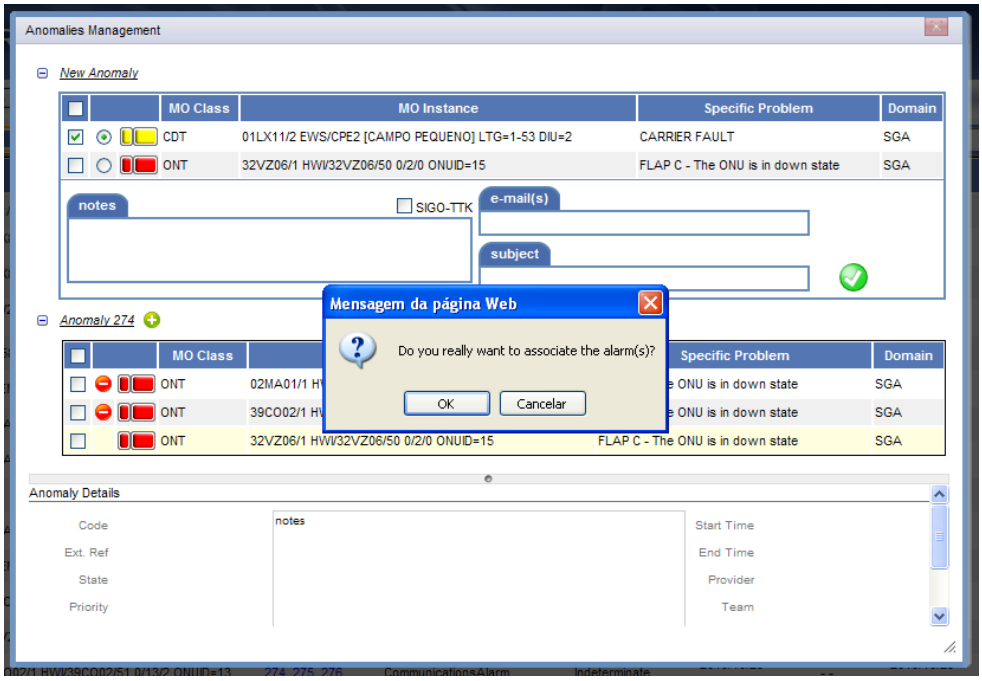
Figure 155 shows the alarm to be associated with anomaly 274. To do this, one must select the alarm as shown in Figure 156.

Figure 156. Selecting alarms to associate with an existing anomaly



Once selected, the option to associate to the anomaly is available and represented by the symbol .

Figure 157. Confirmation to associate the alarm to the anomaly



The final step is to confirm the association.

Figure 158. Recently associated alarm

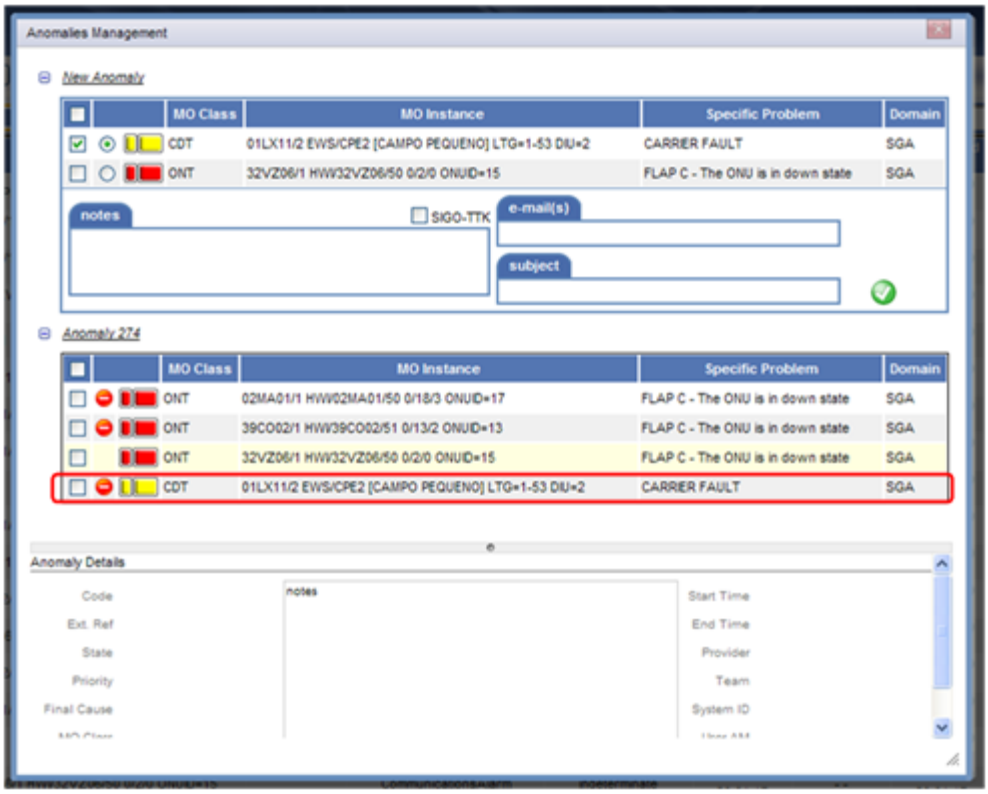
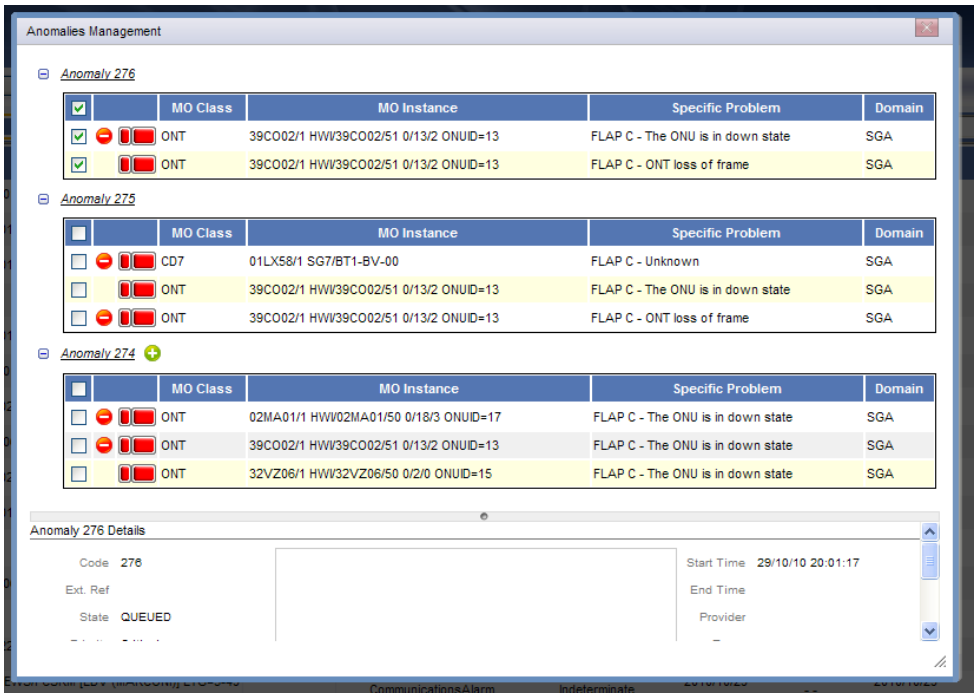


Figure 158 highlights the recently associated alarm.

Associate alarms between anomalies

On the anomalies management window it is possible to associate an alarm from an anomaly to another if not already associated with the latter. The example of this feature can be seen in Figure 159.

Figure 159. Add alarms from one anomaly to another



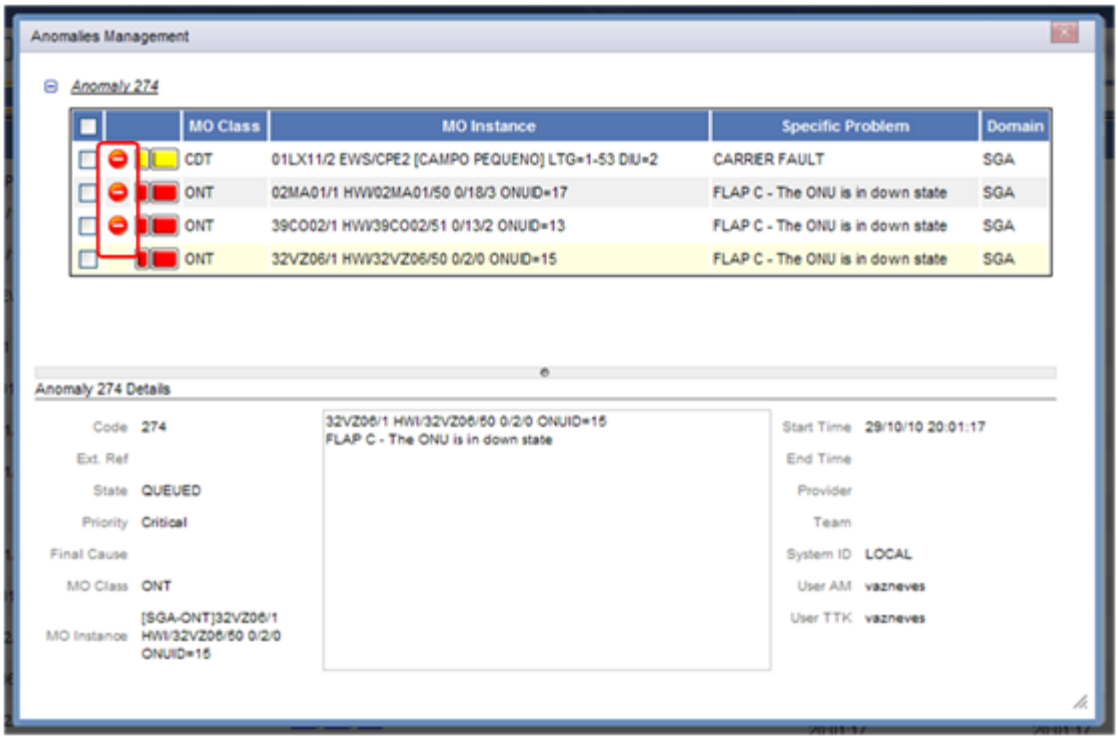
Dissociate alarms from anomalies

To dissociate an alarm from an anomaly it is necessary to select the anomaly. To select the desired anomaly will be necessary to enable the column ‘Anomalies’ in the alarm window.

Figure 160. Finding anomalies in the Active Alarms Window

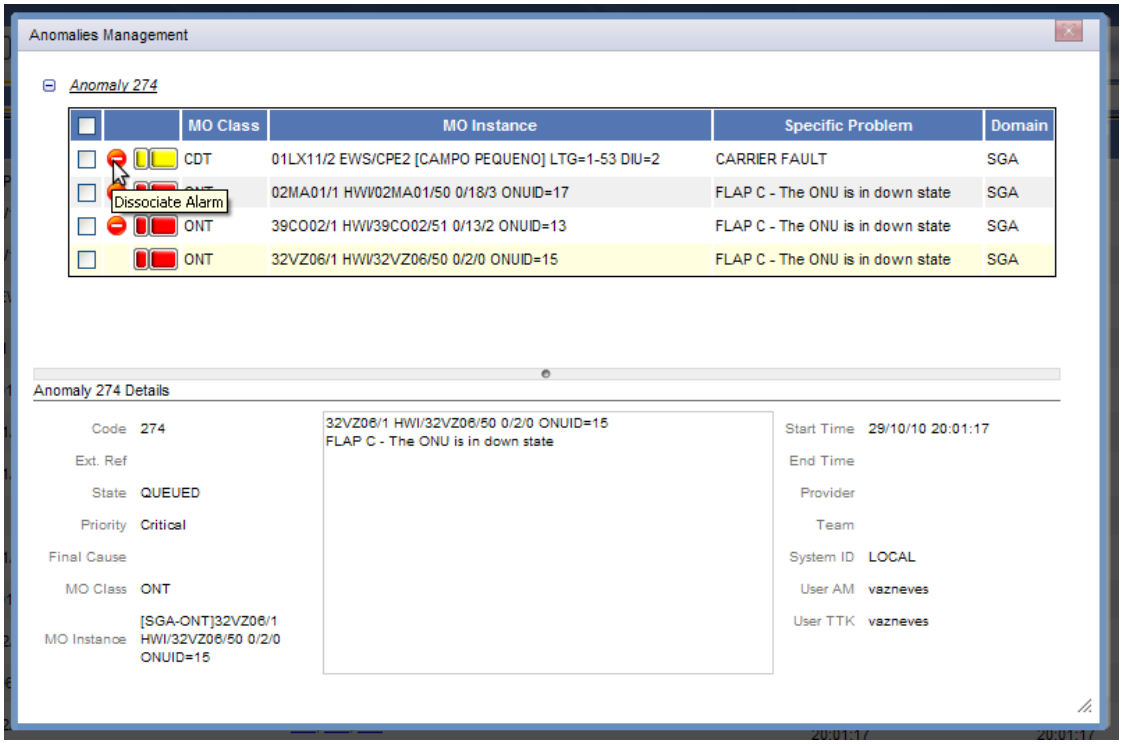
After clicking on an anomaly a window is shown with its details, as in Figure 161.

Figure 161. Anomaly details



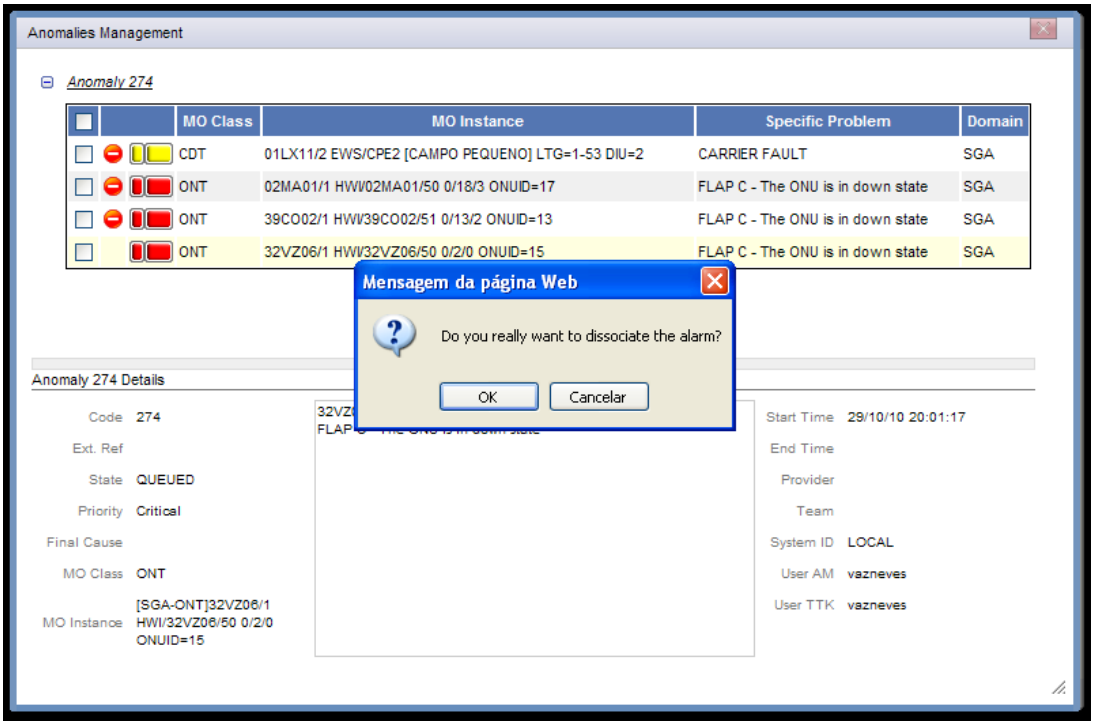
To dissociate an alarm one must click on the appropriate symbol as shown in Figure 162.

Figure 162. Dissociate Alarm



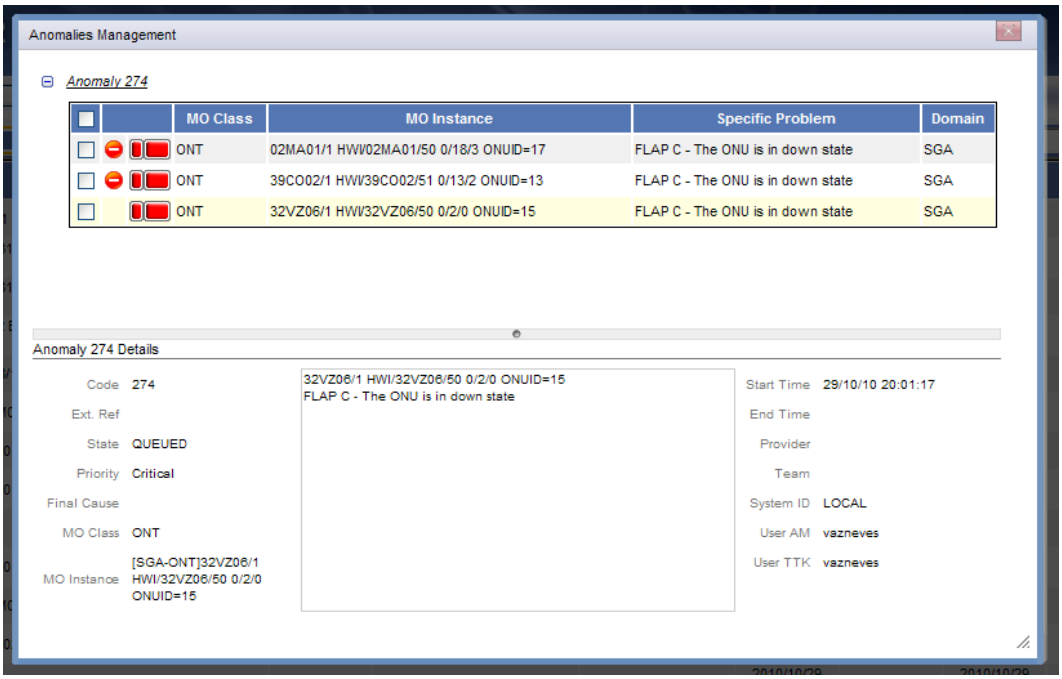
The final step is to confirm the dissociation.

Figure 163. Confirmation to dissociate an alarm



After confirmation the alarm is no longer present, as shown in Figure 164.

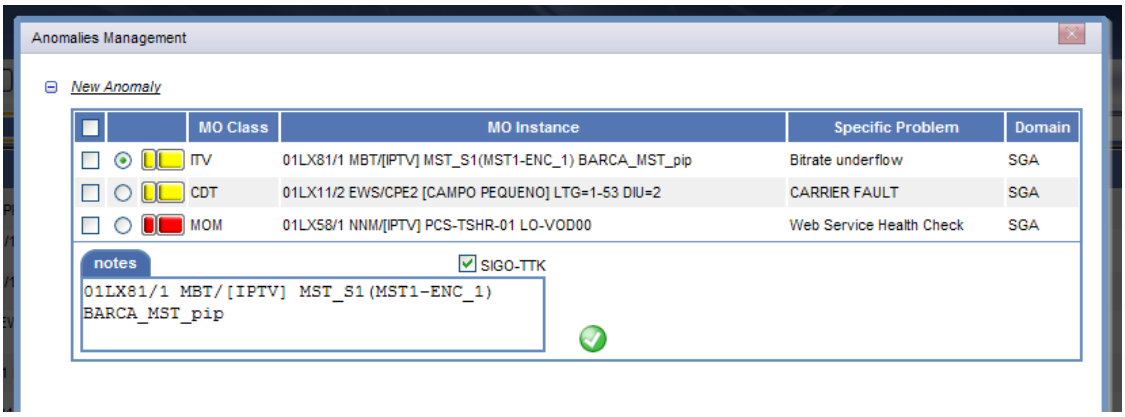
Figure 164. Anomaly after dissociation of the alarm



Register anomalies in the system of faults SIGO® TTK.

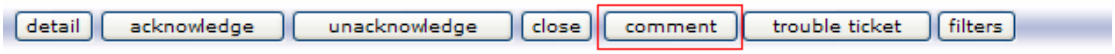
To register an anomaly on SIGO ® TTK, select the checkbox SIGO-TTK, as shown in Figure 165.

Figure 165. Registering an anomaly in the system SIGO-TTK



Alarm comments

Figure 166. Add a comment to the selected alarms



To add a comment on one or more alarms, select the desired alarm(s) and press comment button. Insert the comment on the window that should open and press enter. To cancel the operation press escape. The comment can be read in Alarm details window.

Figure 167. Comment window

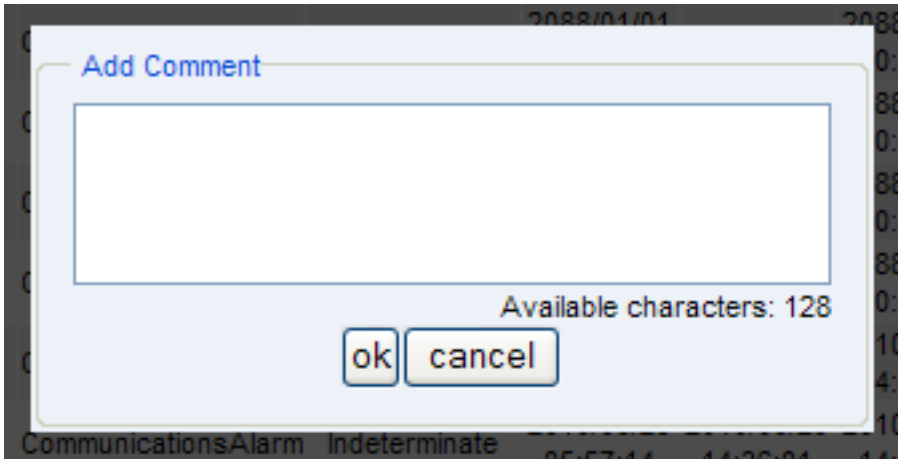
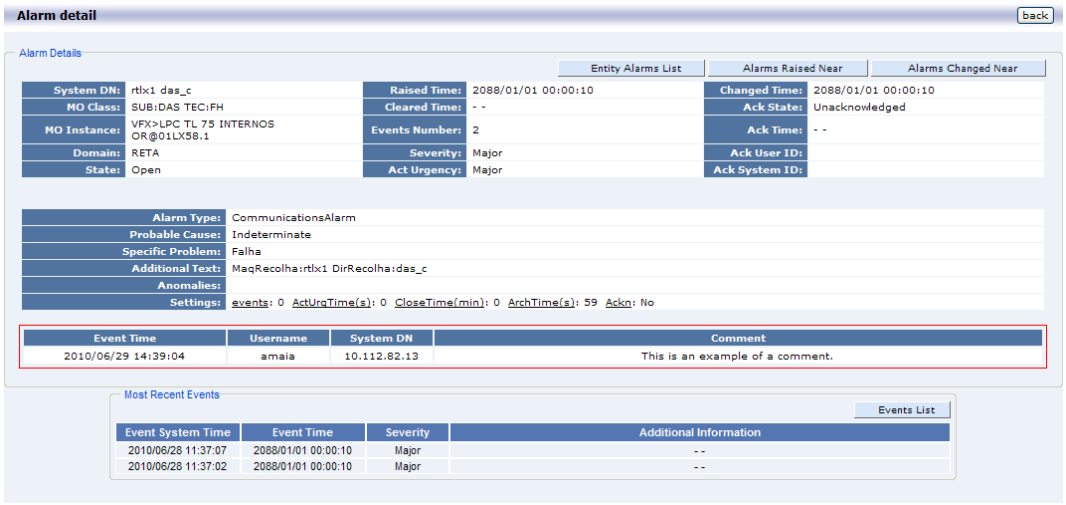


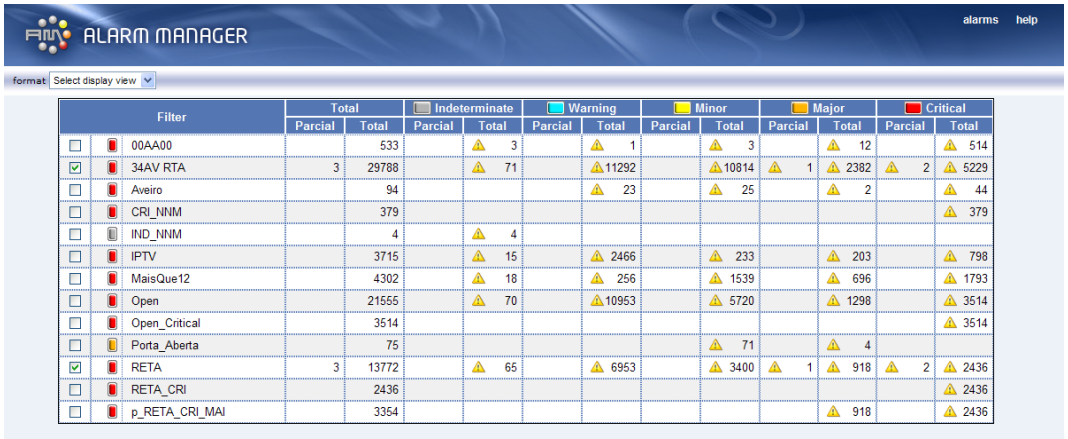
Figure 168. Comment in alarm details



Alarm Counters

Alarm counters allow the display of a summary with the numbers of received alarms that validate each filter. Thus, before accessing this functionality, it's advisable to create at least one filter, as specified previously (see "Alarm Filtering"). Clicking on counters (in the main window), a new window will be opened, showing the defined filters and the total number of alarms, organized by urgency of action.

Figure 169. Counters Table

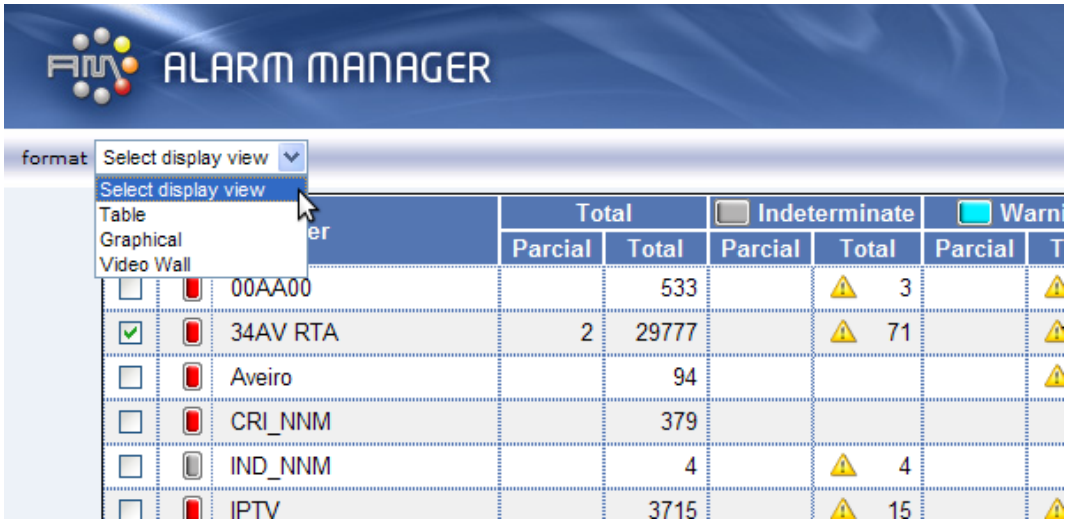


Filter	Total		Indeterminate		Warning		Minor		Major		Critical	
	Parcial	Total	Parcial	Total	Parcial	Total	Parcial	Total	Parcial	Total	Parcial	Total
00AA00		533		3		1		3		12		514
34AV RTA	3	29788		71		11292		10814	1	2382	2	5229
Aveiro		94				23		25		2		44
CRI_NNM		379										379
IND_NNM		4		4								
IPTV		3715		15		2466		233		203		798
MaisQue12		4302		18		256		1539		696		1793
Open		21555		70		10953		5720		1298		3514
Open_Critical		3514										3514
Porta_Aberta		75						71		4		
RETA	3	13772		65		6953		3400	1	918	2	2436
RETA_CRI		2436										2436
p_RETA_CRI_MAI		3354								918		2436

By selecting a specific filter (in the checkbox), the table will be updated with the following information to each filter:

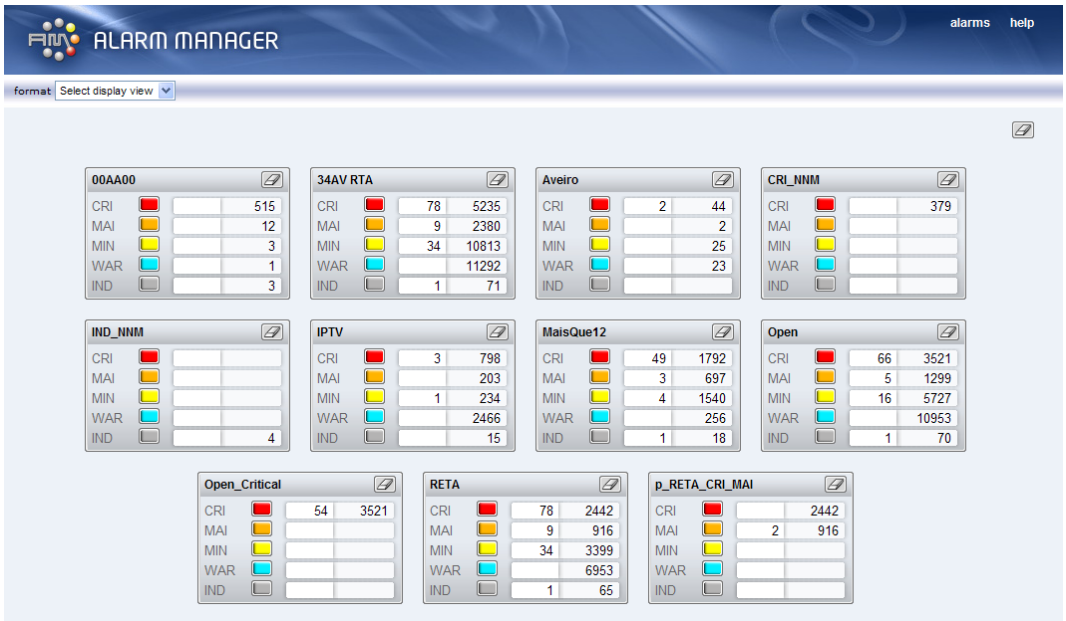
- Counter: total number of the alarms per urgency of action
- Partial Counter: total number of events or state changes, from that specific point in time onwards

Figure 170. Detail of selected Filter



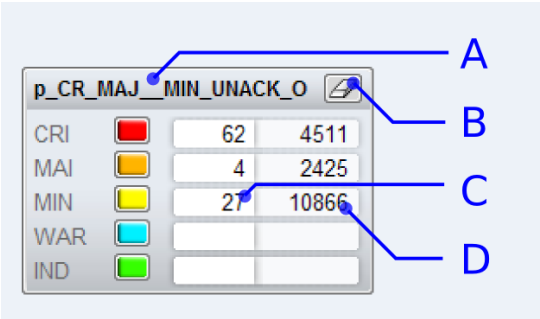
You can choose between three display formats to access the counters, using the Format select box. The first option, Table, is the default one (Figure 171). The Graphical option allows the display of single icons with counters for each filter.

Figure 171. Selection of Display Format



After selecting one or more filters, the Graphical format shows alarm counters for those filters.

Figure 172. Counter Icons



Each filter has the following options:

A. The name of the filter. It is also a link to the pending alarms list applying this filter.

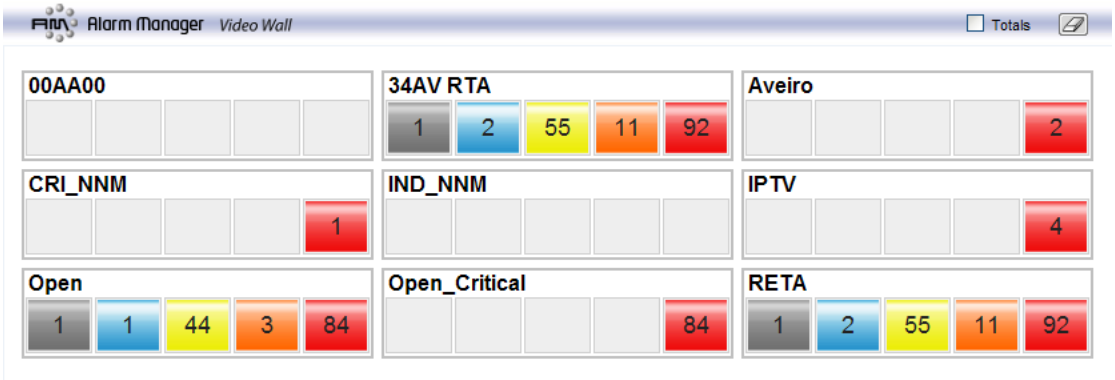
B. Clear button. Resets alarm partial counters.

C. Partial counter. Partial counters show the numbers of received alarms from selection of respective filter or since the last reset to each severity. Also a link to a list of the pointed alarms.

D. Total counter. Total counters show the total number of pending alarms of a respective filter to each severity. It is also a link to the pending alarms window with applying the filter and severity conditions.

Clicking clear will not reset total counters. There is also an option to clear all on the top right corner.

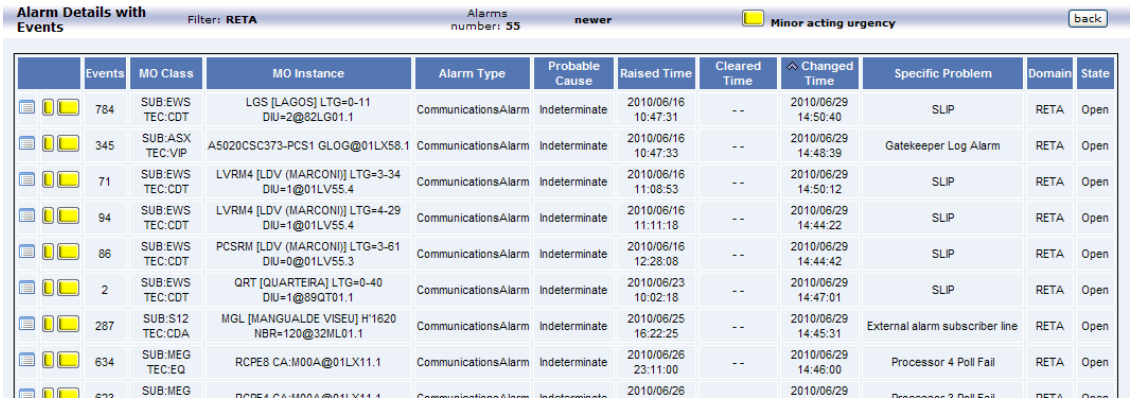
Figure 173. Video Wall



The video wall option is similar to the graphical one but with a cleaner layout, especially conceived to be displayed at wide resolutions. There is a selection box on the top right corner to show/hide total counters.

Clicking on filter name, in both display format, will be shown the main alarm window with the filtered alarms. Click on any counter to see list of alarms for the counter in question.

Figure 174. List of Alarms



	Events	MO Class	MO Instance	Alarm Type	Probable Cause	Raised Time	Cleared Time	Changed Time	Specific Problem	Domain	State
	784	SUB:EWS TEC:CDT	LGS [LAGOS] LTG=0-11 DIU=2@82LG01.1	CommunicationsAlarm	Indeterminate	2010/06/16 10:47:31	- -	2010/06/29 14:50:40	SLIP	RETA	Open
	345	SUB:ASX TEC:VIP	A5020CSC373-PCS1 GLOG@01LX58.1	CommunicationsAlarm	Indeterminate	2010/06/16 10:47:33	- -	2010/06/29 14:48:39	Gatekeeper Log Alarm	RETA	Open
	71	SUB:EWS TEC:CDT	LVRM4 [LDV (MARCONI)] LTG=3-34 DIU=1@01LV55.4	CommunicationsAlarm	Indeterminate	2010/06/16 11:08:53	- -	2010/06/29 14:50:12	SLIP	RETA	Open
	94	SUB:EWS TEC:CDT	LVRM4 [LDV (MARCONI)] LTG=4-29 DIU=1@01LV55.4	CommunicationsAlarm	Indeterminate	2010/06/16 11:11:18	- -	2010/06/29 14:44:22	SLIP	RETA	Open
	86	SUB:EWS TEC:CDT	PCSRM [LDV (MARCONI)] LTG=3-61 DIU=0@01LV55.3	CommunicationsAlarm	Indeterminate	2010/06/16 12:28:08	- -	2010/06/29 14:44:42	SLIP	RETA	Open
	2	SUB:EWS TEC:CDT	QRT [QUARTEIRA] LTG=0-40 DIU=1@89QT01.1	CommunicationsAlarm	Indeterminate	2010/06/23 10:02:18	- -	2010/06/29 14:47:01	SLIP	RETA	Open
	287	SUB:S12 TEC:CDA	MGL [MANGUALDE VISEU] H'1620 NBR=120@32ML01.1	CommunicationsAlarm	Indeterminate	2010/06/25 16:22:25	- -	2010/06/29 14:45:31	External alarm subscriber line	RETA	Open
	634	SUB:MEG TEC:EQ	RCPE8 CA:M00A@01LX11.1	CommunicationsAlarm	Indeterminate	2010/06/26 23:11:00	- -	2010/06/29 14:46:00	Processor 4 Poll Fail	RETA	Open
	[illegible]	SUB:MEG	[illegible]	[illegible]	[illegible]	2010/06/26		2010/06/29	[illegible]	[illegible]	[illegible]

Report Management

Current version of Alarm Manager supports two reporting frameworks, although only one can be available at each moment. This selection is performed at installation time.

Classical framework supports managing reports, defining filter conditions and info selection. These reports query the archived alarms historic and allow data exportation in several formats.

Exploration reports tune data exploration by allowing search criteria refinement. These reports access not only archived alarms but also pending alarms. Events correlated by each alarm can be consulted by simply clicking over an alarm, no matter if it is a pending or an archived alarm.

Alarm Exploration Reports

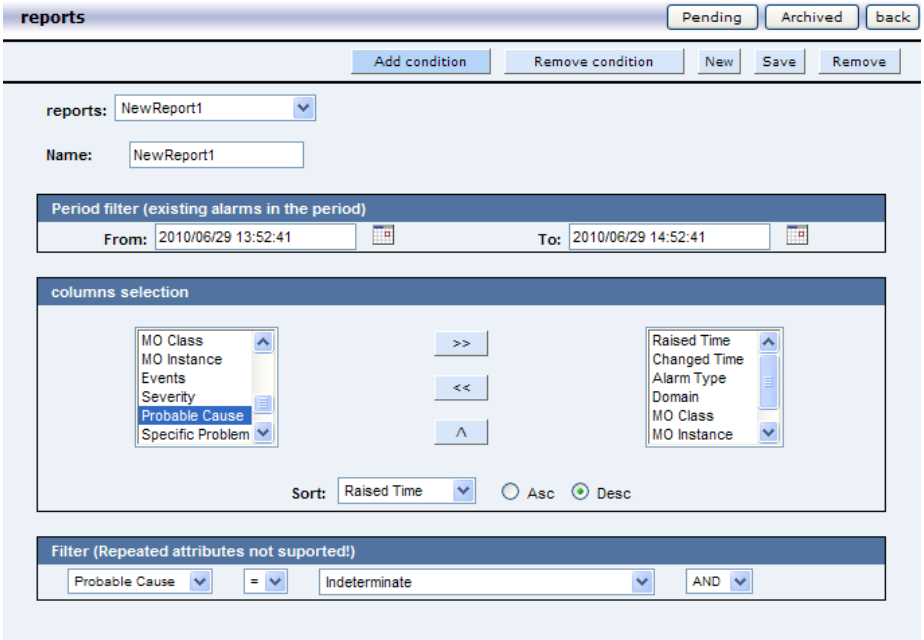
To access this functionality click on the Reports link to see the reports page (Figure 175). This page allows configuring the fields that should be displayed in the reports, the dates between the report presentation, and other additional filters that works the same way as alarm filters.

Previously saved reports can be selected or predefined reports are also available to avoid columns selection. By selecting a predefined report, the columns will become available, and they can be modified to produce a new report. Changes in columns, however, won't change the original predefined report.

Access to a report using the selection list (predefined Reports or Reports) and clicking Save, it alters the previously selected reports, even when the name is changed.

To create a new report select the icon New Report, select the columns, give them a name, and click on Save Report. To remove it, click on Remove Report.

Figure 175. Generation of Alarms' Report



Reports must specify time interval which is the interval where we want to look for alarms. There are considered valid the following situations:

- The alarm begun and end inside the interval;
- The alarm begun before the interval and ended inside it or after it;
- The alarm begun inside the interval and ended after it;

After concluded temporal specification, there must be selected the columns we want to present in the report and also the ordination field. Ordination can be ascending or descending.

Besides temporal conditions, other filtering criteria can be specified. To add a new filtering criteria press Add new condition and to remove it Remove last condition. To read more about filtering criteria go to "Alarm Filtering" section.

There are two types of reports available: Pending and Archived accessible from the buttons on right top of the frame. The first type searches over pending alarms while second report is supported over alarms already archived.

Figure 180 shows the result of a pending alarms report. In Figure 181 is shown the result for a report on archived alarms.

The presentation of reports is performed by a dedicated platform that manages search results by pagination, navigation between pages, re-ordination, data exportation, filtering specialization and other functionalities. By default reports are limited to a maximum of 100.000 alarm record.

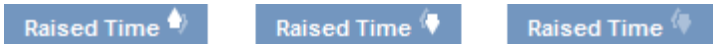
Results exploration

Navigation between pages is performed in an incremental manner, page by page, through right/left arrows or directly to first/last page through double left/right arrow on the navigation menu. This menu presents current page index ant total number of pages between arrows. At the right, there are visible alarm index presented on current page and also total number of alarms in current query result.

Figure 176. Navigation menu

It's possible to reorder results from certain columns. These are marked by a two vertical arrows. By clicking in the column header it's applied an ascending order. After applied previous order, with a new click the ordination turns descending, as seen in Figure 177.

Figure 177. Ordering results



Search Refinement

Each time a new report is generated it presents a correspondent initial subset of alarms. The experience in network monitoring and fault detection states that normally the initial query must be refined to isolate interesting events. Some fields were elected, taking into account reporting performance, to support fast refinement of initial query conditions on the report platform itself.

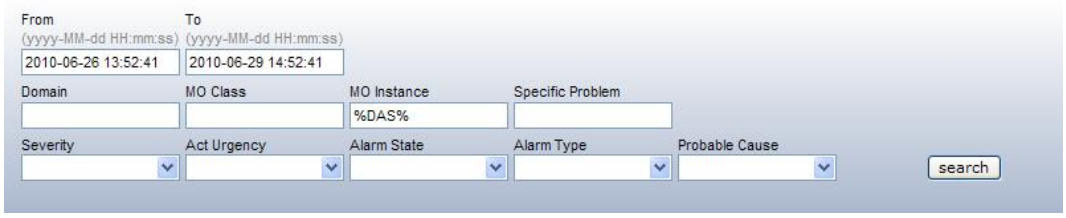
This menu can be used to redefine the interval of search. Pay attention to date and time format that must be respected (YYYY-MM-DD HH;MIN:SS). Other fields can also be redefined, such as: Domain, Managed Object Class, Managed Object Instance and Specific Problem.

NOTE: in text fields, operator '%' can be combined before or/and after words, with the following interpretations:

- searchWord% – same as 'Begins with'
- % searchWord – same as 'Ends with'
- % searchWord % – same as 'Contains'
- searchWord – same as 'Equal'

Using the operator '%' in the beginning of the search parameter degrades heavily search performance. It must be used with proper caution.

Figure 178. Search refinement menu



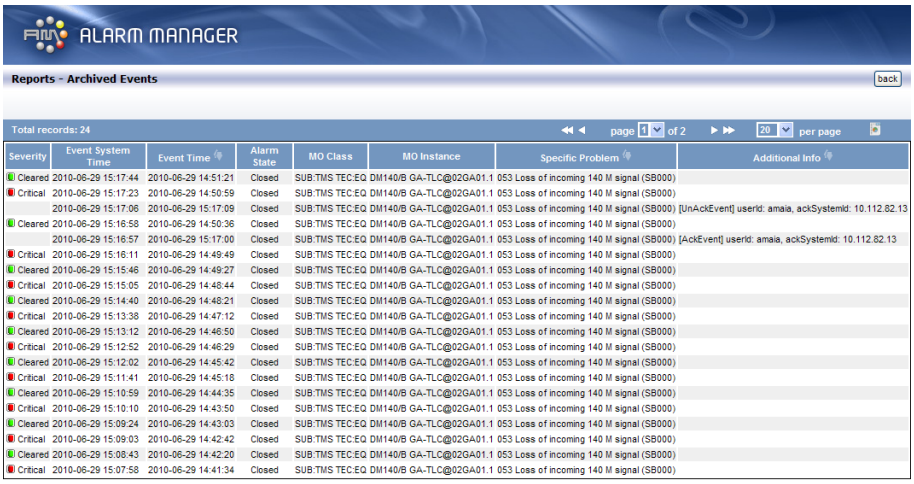
Pending alarms report only contains initial query alarm time, since pending alarms were not archived yet.

Events visualization

Alarm reports (either pending or archived) present as result of queries alarms that can correlate more than one network events. Pay attention on Number of Events.

In both alarm report types, it is possible to navigate to the list of events associated to an alarm by simply clicking on it. Figure 179 shows an example of a list of events correlated by an alarm.

Figure 179. Events List

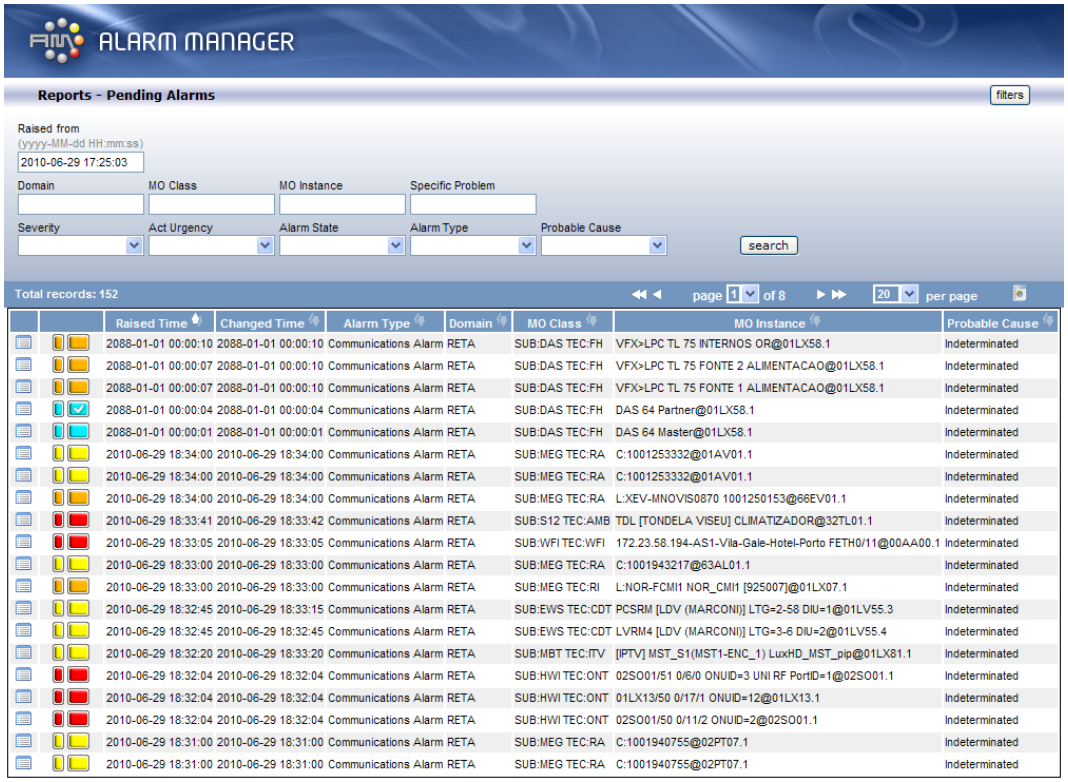


Severity	Event System Time	Event Time	Alarm State	MO Class	MO Instance	Specific Problem	Additional Info
Cleared	2010-06-29 15:17:44	2010-06-29 14:51:21	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:17:23	2010-06-29 14:50:59	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
	2010-06-29 15:17:06	2010-06-29 15:17:09	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	[UnAckEvent] userId: amaia, ackSystemId: 10.112.82.13
Cleared	2010-06-29 15:16:58	2010-06-29 14:50:36	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
	2010-06-29 15:16:57	2010-06-29 15:17:00	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	[AckEvent] userId: amaia, ackSystemId: 10.112.82.13
Critical	2010-06-29 15:16:11	2010-06-29 14:49:49	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Cleared	2010-06-29 15:15:46	2010-06-29 14:49:27	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:15:05	2010-06-29 14:48:44	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Cleared	2010-06-29 15:14:40	2010-06-29 14:48:21	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:13:38	2010-06-29 14:47:12	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Cleared	2010-06-29 15:13:12	2010-06-29 14:46:50	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:12:52	2010-06-29 14:46:29	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Cleared	2010-06-29 15:12:02	2010-06-29 14:45:42	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:11:41	2010-06-29 14:45:18	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Cleared	2010-06-29 15:10:59	2010-06-29 14:44:35	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:10:10	2010-06-29 14:43:50	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Cleared	2010-06-29 15:09:24	2010-06-29 14:43:03	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:09:03	2010-06-29 14:42:42	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Cleared	2010-06-29 15:08:43	2010-06-29 14:42:20	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	
Critical	2010-06-29 15:07:58	2010-06-29 14:41:34	Closed	SUB:TMS TEC:EQ	DM140/B GA-TLC@02GA01.1	053 Loss of incoming 140 M signal (SB000)	

Pending alarms example report

Figure 180 exemplifies a report on pending alarms.

Figure 180. Pending alarms report

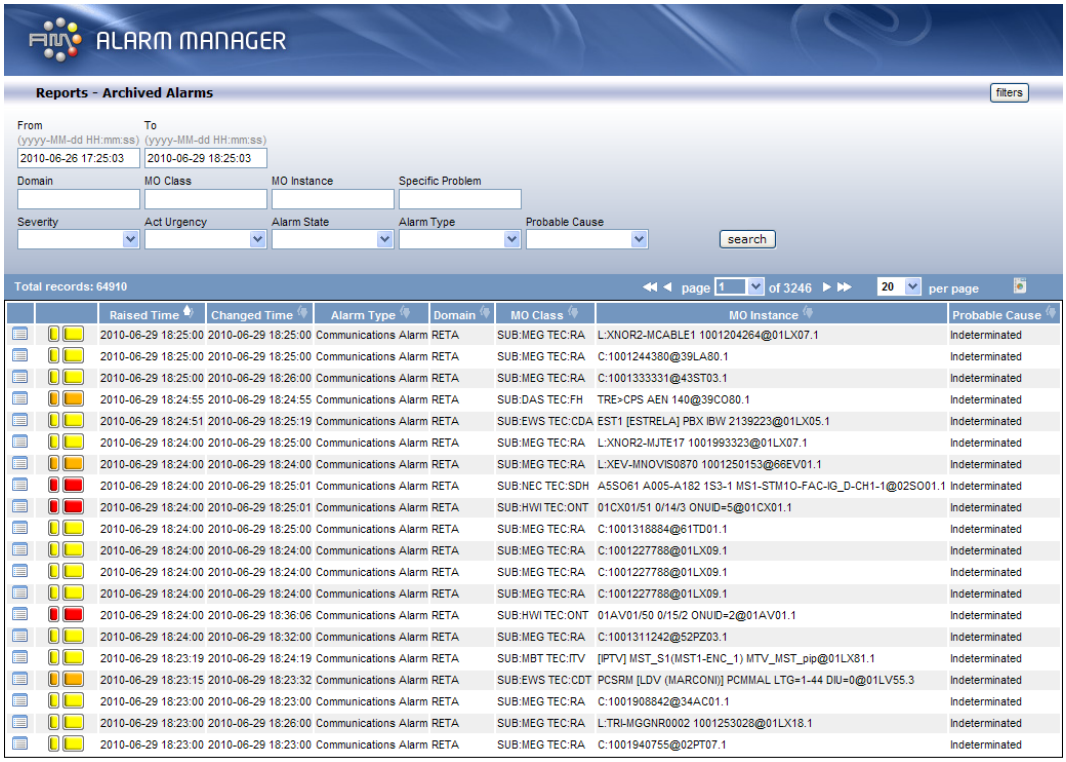


Raised Time	Changed Time	Alarm Type	Domain	MO Class	MO Instance	Probable Cause
2088-01-01 00:00:10	2088-01-01 00:00:10	Communications Alarm	RETA	SUB:DAS TEC:FH	VFX>LPC TL 75 INTERNOS OR@01LX58.1	Indeterminated
2088-01-01 00:00:07	2088-01-01 00:00:10	Communications Alarm	RETA	SUB:DAS TEC:FH	VFX>LPC TL 75 FONTE 2 ALIMENTACAO@01LX58.1	Indeterminated
2088-01-01 00:00:07	2088-01-01 00:00:10	Communications Alarm	RETA	SUB:DAS TEC:FH	VFX>LPC TL 75 FONTE 1 ALIMENTACAO@01LX58.1	Indeterminated
2088-01-01 00:00:04	2088-01-01 00:00:04	Communications Alarm	RETA	SUB:DAS TEC:FH	DAS 64 Partner@01LX58.1	Indeterminated
2088-01-01 00:00:01	2088-01-01 00:00:01	Communications Alarm	RETA	SUB:DAS TEC:FH	DAS 64 Master@01LX58.1	Indeterminated
2010-06-29 18:34:00	2010-06-29 18:34:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001253332@01AV01.1	Indeterminated
2010-06-29 18:34:00	2010-06-29 18:34:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001253332@01AV01.1	Indeterminated
2010-06-29 18:34:00	2010-06-29 18:34:00	Communications Alarm	RETA	SUB:MEG TEC:RA	L:XEV-MNOVIS0870 1001250153@66EV01.1	Indeterminated
2010-06-29 18:33:41	2010-06-29 18:33:42	Communications Alarm	RETA	SUB:S12 TEC:AMB	TDL [TONDELA VISEU] CLIMATIZADOR@32TL01.1	Indeterminated
2010-06-29 18:33:05	2010-06-29 18:33:05	Communications Alarm	RETA	SUB:WFI TEC:WFI	172.23.58.194-AS1-Vila-Gale-Hotel-Porto FETH0/11@00AA00.1	Indeterminated
2010-06-29 18:33:00	2010-06-29 18:33:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001943217@63AL01.1	Indeterminated
2010-06-29 18:33:00	2010-06-29 18:33:00	Communications Alarm	RETA	SUB:MEG TEC:RI	L:NOR-FCMI1 NOR_CMI1 [925007]@01LX07.1	Indeterminated
2010-06-29 18:32:45	2010-06-29 18:33:15	Communications Alarm	RETA	SUB:EWS TEC:CDT	PCSRM [LDV (MARCONI)] LTG=2-58 DIU=1@01LV55.3	Indeterminated
2010-06-29 18:32:45	2010-06-29 18:32:45	Communications Alarm	RETA	SUB:EWS TEC:CDT	LVRM4 [LDV (MARCONI)] LTG=3-6 DIU=2@01LV55.4	Indeterminated
2010-06-29 18:32:20	2010-06-29 18:33:20	Communications Alarm	RETA	SUB:MBT TEC:ITV	[IPTV] MST_S1(MST1-ENC_1) LuxHD_MST_pip@01LX81.1	Indeterminated
2010-06-29 18:32:04	2010-06-29 18:32:04	Communications Alarm	RETA	SUB:HWI TEC:ONT	02SO01/51 0/6/0 ONUID=3 UNI RF PortID=1@02SO01.1	Indeterminated
2010-06-29 18:32:04	2010-06-29 18:32:04	Communications Alarm	RETA	SUB:HWI TEC:ONT	01LX13/50 0/17/1 ONUID=12@01LX13.1	Indeterminated
2010-06-29 18:32:04	2010-06-29 18:32:04	Communications Alarm	RETA	SUB:HWI TEC:ONT	02SO01/50 0/11/2 ONUID=2@02SO01.1	Indeterminated
2010-06-29 18:31:00	2010-06-29 18:31:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001940755@02PT07.1	Indeterminated
2010-06-29 18:31:00	2010-06-29 18:31:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001940755@02PT07.1	Indeterminated

Archived alarms example report

Figure 181 exemplifies a report on archived alarms.

Figure 181. Archived alarms report



Raised Time	Changed Time	Alarm Type	Domain	MO Class	MO Instance	Probable Cause
2010-06-29 18:25:00	2010-06-29 18:25:00	Communications Alarm	RETA	SUB:MEG TEC:RA	L:XNOR2-MCABLE1 1001204264@01LX07.1	Indeterminated
2010-06-29 18:25:00	2010-06-29 18:25:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001244380@39LA80.1	Indeterminated
2010-06-29 18:25:00	2010-06-29 18:26:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001333331@43ST03.1	Indeterminated
2010-06-29 18:24:55	2010-06-29 18:24:55	Communications Alarm	RETA	SUB:DAS TEC:FH	TRE>CPS AEN 140@39CO80.1	Indeterminated
2010-06-29 18:24:51	2010-06-29 18:25:19	Communications Alarm	RETA	SUB:EWS TEC:CDA	EST1 [ESTRELA] PBX IBW 2139223@01LX05.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:25:00	Communications Alarm	RETA	SUB:MEG TEC:RA	L:XNOR2-MJTE17 1001993323@01LX07.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:24:00	Communications Alarm	RETA	SUB:MEG TEC:RA	L:XEV-MNOVIS0870 1001250153@66EV01.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:25:01	Communications Alarm	RETA	SUB:NEC TEC:SDH	A5SO61 A005-A182 1S3-1 MS1-STM1O-FAC-IG_D-CH1-1@02SO01.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:25:01	Communications Alarm	RETA	SUB:HWI TEC:ONT	01CX01/51 0/14/3 ONUID=5@01CX01.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:25:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001318884@61TD01.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:24:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001227788@01LX09.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:24:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001227788@01LX09.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:24:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001227788@01LX09.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:36:06	Communications Alarm	RETA	SUB:HWI TEC:ONT	01AV01/50 0/15/2 ONUID=2@01AV01.1	Indeterminated
2010-06-29 18:24:00	2010-06-29 18:32:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001311242@52PZ03.1	Indeterminated
2010-06-29 18:23:19	2010-06-29 18:24:19	Communications Alarm	RETA	SUB:MBT TEC:ITV	[IPTV] MST_S1(MST1-ENC_1) MTV_MST_pip@01LX81.1	Indeterminated
2010-06-29 18:23:15	2010-06-29 18:23:32	Communications Alarm	RETA	SUB:EWS TEC:CDT	PCSRM [LDV (MARCONI)] PCMMAL LTG=1-44 DIU=0@01LV55.3	Indeterminated
2010-06-29 18:23:00	2010-06-29 18:23:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001908842@34AC01.1	Indeterminated
2010-06-29 18:23:00	2010-06-29 18:26:00	Communications Alarm	RETA	SUB:MEG TEC:RA	L:TRI-MGGNR0002 1001253028@01LX18.1	Indeterminated
2010-06-29 18:23:00	2010-06-29 18:23:00	Communications Alarm	RETA	SUB:MEG TEC:RA	C:1001940755@02PT07.1	Indeterminated

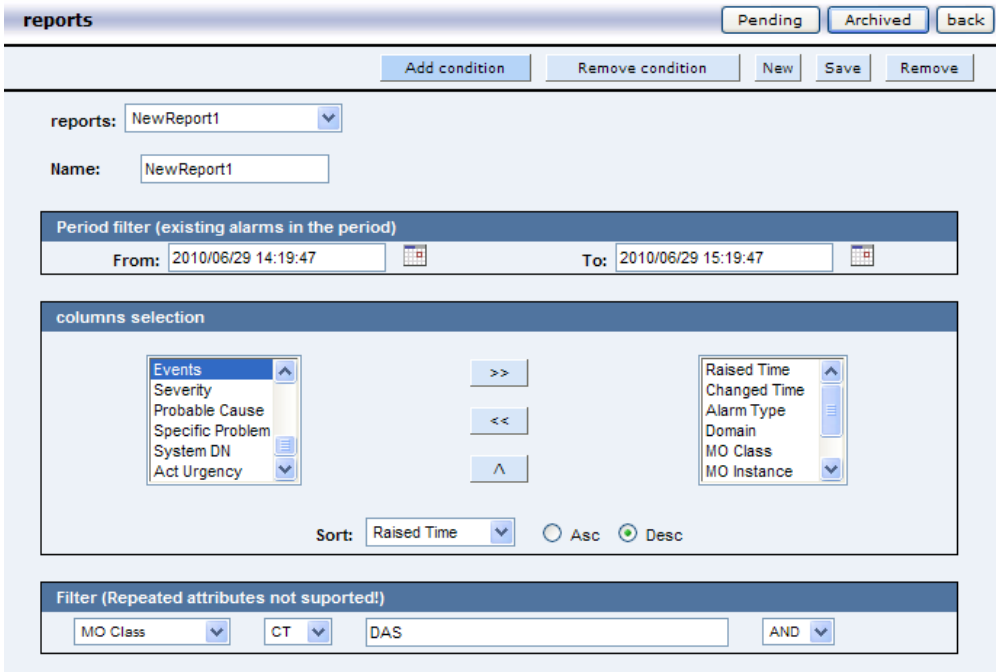
Classical Reports

To access this functionality click on the Reports link to see the reports page (Figure 182). This page allows configuring the fields that should be displayed in the reports, the dates between the report presentation, and other additional filters that works the same way as alarm filters. Previously saved reports can be selected or predefined reports are also available to avoid columns selection. By selecting a predefined report, the columns will become available, and they can be modified to produce a new report. Changes in columns, however, won't change the original predefined report.

Access to a report using the selection list (predefined Reports or Reports) and clicking Save, it alters the previously selected reports, even when the name is changed. To create a new report select the icon New Report, select the columns, give them a name, and click on Save Report. To remove a report click on Remove Report.

There are three possible report presentation formats: HTML, PDF and Excel. In case of PDF, Acrobat Reader must be correctly installed in client side. In case of an Excel report, MSExcel must be correctly installed in client side. Presentation form can be selected by respectively clicking on Generate Report or Generate PDF Report or Generate Excel Report.

Figure 182. Generation of Alarms Report



The HTML type report is shown in Figure 183 and the PDF report is shown in Figure 184. Report results in MS Excel format are displayed in Figure 185.

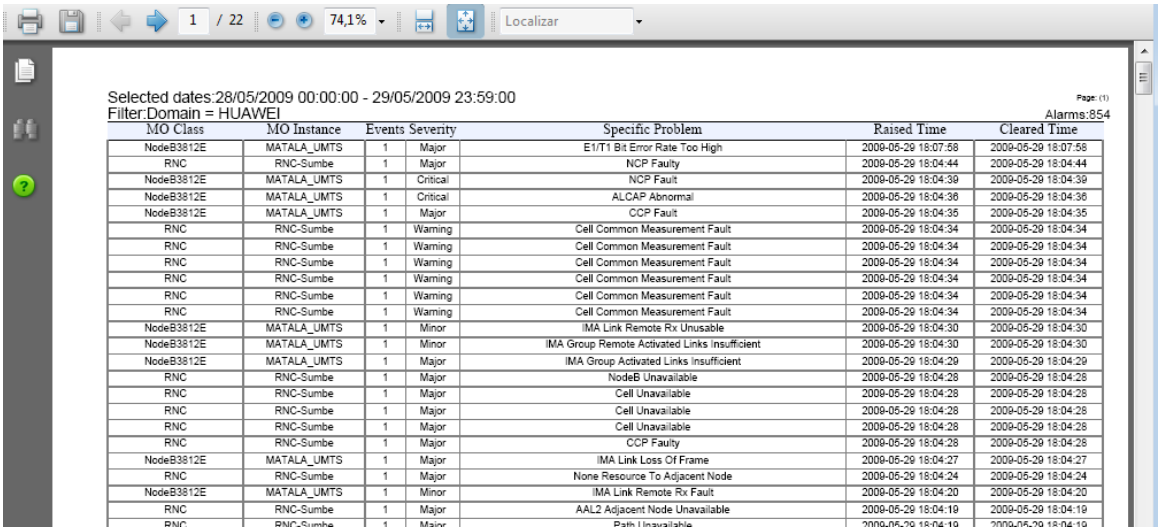
Figure 183. Alarm Report (HTML)

Selected dates:28/05/2009 00:00:00 - 29/05/2009 23:59:00 Alarms:11407

Filter:

Alarm Type	MO Class	MO Instance	Events	Severity	Specific Problem	Raised Time	Cleared Time
CommunicationsAlarm	P_GBIT_ETH	MC7_CO:PL_MC7_4GBE MC7_CO/16/1	19	Critical	LOS: Loss of signal	2008-07-28 17:03:48	2033-06-17 19:08:54
CommunicationsAlarm	P_2M	E2V8:PL_E2V8 LTSHDSL8g_175/1/2/1/2	3	Critical	LOS: Loss of signal	2009-01-28 14:50:57	2019-01-28 18:55:40
CommunicationsAlarm	P_2M	E2V8:PL_E2V8 LTSHDSL8g_175/1/2/1/3	3	Critical	LOS: Loss of signal	2009-01-28 14:50:57	2019-01-28 18:55:40
CommunicationsAlarm	P_2M	E2V8:PL_E2V8 LTSHDSL8g_175/1/2/1/4	4	Critical	LOS: Loss of signal	2009-01-28 14:50:56	2019-01-28 18:55:40
CommunicationsAlarm	P_2M	E2V8:PL_E2V8 LTSHDSL8g_175/1/2/1/5	4	Critical	LOS: Loss of signal	2009-01-28 14:50:56	2019-01-28 18:55:40
CommunicationsAlarm	P_2M	E2V8:PL_E2V8 LTSHDSL8g_175/1/2/1/6	4	Critical	LOS: Loss of signal	2009-01-28 14:50:56	2019-01-28 18:55:40
CommunicationsAlarm	P_2M	E2V8:PL_E2V8 LTSHDSL8g_175/1/2/1/7	4	Critical	LOS: Loss of signal	2009-01-28 14:50:56	2019-01-28 18:55:40
CommunicationsAlarm	P_2M	E2V8:PL_E2V8 LTSHDSL8g_175/1/2/1/8	4	Critical	LOS: Loss of signal	2009-01-28 14:50:56	2019-01-28 18:55:40
CommunicationsAlarm	P_2M	MAIS1:PL_MAIS_T2S1E16D0G0 MAIS1-Cadime/1/11	4	Warning	IMALNK: IMA Link Error	2009-05-27 23:46:11	2009-05-28 00:04:11
CommunicationsAlarm	IFL_IMA_ATM	MAIS1:PL_MAIS_T2S1E16D0G0 MAIS1-Cadime/1/27	5	Critical	LOC: Loss of cell delineation	2009-05-27 23:46:11	2009-05-28 00:04:12
CommunicationsAlarm	P_2M	MAIS16:PL_MAIS-T4 MAIS16_CADIME/1/4	4	Warning	IMALNK: IMA Link Error	2009-05-27 23:46:17	2009-05-28 00:04:17
CommunicationsAlarm	IFL_IMA_ATM	MAIS16:PL_MAIS_AG MAIS16_CADIME/9/33	4	Critical	LOC: Loss of cell delineation	2009-05-27 23:46:17	2009-05-28 00:04:17

Figure 184. Alarm Report (PDF)

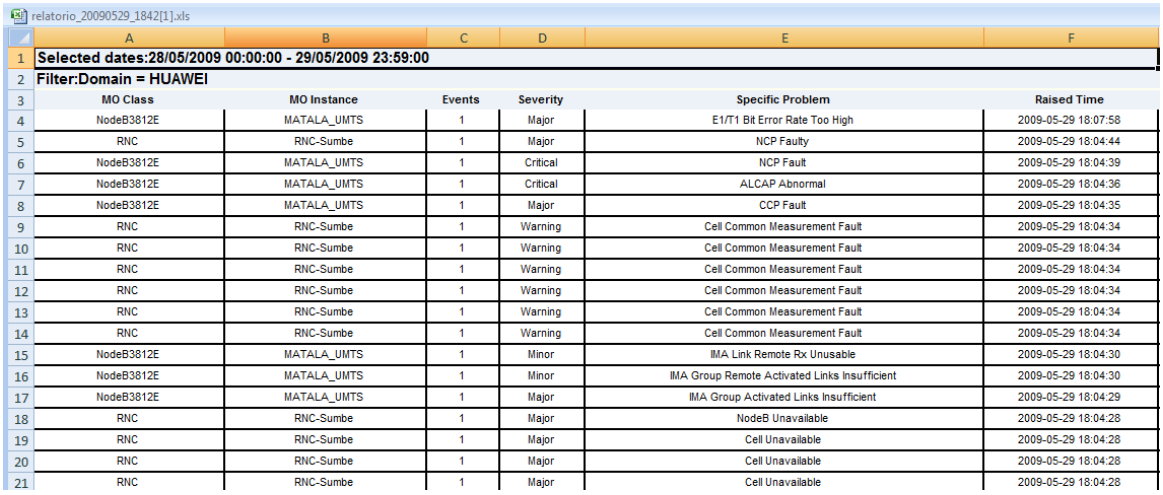


Selected dates:28/05/2009 00:00:00 - 29/05/2009 23:59:00
Filter:Domain = HUAWEI

Page: (1)
Alarms:854

MO Class	MO Instance	Events	Severity	Specific Problem	Raised Time	Cleared Time
NodeB3812E	MATALA_UMTS	1	Major	E1/T1 Bit Error Rate Too High	2009-05-29 18:07:58	2009-05-29 18:07:58
RNC	RNC-Sumbe	1	Major	NCP Faulty	2009-05-29 18:04:44	2009-05-29 18:04:44
NodeB3812E	MATALA_UMTS	1	Critical	NCP Fault	2009-05-29 18:04:39	2009-05-29 18:04:39
NodeB3812E	MATALA_UMTS	1	Critical	ALCAP Abnormal	2009-05-29 18:04:36	2009-05-29 18:04:36
NodeB3812E	MATALA_UMTS	1	Major	CCP Fault	2009-05-29 18:04:35	2009-05-29 18:04:35
RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34	2009-05-29 18:04:34
RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34	2009-05-29 18:04:34
RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34	2009-05-29 18:04:34
RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34	2009-05-29 18:04:34
RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34	2009-05-29 18:04:34
RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34	2009-05-29 18:04:34
NodeB3812E	MATALA_UMTS	1	Minor	IMA Link Remote Rx Unusable	2009-05-29 18:04:30	2009-05-29 18:04:30
NodeB3812E	MATALA_UMTS	1	Minor	IMA Group Remote Activated Links Insufficient	2009-05-29 18:04:30	2009-05-29 18:04:30
NodeB3812E	MATALA_UMTS	1	Major	IMA Group Activated Links Insufficient	2009-05-29 18:04:29	2009-05-29 18:04:29
RNC	RNC-Sumbe	1	Major	NodeB Unavailable	2009-05-29 18:04:28	2009-05-29 18:04:28
RNC	RNC-Sumbe	1	Major	Cell Unavailable	2009-05-29 18:04:28	2009-05-29 18:04:28
RNC	RNC-Sumbe	1	Major	Cell Unavailable	2009-05-29 18:04:28	2009-05-29 18:04:28
RNC	RNC-Sumbe	1	Major	Cell Unavailable	2009-05-29 18:04:28	2009-05-29 18:04:28
RNC	RNC-Sumbe	1	Major	CCP Faulty	2009-05-29 18:04:28	2009-05-29 18:04:28
NodeB3812E	MATALA_UMTS	1	Major	IMA Link Loss Of Frame	2009-05-29 18:04:27	2009-05-29 18:04:27
RNC	RNC-Sumbe	1	Major	None Resource To Adjacent Node	2009-05-29 18:04:24	2009-05-29 18:04:24
NodeB3812E	MATALA_UMTS	1	Minor	IMA Link Remote Rx Fault	2009-05-29 18:04:20	2009-05-29 18:04:20
RNC	RNC-Sumbe	1	Major	AAL2 Adjacent Node Unavailable	2009-05-29 18:04:19	2009-05-29 18:04:19
RNC	RNC-Sumbe	1	Major	Path Unavailable	2009-05-29 18:04:19	2009-05-29 18:04:19

Figure 185. Alarm Report EXCEL



	A	B	C	D	E	F
1	**Selected dates:28/05/2009 00:00:00 - 29/05/2009 23:59:00**					
2	**Filter:Domain = HUAWEI**					
3	**MO Class**	**MO Instance**	**Events**	**Severity**	**Specific Problem**	**Raised Time**
4	NodeB3812E	MATALA_UMTS	1	Major	E1/T1 Bit Error Rate Too High	2009-05-29 18:07:58
5	RNC	RNC-Sumbe	1	Major	NCP Faulty	2009-05-29 18:04:44
6	NodeB3812E	MATALA_UMTS	1	Critical	NCP Fault	2009-05-29 18:04:39
7	NodeB3812E	MATALA_UMTS	1	Critical	ALCAP Abnormal	2009-05-29 18:04:36
8	NodeB3812E	MATALA_UMTS	1	Major	CCP Fault	2009-05-29 18:04:35
9	RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34
10	RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34
11	RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34
12	RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34
13	RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34
14	RNC	RNC-Sumbe	1	Warning	Cell Common Measurement Fault	2009-05-29 18:04:34
15	NodeB3812E	MATALA_UMTS	1	Minor	IMA Link Remote Rx Unusable	2009-05-29 18:04:30
16	NodeB3812E	MATALA_UMTS	1	Minor	IMA Group Remote Activated Links Insufficient	2009-05-29 18:04:30
17	NodeB3812E	MATALA_UMTS	1	Major	IMA Group Activated Links Insufficient	2009-05-29 18:04:29
18	RNC	RNC-Sumbe	1	Major	NodeB Unavailable	2009-05-29 18:04:28
19	RNC	RNC-Sumbe	1	Major	Cell Unavailable	2009-05-29 18:04:28
20	RNC	RNC-Sumbe	1	Major	Cell Unavailable	2009-05-29 18:04:28
21	RNC	RNC-Sumbe	1	Major	Cell Unavailable	2009-05-29 18:04:28

Rules

Concept

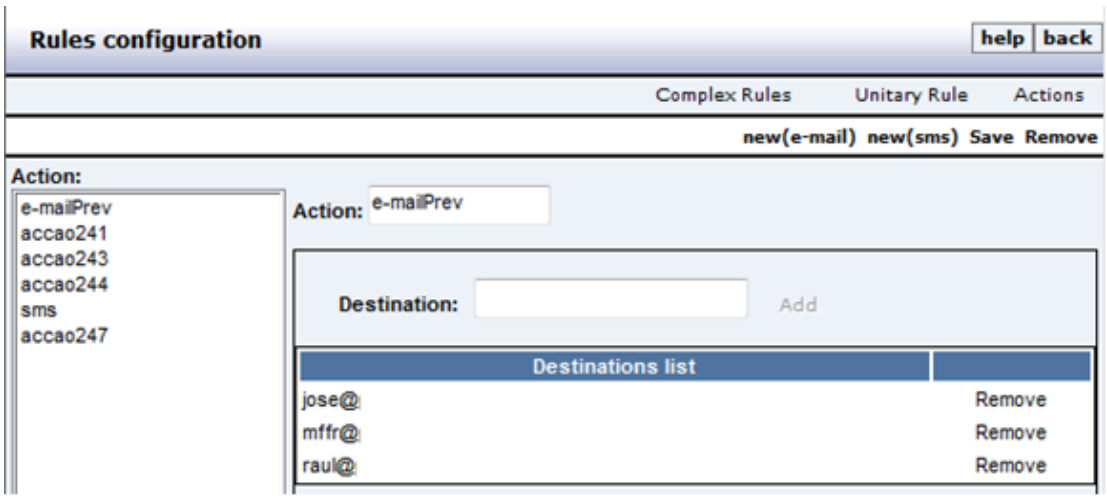
A validation system of received alarms was created to assist generations of automatic actions that depend on validations of rules on dynamic alarm properties. A received alarm is submitted to validation of complex active rules. Whenever one of these rules is true, an e-mail is sent to the address(es) in the action associated to the Complex rule. To configure rules, click on the rules link on the top right corner of the main window.

The blue bar is used for browsing through the configuration of Complex Rules, Unitary Rules and Actions, by selecting the respective icons.

Actions

An action identifies the e-mail address(es) or SMS number(s) of all destination receivers in case of a complex rule, to which this action is associated, is verified with an alarm received event.

Figure 186. Action configuration window



To create a new action click on new(e-mail) or new(sms), on the top right corner. A new rule is then created with a default name and an automatically generated e-mail address if it is an e-mail action (it will work as the address of the sender). Create the table with destination address(es), writing them on the Destination field, and clicking Add. To remove the destination e-mail or sms address, click on Remove on the same line.

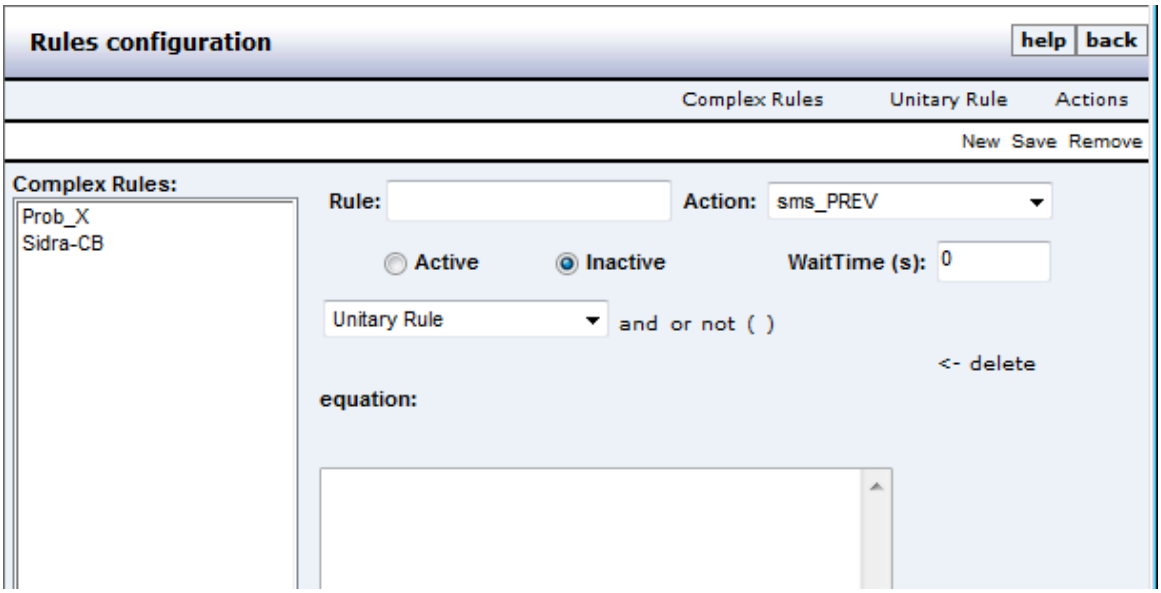
Click Save to refresh information for each action.

An action can be removed by selecting it in the list on the left, and clicking Remove on the white toolbar.

Complex Rules

A complex rule is a boolean expression, consisting in one or more unitary rules that represent terms of the given equation. The equation is the rule that will validate the received alarms.

Figure 187. Complex Rules Configuration Window



To create a new complex rule, both unitary rules and the action to be used must be previously created. Click on New to create a new complex rule.

A new complex rule is created intuitively, by creating an equation using unitary rules, boolean operators and parenthesis.

A complex rule can be immediately active if the Active icon is selected when the rule is saved. Alarms are then validated with this rule. To deactivate the rule, just select the Inactive icon and then Save.

To save any change to a complex rule, click on Save.

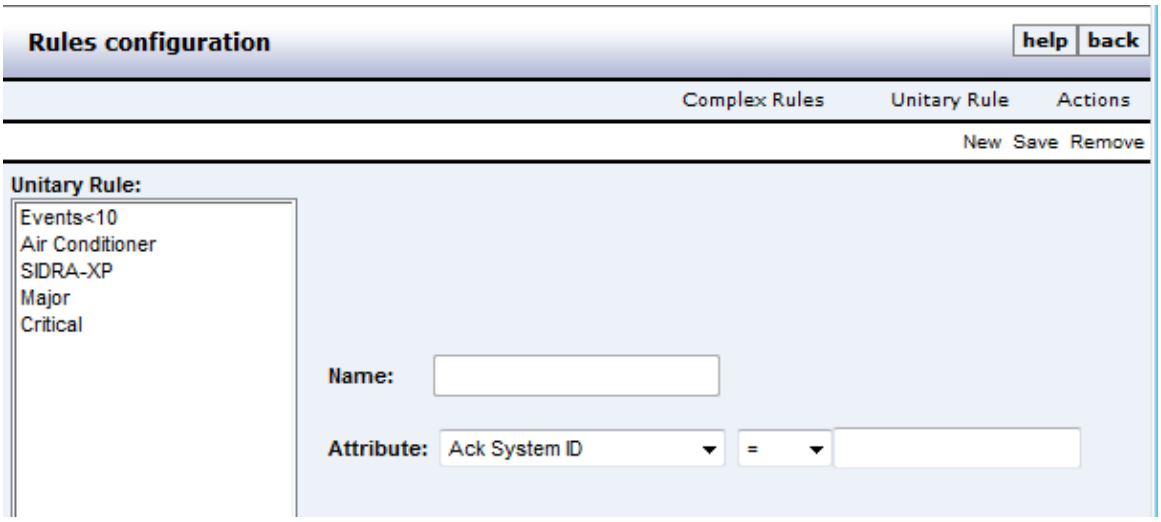
To remove a complex rule, select the desired rule on the left and click Remove.

The attribute 'Waiting Time(s)' allows definition of waiting time in action execution. If, after this period of time, the alarm that validates the rule and started the action is still active and validates the condition, then the action is performed. Otherwise, the action is not performed.

Unitary Rules

The unitary rule is a term of equation that can be combined with logical operators in the complex rule. The expression of the unitary rule points out the attribute which will be validated and its value, or to which values the expression is true.

Figure 188. Unitary Rule Configuration Window



A new unitary rule is created by clicking on New. The attribute is selected from the attributes list and, depending on the type of the accepted data, the value field is altered between data introduction field, free field or selection with predefined values.

Click Save to store in the database, the existing information on the window.

To remove a rule, select the rule from the list and click Remove.

Example

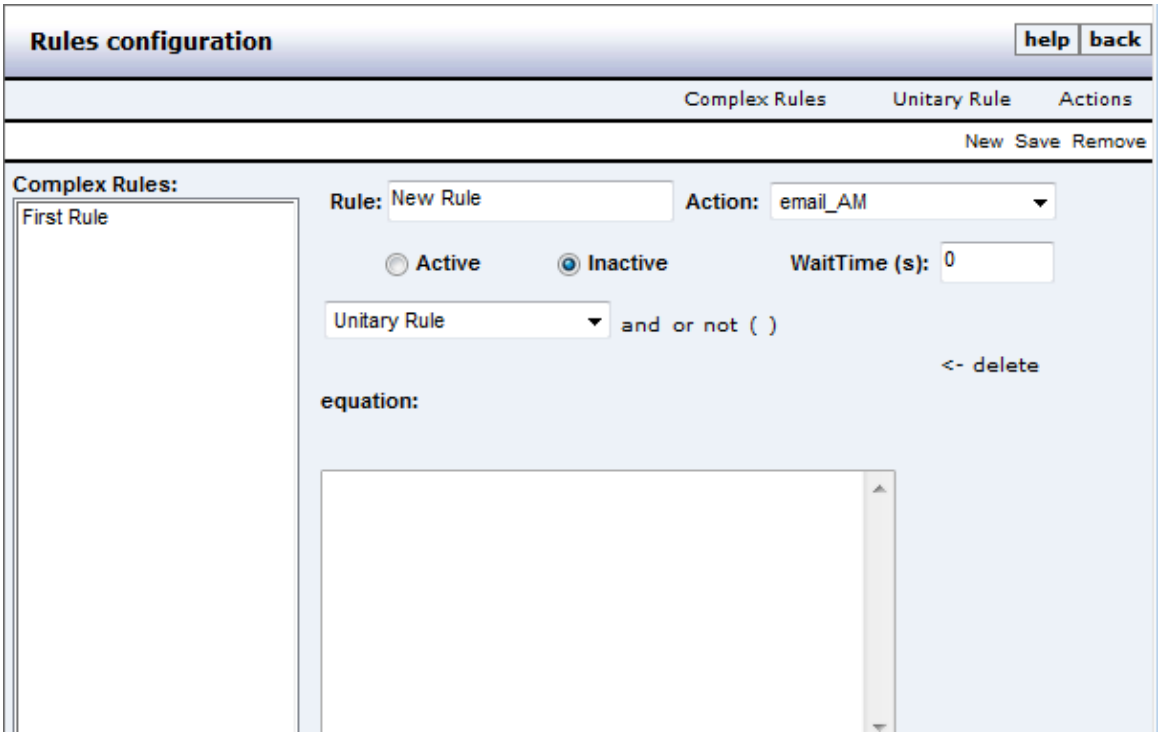
This chapter will show the creation of a complex rule, to illustrate the creation of Complex Rules, Unitary Rules and Actions.

To create a Complex Rule, the Unitary Rule and Action that will be used must be previously created.

Creation of a new Action

In the Actions setup window, click new(e-mail).

Figure 189. New Action



A new e-mail action with preset name is created. For this example we will change the Action name to mail-exemplo. Click Add.

Figure 190. Altering preset data

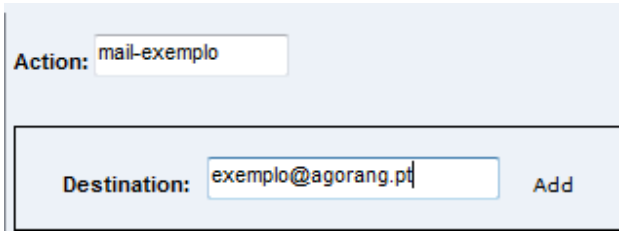
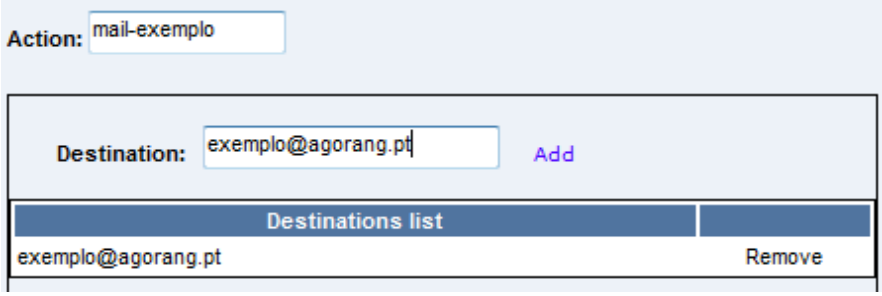


Figure 191. After adding E-Mail



To save this Action, click Save.

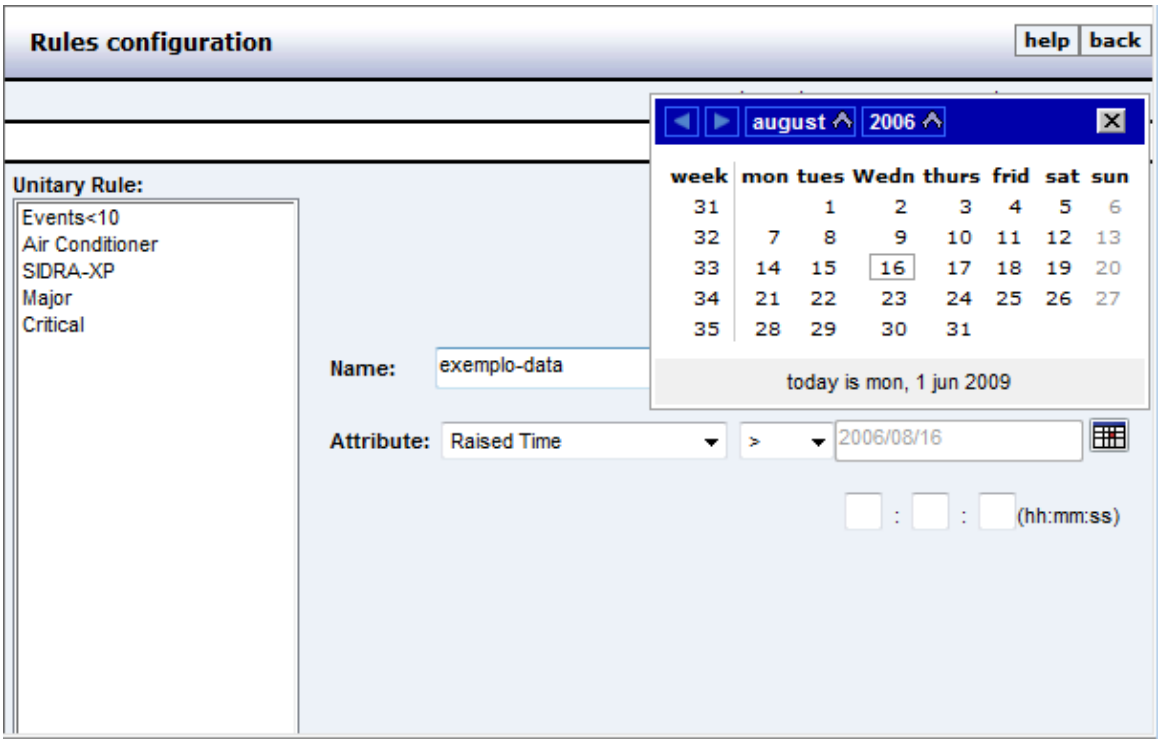
To create a sms action the procedure is identical.

Creation of a new Unitary Rule

Click on Unitary Rule to access the Unitary Rule window. For this example we will create 3 Unitary Rules that will cover different types of information: date (exemplo-Data), free field (exemplo-livre), and catalogue data (exemplo-select).

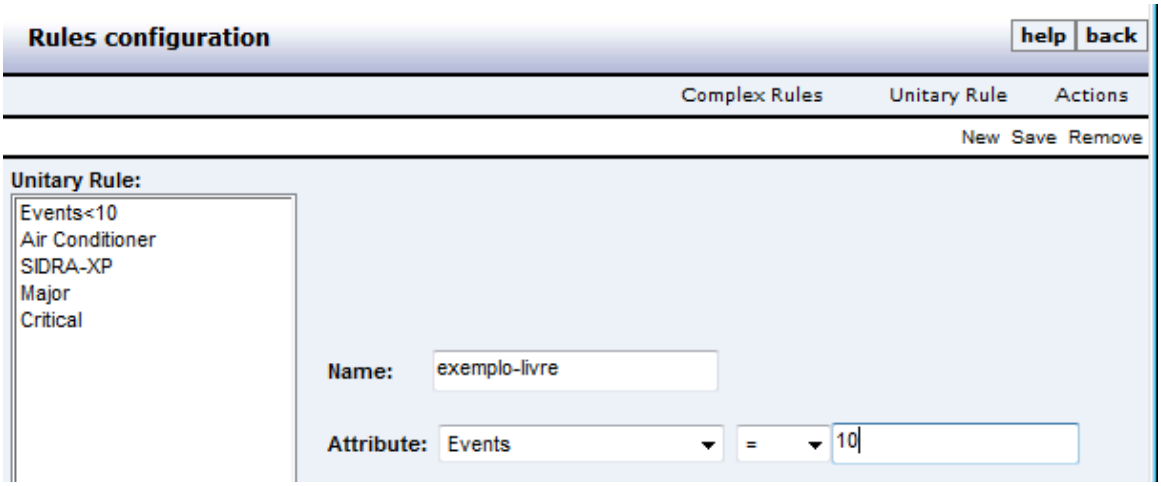
In exemplo-data, a Unitary Rule will be created to return true when the compared alarm has a Raised Time higher than 16/08/2006 00:00:00. To do this, after the creation of a new rule, select 'Cleared Time', the operator >, and the date by clicking on the calendar icon at right of the textbox. A small window will open, with the calendar of the current month. There, you can select the desired date. Click Save to finish.

Figure 192. Exemplo-Data



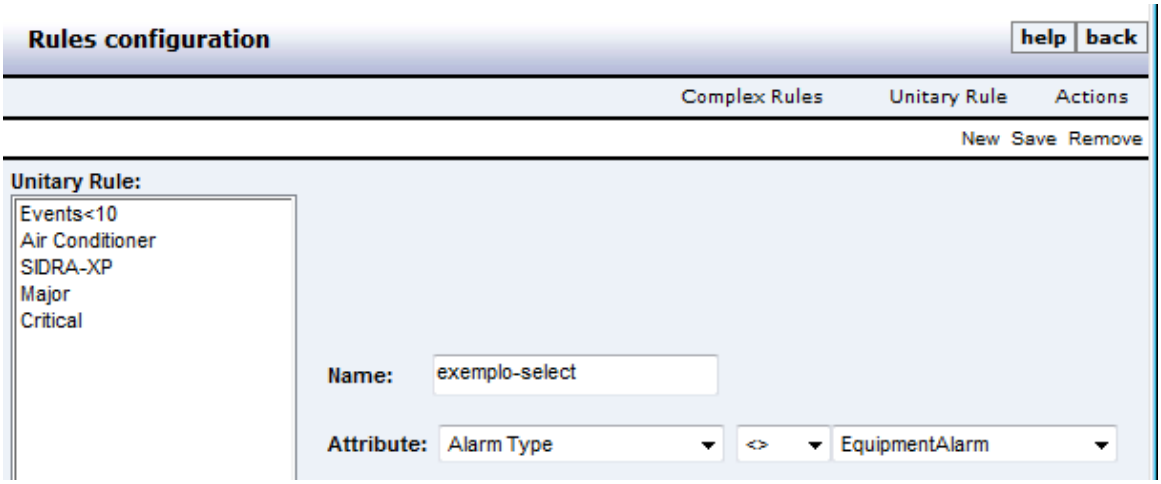
Exemplo-livre is created (after generating a new Unitary Rule), by choosing the attribute Events, the operator =, the value 10, and saving. This rule returns true when the number of alarm events are equal to 10. When the typed field is a set of characters, there are three special operators for text, which are CT (Contains Text), CTI (Contains Text Initial) and CTF (Contains Text Final).

Figure 193. Exemplo-Livre



To create exemplo-select, click New, select the attribute Alarm Type, operator <>, and the value "Equipment Alarm". This will create a rule that will return true when the verified alarm is different from "Equipment Alarm".

Figure 194. Exemplo-select

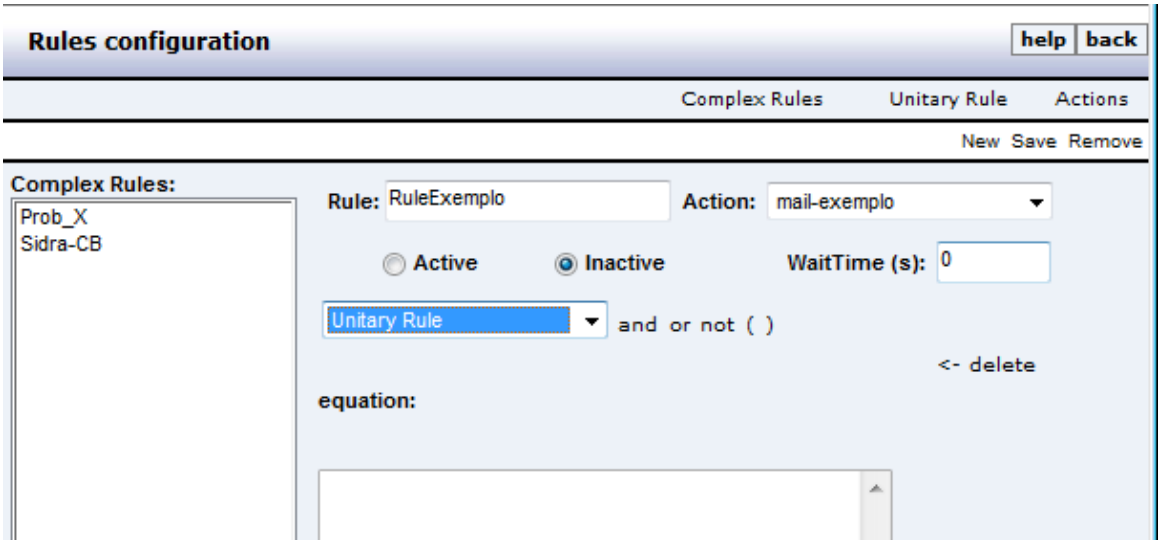


Creation of a new Complex Rule

Once the Unitary Rules and Action have been created, create a new Complex Rule. This Complex Rule shall be called RegraExemplo, it will be defined as inactive, associated to mail-exemplo Action, and with the following equation:

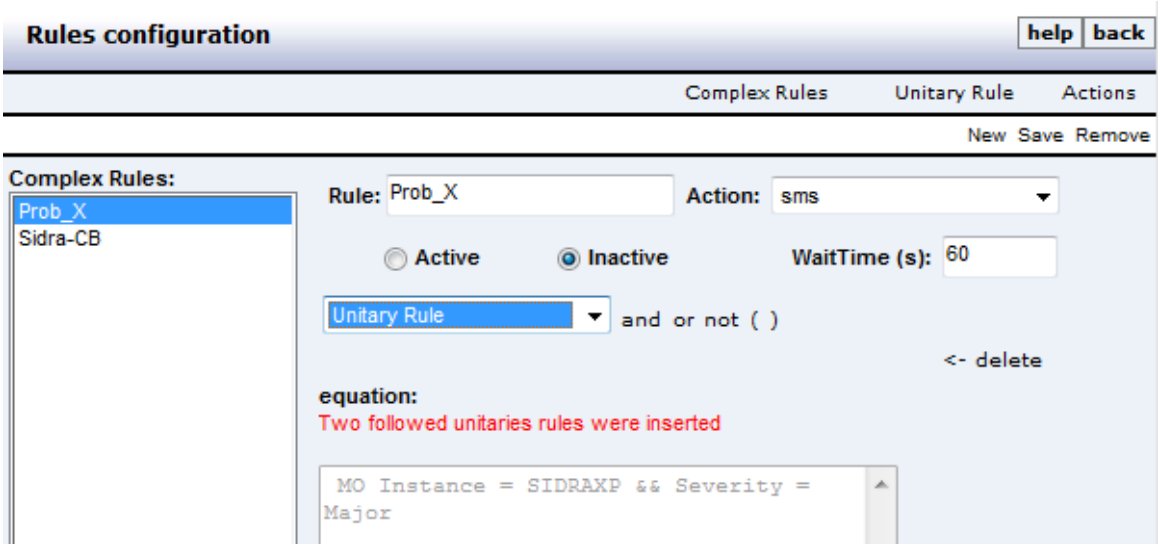
exemplo-Livre && !(exemplo-select || exemplo-Data)

Figure 195. Introduction of Unitary Rule



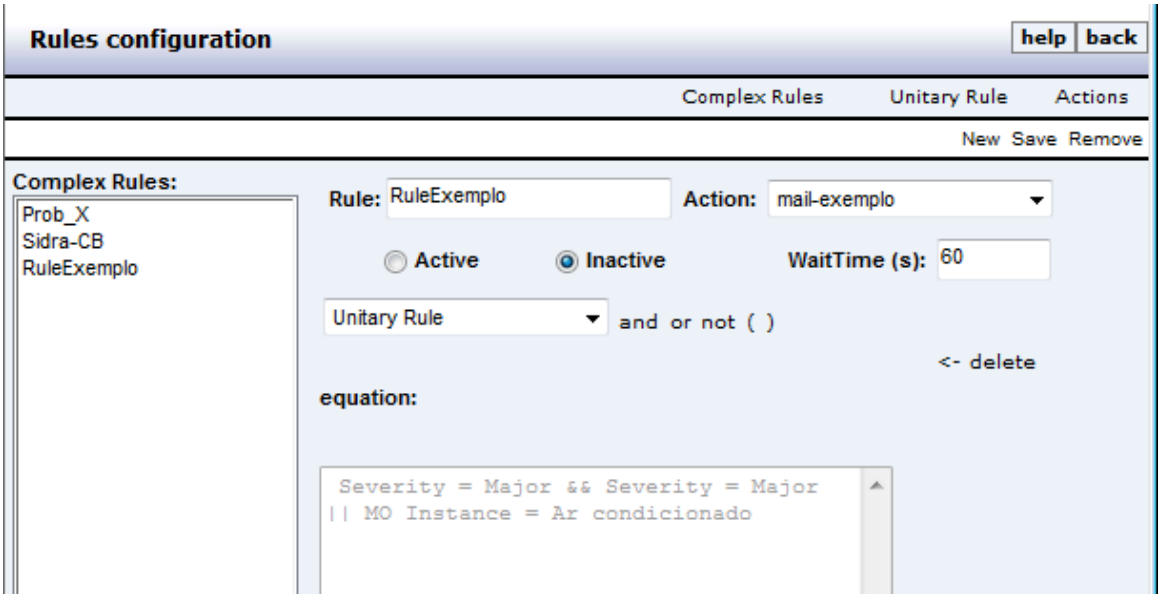
The equation is created in the same way it is written, i.e., select attribute exemplo-Livre, click on and, not and (. Select attribute exemplo-select, etc. and equation will appear in the equation field as long as it's being created. In case of mistake, click Erase to remove the typed field. Errors are shown in the Rules configuration table.

Figure 196. Display error when typing a rule



After typing the rule, click Save to create the rule. Click Active for system validation.

Figure 197. Complex Rule



Access Control System

Introduction

The Access Control System (SCA) is an independent system for the management of security and simultaneous access to a set of applications running on a same platform or portal. Its purpose is to centrally manage the users and their access rights profiles on one or several applications, as well as to provide methods to control the access to each one of these applications. These methods can be used to authenticate a user on a certain portal or on a certain application of that portal, and also verify the access rights on application internal checkpoints.

This Section is made for system administrators with the duty to manage the users' access to the applications available on the same platform, and that will gain access to the SCA administration Web interface. This interface, being the visible part of the SCA management system, is itself subject to access control, so access rules will have to be defined also for the administrators.

"SCA System" section will introduce to some of the basic concepts on which the access control policies of the SCA are based, its main features, the software modules implementing it and how they are used.

"User Interface" section describes in detail the user interface, sub-divided into the several available menu options, showing one by one the respective screenshots of the graphical interface and the way to use it.

Further sections contain useful information for the set-up of the SCA system itself, namely the list of its subsystems and intermediate points, the basic user profiles needed for the system's operation, and the presentation of the first user of the system, the "builder", with his special privileges on some options that will be inhibited to the SCA operational users.

SCA System

General Concepts

On the SCA, the access control is based on a set of base entities that have to be configured and managed, considering the access requirements and characteristics of each management system. These entities will be defined hereafter.

Application

Same as management system or system (like Customer Care, NGIN Manager, Altaia, CadRede, etc.).

Management System

Target application for which centralized access control policy is required.

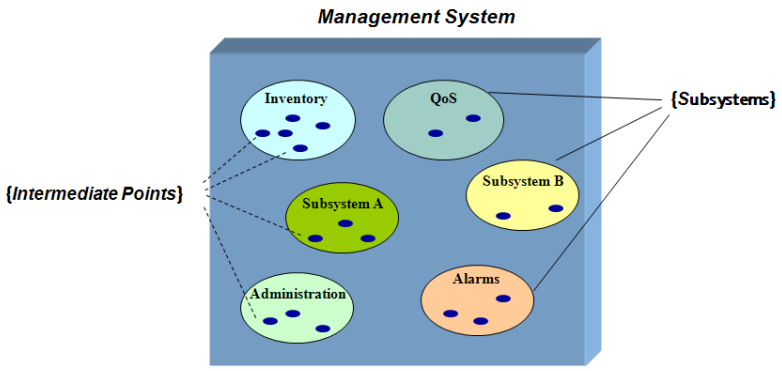
Subsystem

Functional component of a system, able to operate autonomously, but linked to other subsystems in a management system. Same as module.

Intermediate Points

Intermediate access checkpoint within a subsystem where access privileges must be verified before proceeding. At this point, the privileges assigned to the user for this particular subsystem are compared to the minimum privilege level defined for the checkpoint. Access will be denied to the user if he/she has not equal or major access rights.

Figure 198. Management systems, subsystems and intermediate check points



Access Type

Access privilege granted to a user on a given subsystem (by attribution on a profile), or, when referring to an intermediate access check point, the minimal level of privilege needed for the user to gain access to that point. For example: View, Operation, Configuration, Management, or simply 1, 2, 3, n. There should be a natural hierarchical order of the access privilege levels, for example the "View" type is included in the "Operation" type, "Operation" is included in "Configuration", which is itself included in "Management". This order relation is determined by an associated numerical code.

Managed Domain

Partition or view of a set of managed entities. This partition can be related by geographical, technological or other affinity. It can be any attribute of an application that determines the partition of the managed universe, in order to organize the user access control on this application.

Management Center

Organizational entity responsible for the management of part of the managed network. It can be a department, a supervision center or any sub-division of the telecommunications operator's organizational hierarchy.

Each user of the system is member of only one management center.

A management center can be in charge of several managed domains, and also several management centers can share a managed domain.

Possibilities Matrix

Matrix mapping management centers to managed domains. Restricts the universe of managed domains that can be assigned to a user that is member of a certain management center.

Profile

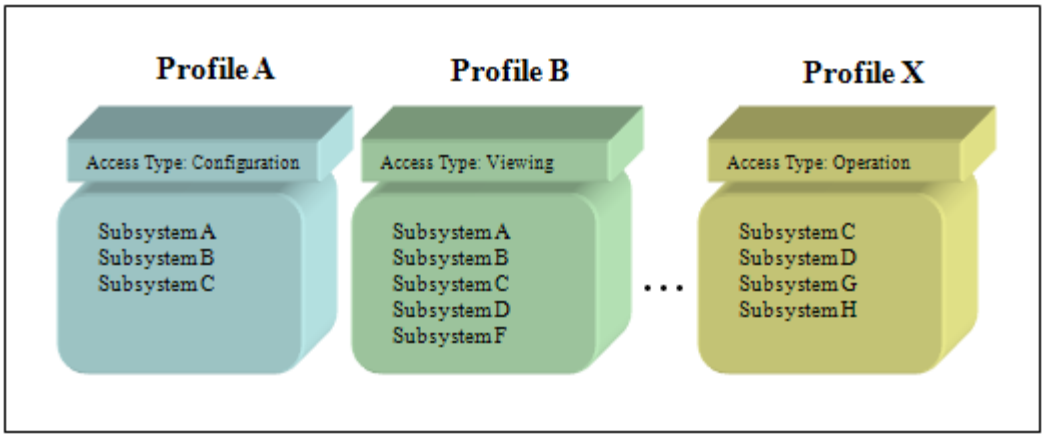
Bundling of one or more management Subsystems that can be accessed by one access type.

The same profile can be assigned to several users.

The definition of profiles independently from users sees its advantage in the reusability of access rights combinations, and therefore simplification of user configuration on a management system. For example, a set of basic profiles can be defined ahead on the SCA, and then assigned to the users as they are being created. For example, if ten users have the same access rights on the same subsystems, so only one single profile is defined and assigned to all of the ten users. A user can have several profiles if the diversity of his roles on the system requires it. On attributing a profile to a user, and depending on his management center, the managed domains to which the user can have access are extracted from the matrix of possibilities, to be able to select those to whom, in this profile, he will access.

A subsystem can be included in more than one profile, with the same or different access types.

Figure 199. Profiles of a management system



Security Domain

Security domain, or network domain, is a new concept of SCA V3 which arises on the need for the SCA user's repository can be supplemented with some kind of information of other security domains native users, for the purpose of Single Sign On functionality. In view of the SCA, a security domain identifies a network server where is located the repository of users that are authorized to have access to physical or logical resources belonging to a specific network whose scope can be extended to an organization, a company, a geographical area, etc.

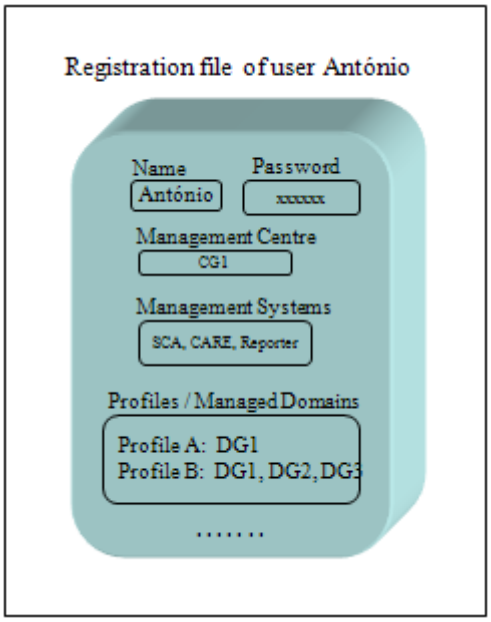
In the context of this manual, the network domain identification by the name of the external repository and, in particular, of LDAP repository will be frequent, since it is this technology that supports user authentication of such domains.

User

User with credentials to access to one or more management systems. The user register on the SCA includes:

- Username
- Password
- Management center
- Preferred working language
- Security domain
- Authorized management system(s)
- List of profiles defining to which subsystems the user can access, the respective access type and the list of authorized managed domains
- Set of optional attributes as: maximum number of login attempts and of simultaneous sessions, maximum session and idle time, personal information

Figure 200. Information associated to a user register



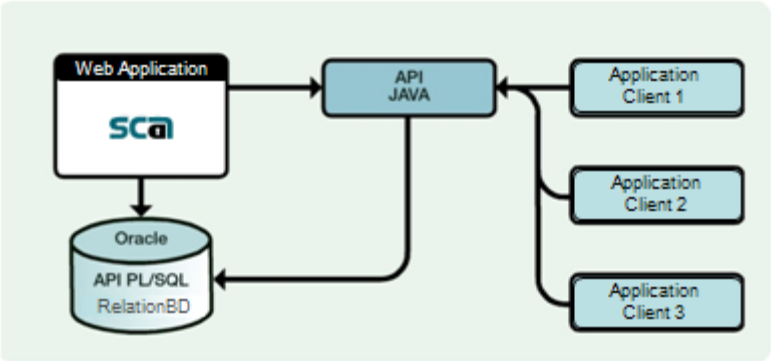
Functional View

The SCA is divided into two main functional components:

- The graphical interface for the management of users, profiles, applications, managed domains and other information. It is based on Web technology and is available via Internet/Intranet, using an application server (e.g. Tomcat, Weblogic, etc..)
- The functional API called in real time by the applications for the authentication of their users and validation of their respective privileges. This API is available in Java and PL/SQL and is linked with the applications needing to query the SCA database for access control

Next figure illustrates these two features of the SCA.

Figure 201. Functional components of the SCA



Through its administration interface, the SCA provides functions to:

- Configure the managed applications (management systems), its modules (subsystems) and function points (intermediate points)
- Configure the organizational hierarchies (management or supervision centers) to which the users of the application belong
- Configure managed domains according to different aspects, thus allowing a natural division of the managed universe and the possibility to restrict the user's view on the objects of that same universe
- Map managed domains to management and supervision centers, by means of a possibilities matrix, allowing to define restricted views over the managed universe
- Configure users for any application or management domain
- Configure management domain (external users repository)
- Integrate users of external repositories, to allow single sign on on the applications from the authentication in these areas
- Configure basic profiles of features that are attached to one or more users
- Relate users with managed objects (e.g. managed domains), functions of the applications (e.g. profiles) and allowed operation types
- Obtain users and profiles reports, according to various criteria
- View open sessions on all applications managed by the SCA
- Perform bulk operations of user creation, change or removal, by the processing of specifically formatted external files

Through its API, with the applications, the SCA provides functions to:

- Authenticate and authorize a user in an applications portal or in a given application
- Change the user's password
- Get the applications to which the user has permissions to access
- Get all functional points on which the user has execution rights
- Validate the permission to manipulate an object in accordance with the assigned managed domains
- Manage session logging information

Implementation

The main software elements included in the SCA are the following:

- **Web Server** – is divided in four software modules:

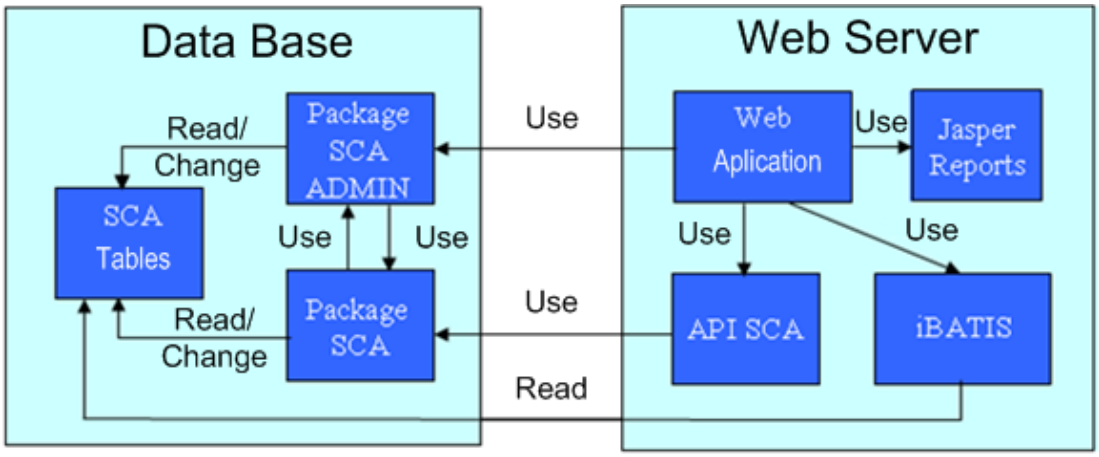
    - **WEB Application** – set of JSP pages and Java classes responsible for building and running the interface seen by the administrator on his browser
    - **JAVA API** – Java code implementing the access control on users and their respective rights within the applications
    - **iBatis** – persistence framework of data that allows interaction between the Web application and database (open source)
    - **Jasper Reports** –Reporting framework (open source)

- **Database** – contains the SCA data repository as well as PL/SQL packages used by the SCA API as well as by the Web Application:

    - **SCA Tables** – contains the configuration data inserted through the administration interface, i.e. about the applications, users, profiles, etc…
    - **SCA ADMIN Package** – set of PL/SQL procedures used by the Web Application
    - **SCA Package** – set of PL/SQL procedures used by the access control API

The following figure illustrates the described elements.

Figure 202. SCA's software elements



Multilingual Interface

With this feature, the SCA provides a multilingual user interface that can be used whenever and wherever justified by a universe of international users. The default interaction language is set automatically according to the user's preferences, but can also be switched manually.

The language to use is chosen as follows:

- On the first call of the SCA or another application managed with the SCA after its installation on a platform, the interface language will be the one configured by default for the web browser
- On the login screen, the choice of one of the available country flags will temporarily switch to the respective language dictionary
- After user authentication, the interface language will automatically switch to the one defined by default for this particular user on his SCA register file
- Each successful authentication will update a cookie on the client computer, referring to the preferred language of the last access to the application. This will be the used language by default on the next access to the SCA application

The access to any other application managed by the SCA will work in the same way, as the user preferred language is one of the attributes made available right after a successful login.

Single Sign On

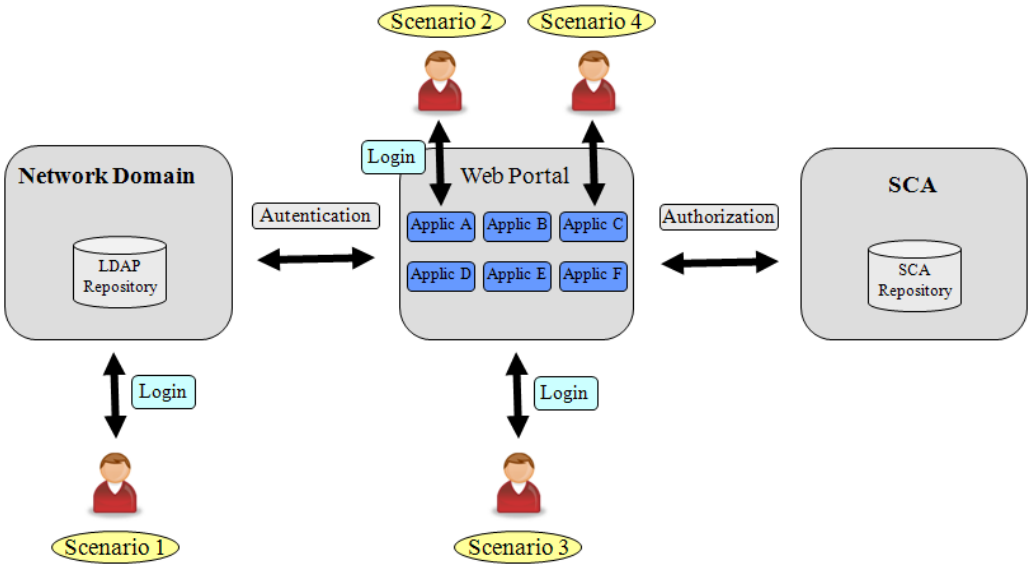
The use of the term single sign on allows a user to log just once time and it allows having access to multiple systems through this certification. This feature can be very useful in systems, which although they are independent, are interconnected and coexist in a single environment.

This concept is strengthened in the SCA by the possibility of linking this one to LDAP external domains or Active Directory. Thus, a user can be authenticated in a network domain and later be allowed in a given application without the repetition of the authentication process.

In this context, the SCA allows various scenarios:

- Scenario 1:
  - To access to an application with the credentials of the currently logged user in the network domain
- Scenario 2:
  - To access to an application with the credentials of the currently logged user in the network domain, but allowing log with another user
- Scenario 3:
  - To Access to an application without prior credentials
- Scenario 4:
  - To Access to an application within a portal session

Figure 203. Integration scenarios of the SCA with LDAP repositories



Apart from the chapters of this manual where certain actions of administrations about this feature are detailed, we recommend to consult the LDAP Administration Manual (SCA_MNMA_AdministraçãoLDAP), especially to those who must set the installation environment of the SCA which is integrated with LDAP domains.

User Interface

In this chapter, you will find the description of graphic options that SCA user can use and how to act in each of them.

Login page

After calling the SCA administration application with a web browser, the user will see the login page where he will be asked to enter is access rights: username and password.

Figure 204. Login page

By making use of the multilingual facilities that the SCA offers, the language displayed in this window can be determined by:

- Language set-up in the browser. This set-up will be used only in the initial stage of any application after the installation of the platform
- Choosing one of the flags displayed in the login screen, which identify the available languages
- The language selected by the last user

In this window, two other functions are available: advice about a forgotten password and changing the password. In the case of a forgotten password, the user's username and his e-mail address will be required by the system in order to send a new randomly generated password. For security reasons, the e-mail address will have to match the one previously configured in the user's records, identified by the username.

When integrated into a portal, the SCA and all its applications will not use this login window, since what is claimed is the existence of a single login point, i.e. the so-called single sign on page. Thus, the information given in the portal login window will be used to access any other application during the same session.

When integrated with LDAP domains, the SCA and all other available applications, including access portals, which delegates to the SCA the access control, will not use the login window, if the current user authenticated by the current network domain has privileges to access to applications and/or portals.

Immediately after the installation of the SCA, there exists a "Builder" user and an "admin" user both of which are pre-configured in the database. The "Builder" user is the super user with unlimited access to all functions. This should not be used in operational environment. The 'admin' is a user with access to most of the resources, but who is not allowed to manage information related to the options that are to be found in the Installation menu.

Application page

Once inside the application, its main background frame will always look the same and will consist of the following:

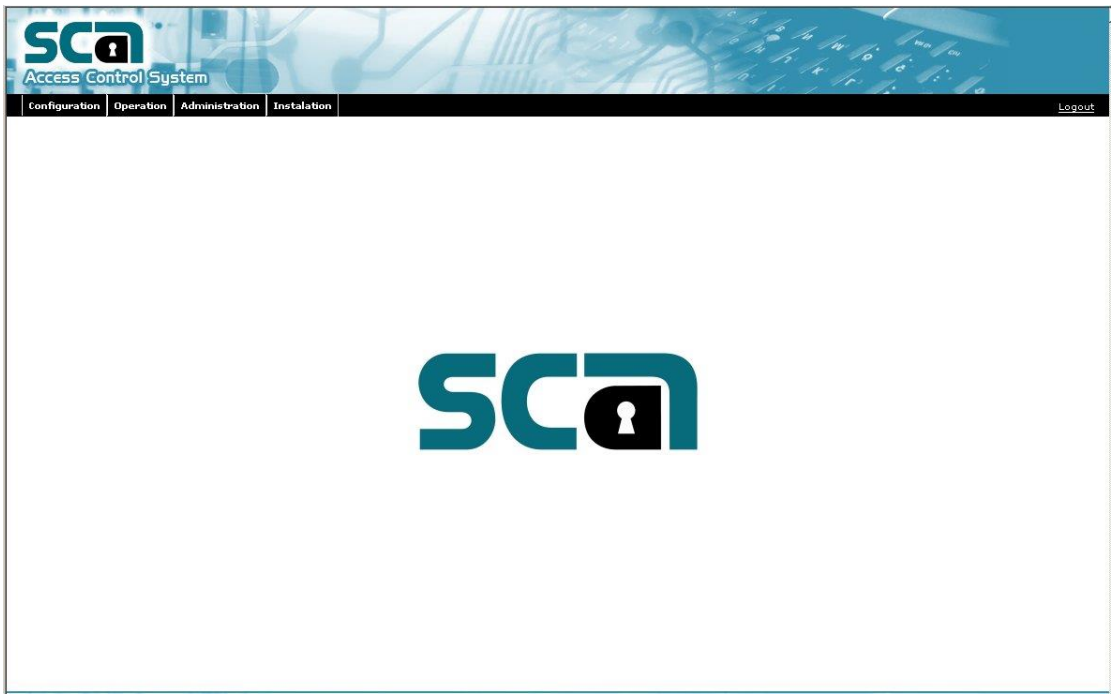
Application identification bar – this contains the name of the SCA application.

Menu bar – this contains the menus with options that the user can access. Depending on user rights, there may be fewer or more menus and options.

Working area – this is the area where SCA data can be consulted or manipulated.

Status bar – this shows, the current user and date/time, the number of logins already made in the application and the date/time of the last visit. On the right, the current SCA version is displayed.

Figure 205. Initial page of the application



Menus

The SCA menu bar shows four main groups of menus:

- Configuration
- Operation
- Administration
- Installation

The Configuration menu includes the options:

- Users
- Profiles

- Bulk Operations

This is a menu that allows frequent access and, for example, to set up new users and profiles, as well as for related basic actions (edit, delete, associate, etc.). The option 'Bulk operations' allows carrying out massive set-up of users by using data base files.

The menu Operation includes the options:

- Logs
- Reports
- Sessions

This menu allows you to see the logs of actions completed in the SCA as well as to consult various types of reports and even to consult all the sessions that are active in all applications controlled by the SCA.

The Administration menu includes the options:

- Management Centers
- Possibility Matrix
- Global Settings
- Job/Functions
- Security Domains

This consists of typical actions which are of an administrative nature, i.e. the defining of management centers, the management of the possible connections between the management centers and the managed domains, the settings which are applicable globally or to a particular management center, and the functions or roles which are applicable to the users and also the set-up of the external security domains. These are rare types of actions, although they are quite normal in operation.

The Installation menu includes the options:

- Management Systems
- Managed Domains
- Access Types
- Languages

It can be noticed that these are factory-installed configurations that cannot be altered without the applications run by the SCA being changed too. In other words, the management systems, subsystems and respective intermediate points are exactly those which are included in a version; the subsystems are those that the systems are designed to manage; the types of access are those that are assigned to the intermediary points of the installed configuration; finally, the languages are those where translations already exist in the systems. In essence, all the alterations to this type of entity automatically require the substitution of the executable software modules of at least one of the running applications.

Configuration Menu

This menu consists of the Users and Profile options, which are described below.

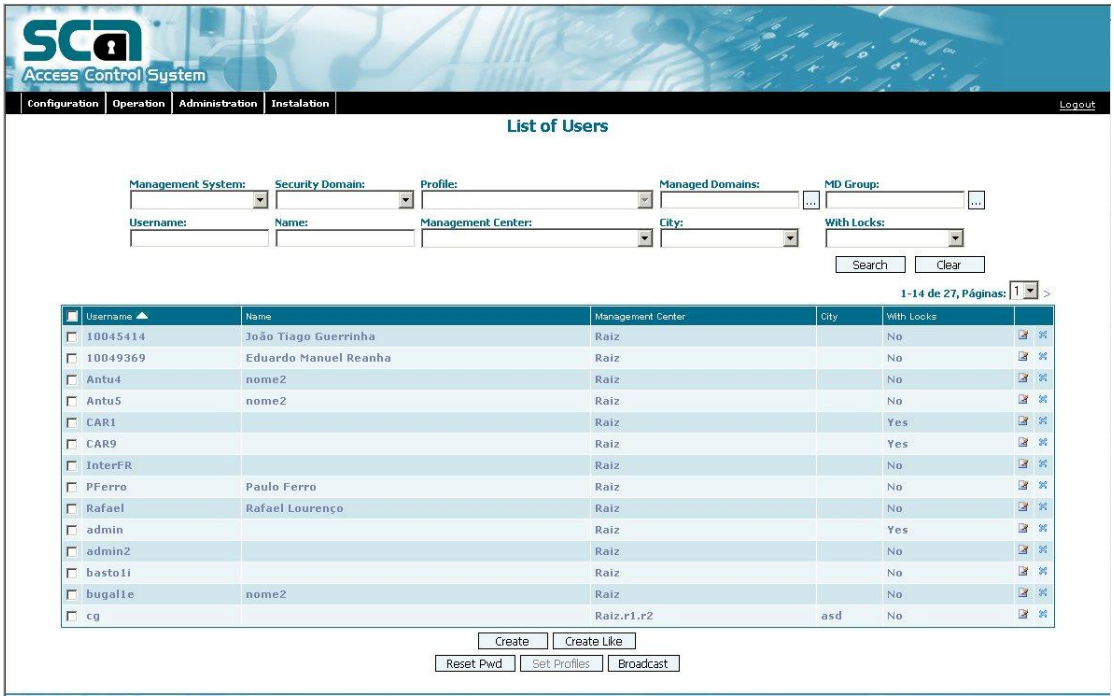
Users

Choosing the option Users allows access to the page where are listed all the users registered in the SCA system or just the users that match certain criteria. Besides the username, name, management center and place, you are also informed if the user has been locked for some reason.

The available criteria for filtering or searching for users are: management system, profile, managed domain, managed domains group, security domain and all the attributes shown in the list. The username, name, management center and place accept any sequence of characters as search criteria. The filter 'With Locks' allows filtering of both locked and unlocked users.

The search button is used to activate all the filters that have been selected and the clear button can erase all the currently applied filters.

Figure 206. List of registered users



The filling of available filters will help you narrow your search results. Below, we present some examples based on the filling of filters:

- A profile and a domain – you wish to filter users who have an assigned domain in a specific profile
- A profile, a domain and a group - you wish to filter users who have assigned domain and group in the chosen profile
- A domain and a group - you wish to filter users who have an assigned domain and a group, regardless of their profile

By pressing the header of each column, the current listing order can be set or changed. The symbol beside the title serves to indicate this ordering parameter.

The list is presented as pages, showing 14 users per page. You can have access to a specific page, selected from the list box located in the upper corner of the list, under the Reset button, and you can go forwards or backwards within the result pages.

At the foot of the list you can find two sets of icons. Those in the first line allow access to the functions that affect one single user. Those in the second line permit access to group functions that are applicable to all currently filtered users.

Below is a description of the possible functions to apply to one or more users:

Create – create a new user.

Create Like – create a user similar to the one previously selected, including the same parameters and access profiles; you just need to introduce the username and password fields.

Modify – modify the information associated to a user.

Remove – remove a user.

Details – allows consultation of all the information about a user. For that you must click the left button of the mouse on top of any field of the required user register.

Reset Password – allows attribution of the default password to a group of users who are currently filtered or the one that has been selected.

Assign Profiles – allows you to assign profiles, domains, and group domains to a previously selected group of users.

Broadcast – allows you to send messages to a previously selected group of users.

The checkbox, on the left of each user register, allows the selection of one or more users for the implementation of group functions, if what is pretended is not to apply them to a universe of users routinely filtered, but to apply them to a more limited universe.

Create / Create as / Modify User

These three actions allow access to a page made up of four panels, each one containing a different type of information about the user:

User attributes – this shows the set of attributes that identify and characterize the user.

Management Systems – this shows the list of management systems that the user is allowed to use.

Profiles – this shows the list of profiles assigned to the user.

Locks – this shows the type of locks associated with the user.

Each panel has its own validation and cancellation icons, so that you can validate the information that has been inserted or altered in one panel and cancel the alterations carried out in another one.

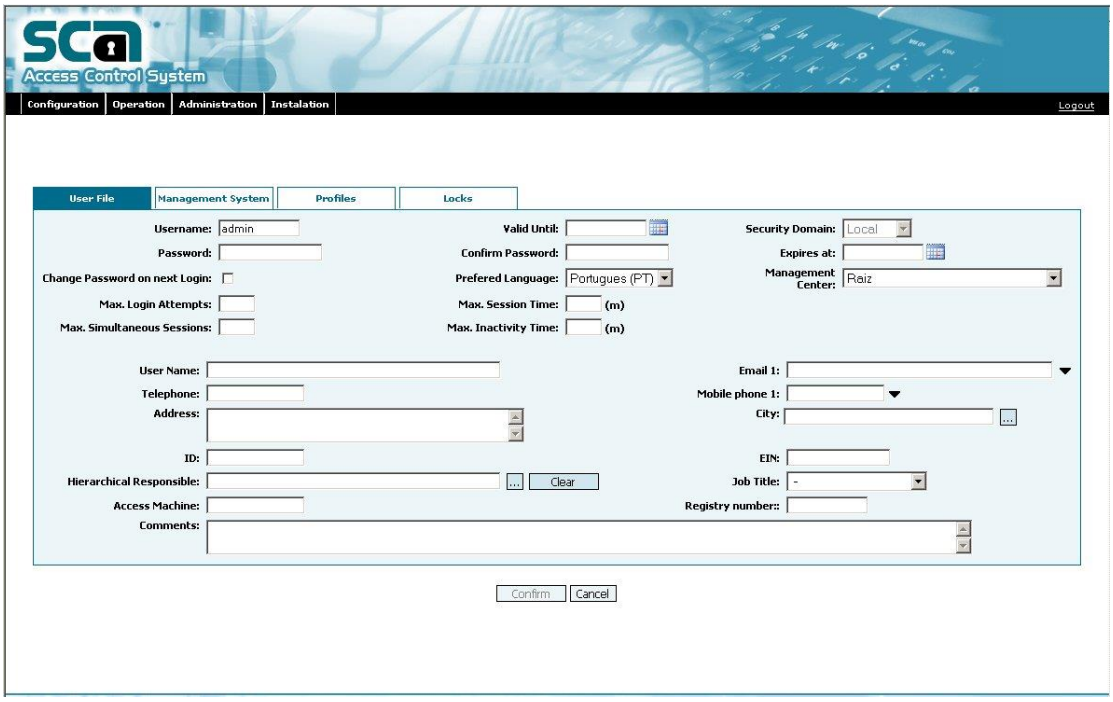
When (or Create Like) a user is created, the only panel that is necessary to fill in is the first, containing the identification and basic characteristics. Until this panel is validated the others remain unavailable, that is, any attempt to change panels by clicking on its tab has no effect.

When a user is modified all the panels are active and the user can navigate between them in any order.

User Attributes

This panel shows the set of attributes that identify and characterize the user. Those that are obligatory are: username, password, preferred language, and management center. There might be obligatory fields in specific installations, like, for example Identity Card number or tax ID number.

Figure 207. User attributes



The Confirm and Cancel icons confirm or cancel respectively the alterations made, but it's only the Exit icon that allows you to return to the previous page. The fields 'Valid until' and 'Expires on' are subject to a calendar for their completion, and to an icon 'Clear' when you wish to them to remain blank.

If the user is locked due to an expired username or password, the respective validity fields can no longer be subject to alteration. Any type of locking has to be removed in the Locking panel ("Locks" section). By default, the 'local' security domain is awarded to native users of the SCA.

Import of external domain user:

This action allows creating a user which has a security domain attribute that is different than 'local'. When you import a user of an external domain, you must just select that security domain in the respective field of the user attributes form. Immediately, LDAP connection is made to that domain which will show, with the data that is found in the original repository, all attributes that are predefined in the configuration of that security domain ("Create/Modify Security Domain" section). The imported attributes are not editable in the SCA. The password of the users is never imported, so the respective fields will be blank. If the import cannot be made for any reason, an informative message will be showed.

Description of the user attributes:

Table 49. User attributes

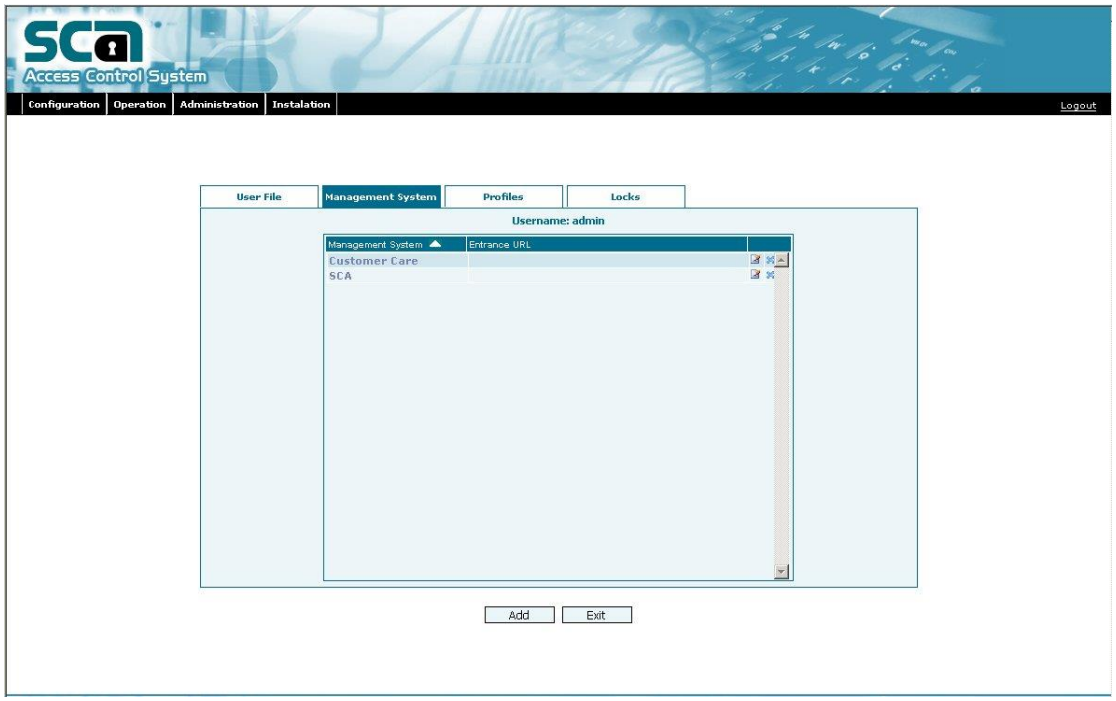
Field	M/O	Description
Username	M	Name of the login assigned to the user
Valid until	O	Validity date of the user
Security domain	M	Security domain where the user belongs. It is automatically filled with the 'local' domain, which identifies the native users of the SCA.
Password	M	Confidential access code
Confirm Password	M	Repetition of the confidential access code
Expires on	O	Password expiry date
Change Password on next login	O	Necessity of altering password on the first login. By default when a new user is created this field remains active and displays the validity of the password for 60 days, allowing you to deactivate as well as delete or assign a new validity to the password.
Preferred Language	M	The language that the user wishes to use in the applications
Management Center	M	Management center that the user belongs to. By default the management center will be the one the current SCA user belongs to. If this is the terminal in the MC tree, it is the only option. If not, it is possible to choose another center lower down in the hierarchy or at the same level as yours. However, if the SCA user is the "Builder" user or if he has been granted a special intermediate point that allows creating users in any management center, then he will be able to do that.
Maximum number of login attempts	O	Maximum number of failed attempts for the login until the user is locked out
Maximum session time	O	Maximum time limit the user can spend in any application in one session

Maximum number of simultaneous sessions	O	Maximum number of simultaneous sessions with the same login in any application
Maximum idle time	O	Maximum amount of time in which a session may be inactive, after which it will be closed automatically.
User name	O	Name of the user
E-mail	O	E-mail address of the user. Up to 3 e-mail addresses may be included, using the button on the right of the field from one to another.
Telephone	O	Telephone contact of the user.
Mobile Phone	O	Mobile phone contact of the user. Up to 3 mobile phone contacts, using the button on the right of the field, from one to another.
Address	O	Work address
City	O	Town/city where user works
ID Card Number	O	Identity Card number
Tax ID Number	O	User's Tax number
Hierarchical Superior	O	Username and name of the user's Superior in the company hierarchy. This is completed by selecting one of the usernames that has already been configured. The list of users can be duly accessed with button '...'
Job title	O	Job/Function of the user
Access Terminal	O	Usual terminal to access to the application
Employee Number	O	User's registration number in the company
Comments	O	Any additional observations

Management Systems

This panel displays the list of management systems already assigned to the user. It consists of the name of the system and preferred entry point for this user in the respective system.

Figure 208. List of the management systems assigned to the user



Four buttons allow access to the possible actions:

Add – this adds a management system to the user's list of authorized system that is being created (or modified)

Modify – this changes the preferred entry point in an authorized management system

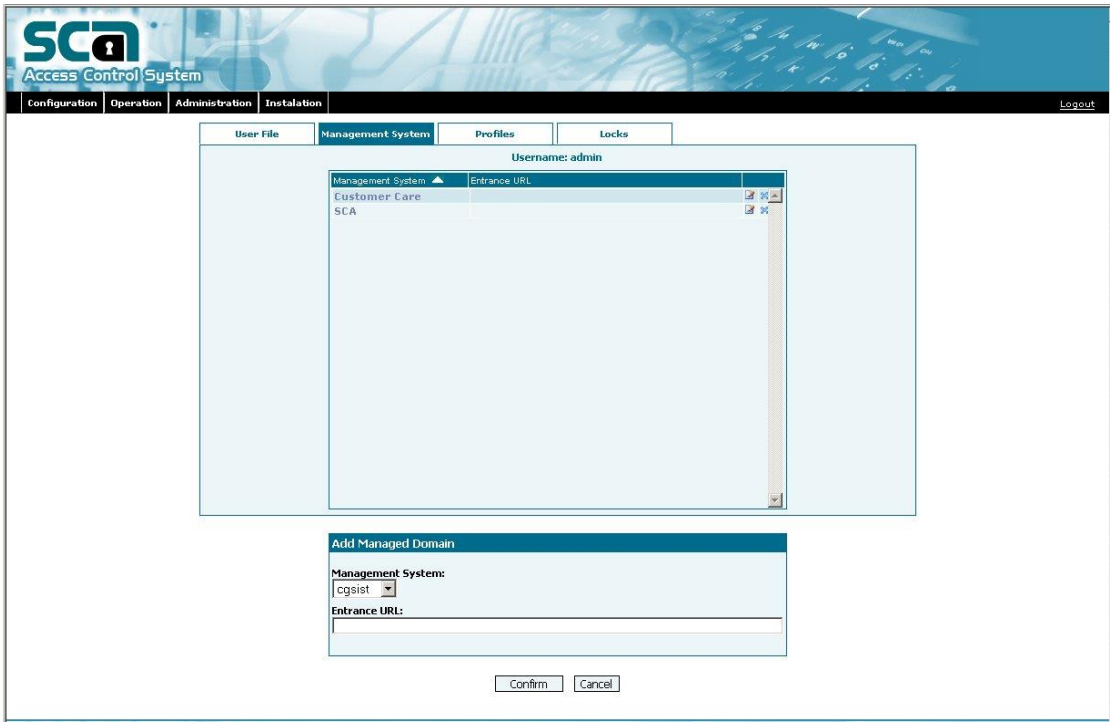
Remove – this allows you to take out a management system from the current user's list of authorized systems

Exit – this returns you to the list of registered users

Add / Modify User's Management System

These two actions open up a new page that extends the previous list of management systems with area where you can add a new system and the respective URL (preferred entry point). If the chosen command is Modify you can only alter the URL. The available management systems are the ones that have previously been registered in the SCA.

Figure 209. Add or modify association of a management system with a user



Remove User's Management System

This action removes a management system from the list of user's authorized systems. Simply press the remove button on the right of the wanted management system and confirm the request in the confirmation box that appears in the window.

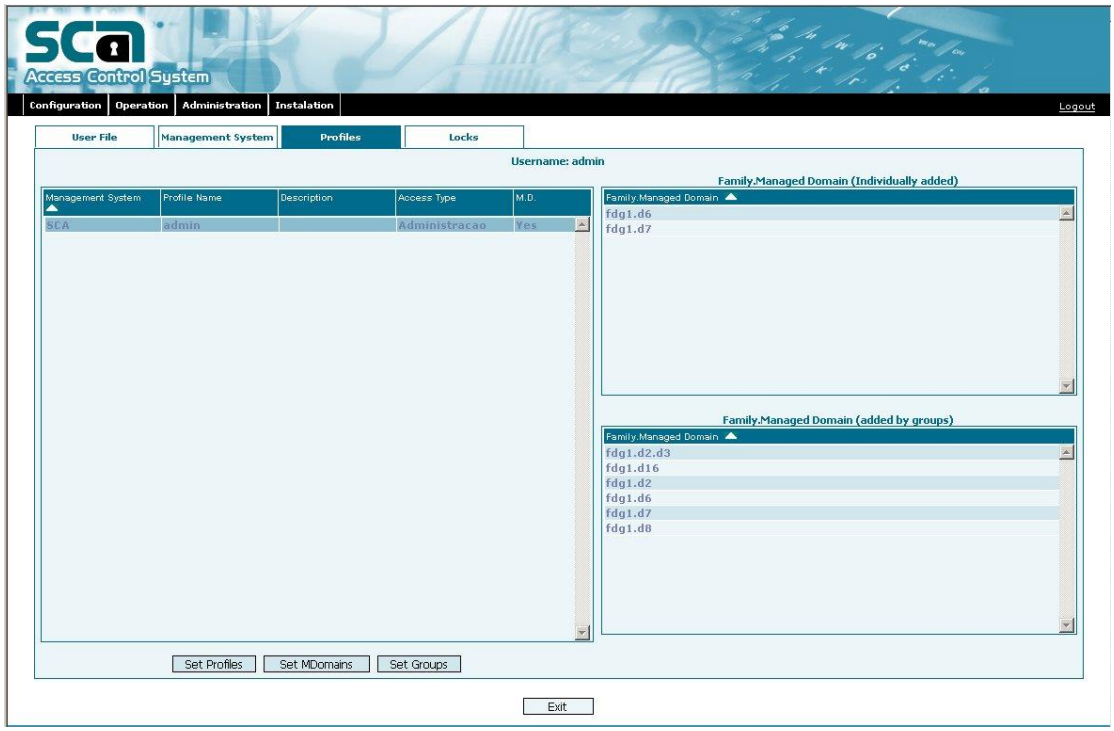
This action will take out all profiles previously assigned to the user on this management system.

Profiles

This panel displays the list of profiles already assigned to the user. It includes the name of the management system, name and description of the profile, access type and an indication of whether the profile requires the attribution of managed domains.

When you select a profile which requires assigned managed domains, you will see on the right a list of managed domains assigned to the user in this profile, differentiating those domains assigned individually and those assigned by means of groups' assignment (see the definition of managed domains groups in "MD Groups" section). There may be repeated information in the two sub-lists.

Figure 210. List of the user's profiles



Four buttons are used to perform the following commands:

Assign Profiles – this adds or removes user profiles

Assign MDs – this adds or removes managed domains from the user profile

Assign Groups – this adds or removes managed domains groups from the user profile

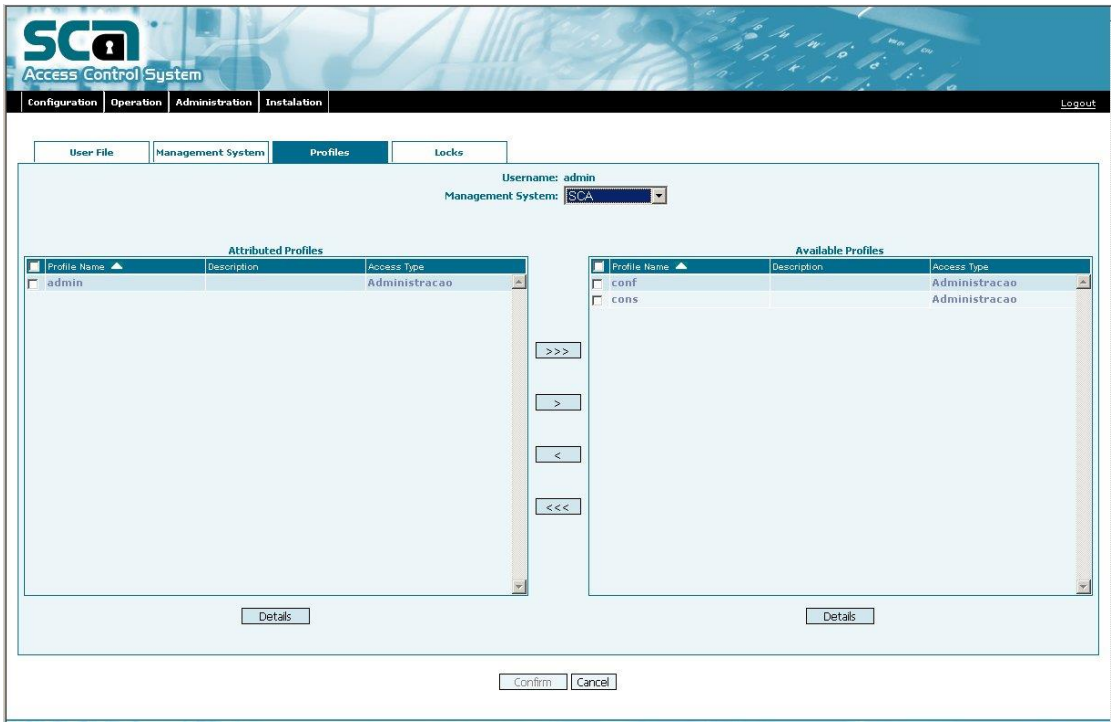
Exit – this returns you to the list of current users

The Assign MDs and Assign Group commands require the previous selection of a profile.

Assign Profiles to a User

This action opens a new page where, after selecting a management system from those assigned to the user, there appear two lists of profiles: on the left is a list of profiles already assigned to the user and on the right those profiles which are available and not yet assigned.

Figure 211. Assign profiles to a user



The possible actions are:

'>' or '<' – this transfers the selected profiles from one list to the other

'>>>' and '<<<' – this transfers all profiles from one list to the other

Details – this shows the composition of a selected profile in terms of subsystems and intermediate points

Confirm – This validates the changes carried out between the two lists, and returns to the page containing the list of user profiles

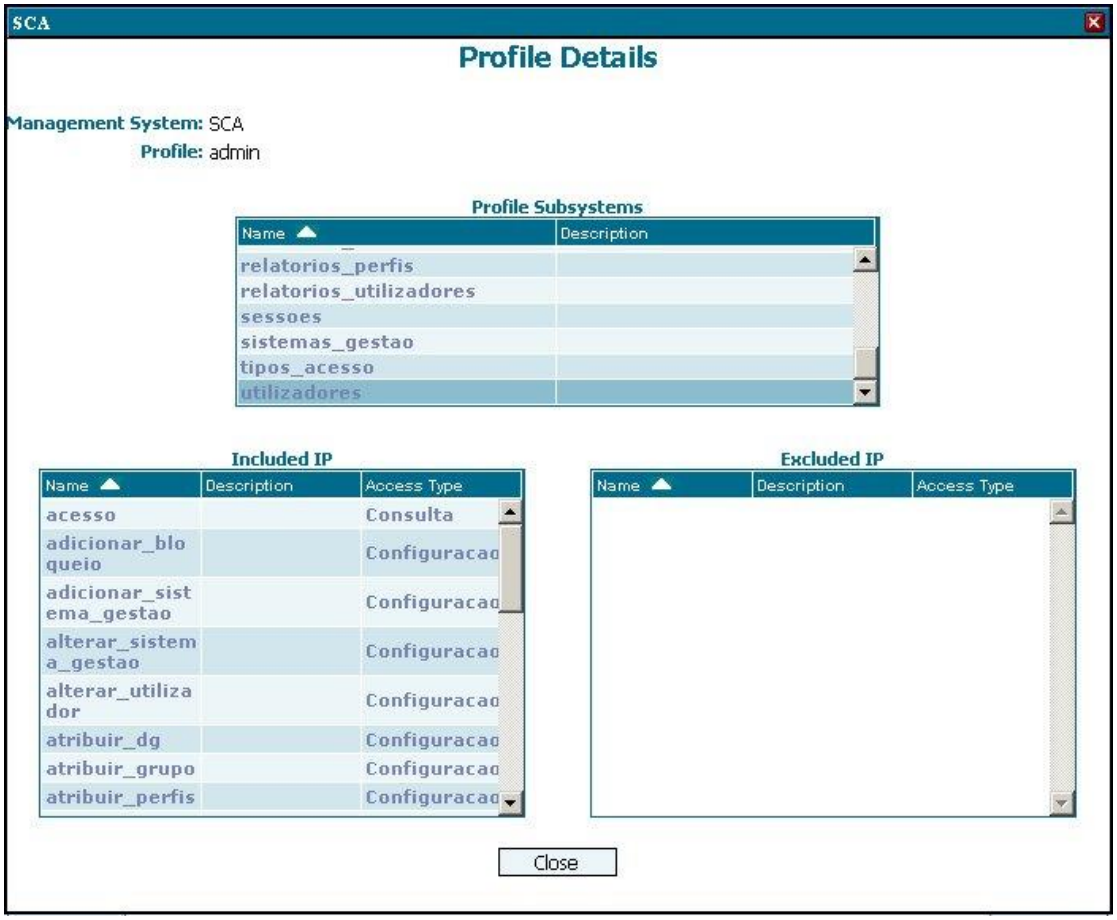
Cancel – this cancels the changes carried out between the two lists, and returns to the page containing the list of user profiles

To select the profiles which you want transfer from one list to another one, you must use the check boxes which are attached to each profile or a check box, on the line of the title, which allows you to select all the profiles of the list.

View Profile Details

For a given selected profile, this action opens a new page where three tables appear: the first contains profile subsystems and the other two, for each selected subsystem, the list of the included and excluded intermediate points, respectively.

Figure 212. View profile details

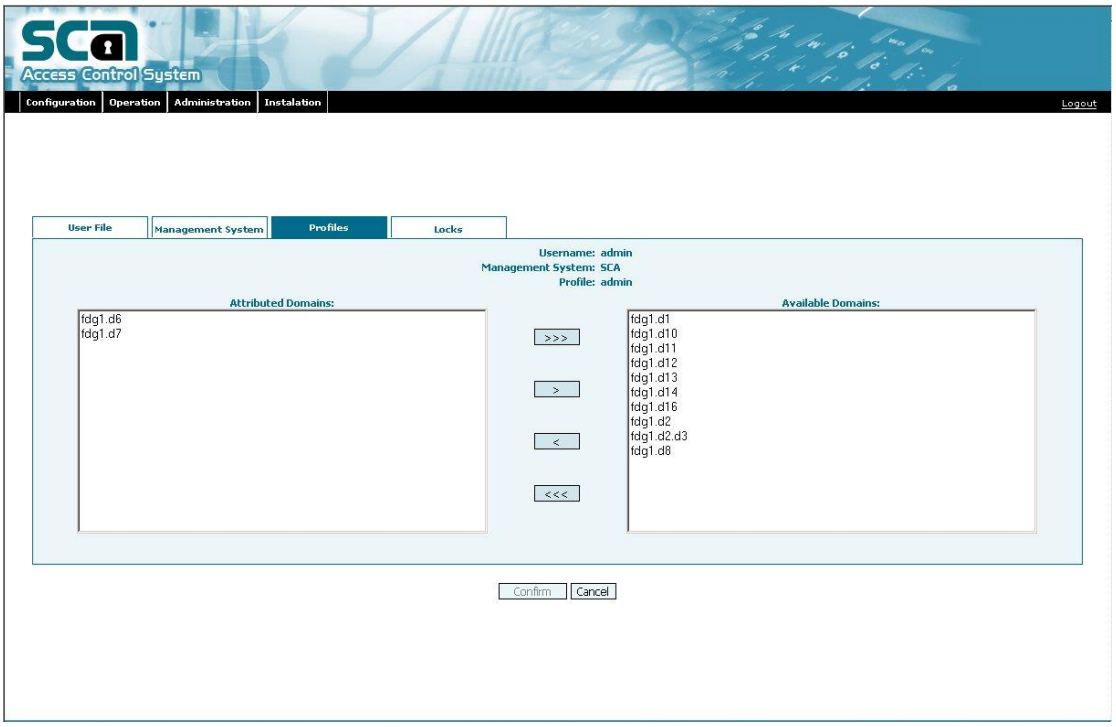


Assign Managed Domains to the User Profile

For any given selected profile this action opens a new page containing two lists of managed domains: on the left are the domains already assigned to the user and on the right those which are available.

N.B. The managed domains that are available are those that have been set up in the possibilities matrix for the management center to which the user belongs ("Possibilities Matrix" section). If the list of available domains has not been previously configured in the possibilities matrix, it will appear blank.

Figure 213. Assign managed domains to a user profile



The possible commands are:

'>' or '<' – this transfers the selected domains from one list to the other; to select multiple items you can use the keys SHIFT + mouse click and CTRL + mouse click

'>>>' and '<<<' – this transfers all the domains from one list to the other

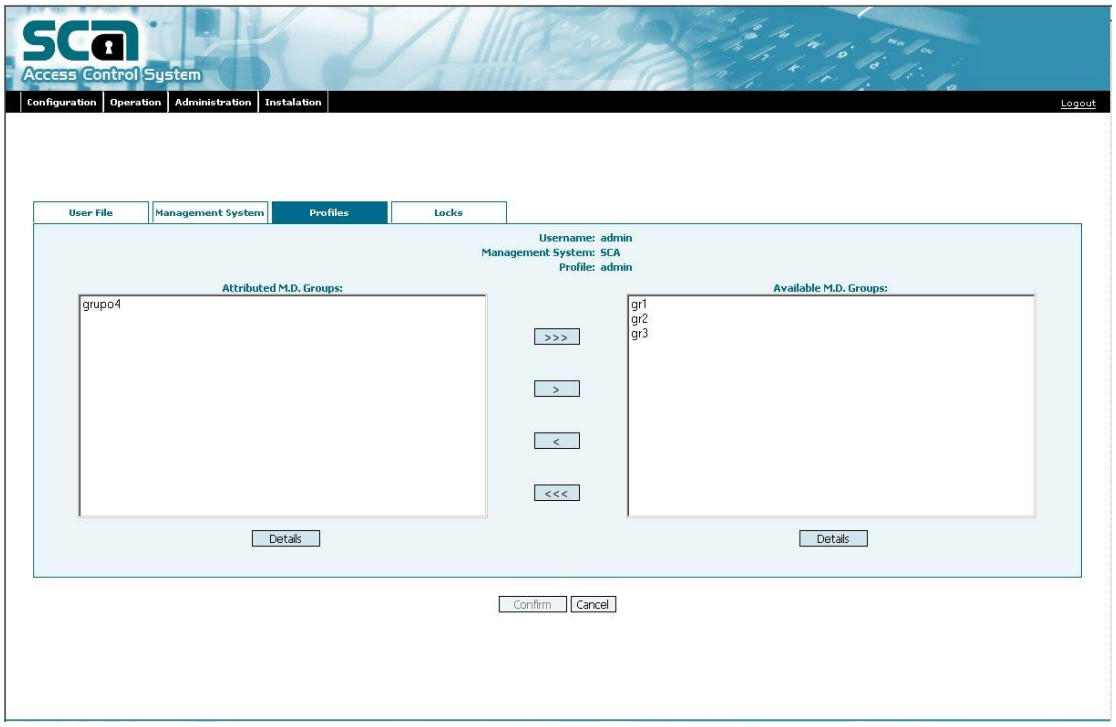
Confirm – this validates the carried out changes between the two lists, and returns to the page containing the list of user profiles

Cancel – this cancels the changes carried out between the two lists, and returns to the page containing the list of user profiles

Assign Managed Domains Groups to the User Profile

For any given selected profile this action opens a new page containing two lists of groups: on the left are the groups already assigned to the user profile and on the right those that are available.

Figure 214. Assign managed domains groups to the user profile



The available commands are:

'>' or '<' – this transfers the selected groups from one list to the other; to select multiple items use the keys SHIFT + mouse click and CTRL + mouse click

'>>>' and '<<<' – this transfers all the groups from one list to the other

Details – this shows the composition of a selected group in terms of managed domains by family

Confirm – this validates the changes carried out between the two lists, and returns to the page containing the list of the user profiles

Cancel – this cancels the changes carried out between the two lists, and returns to the page containing the list of the user profiles

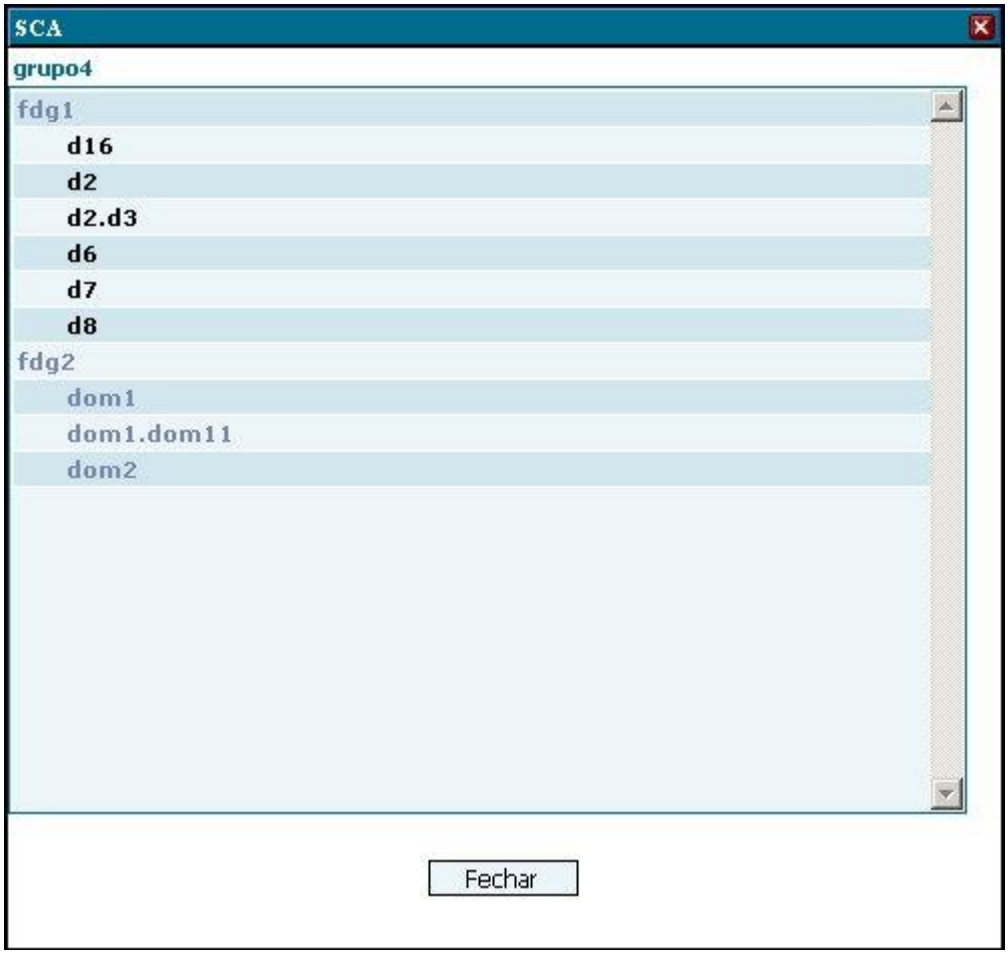
Note 1: The available groups are the ones that have at least one element of an MD family assigned to the current management system. However, from the domains that constitute a group, only those which have been previously configured in the possibilities matrix for the management center to which the user belongs are in fact actually assign to the user profile ("Possibilities Matrix" section). If the possibilities matrix has not been previously configured, the set of domains assign by a group may be blank.

Note 2: Assigning or un-assigning groups to users does not interfere with the list of managed domains that have been directly assigned to the user. In the same way, individual assigning or un-assigning of managed domains does not interfere with the list of assigned groups. That is, a group cannot be considered as assigned to a user when all its managed domains have been assigned individually; neither can a group be removed from a user if some of its managed domains which were assigned individually, but are also part of managed domains groups, are being un-assigned.

View Group Details

By selecting the button Details on the page for assigning groups, and if a given group has been selected in any of the lists, a new page will appear showing its member managed domains, grouped by MD family. In this list, the managed domains which are assignable or which have actually been assigned to the user profile in accordance with the definitions of the possibilities matrix for the user's management center, will appear in Bold.

Figure 215. View details of a managed domains group



Locks

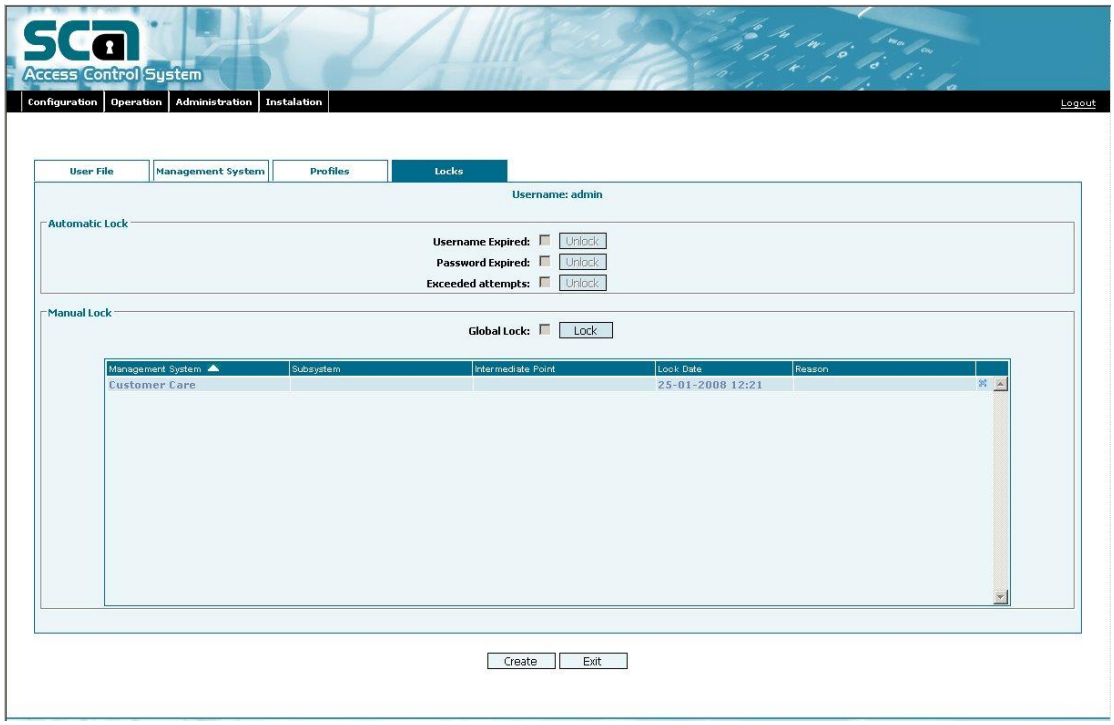
This panel allows consult and manage user locks, which can be of several types:

- **Automatic** – those that are managed by the system itself and where manual intervention is only required to unblock the situation. There are three types of automatic locks:
  - **Expired Username** – when the username's date of validity has expired
  - **Expired Password** – when the password's date of validity has expired
  - **Exceeded login attempts** – when the number of tries to enter the password has been exceeded

- **Manual** – those that are totally managed by the SCA administrator, and include the date of the beginning of the lock as well as the (optional) reason for it. These can be of several types:
    - **Global Lock** – the user is temporarily prevented from carrying out any action in any previously authorized management system
    - **Management System** – the user is temporarily prevented from carrying out any action in the system(s) that have been locked
    - **Subsystem** – the user is temporarily prevented from carrying out any action in the subsystem(s) that have been locked
    - **Intermediate Point** – the user is temporarily prevented from carrying out any action in the intermediate point(s) that have been locked

The automatic locks, as well as the global locks are highlighted in an activated checkbox, and can be deactivated by the respective 'unlock' icon. In the absence of a lock the respective checkbox remains blank and the 'unlock' button is deactivated.

Figure 216. User's locks



Possible commands are:

Unlocking expired Login – this calls up a calendar where a new date to replace the current one should be inserted, or else left blank

Unlocking expired Password – calls a form to insert and confirm a new password, as well as its validity date. The unlocking of the password also forces to its change

Unlocking Exceeded login attempts – the user will be immediately unlocked, and the counter for invalid login attempts reset back to zero

Lock/Unlock Global Lock – the user is locked/unlocked to log into any of the management systems

Add – this adds a line to the table of locks by context after selecting a management system, a subsystem or an intermediate point (Figure 217)

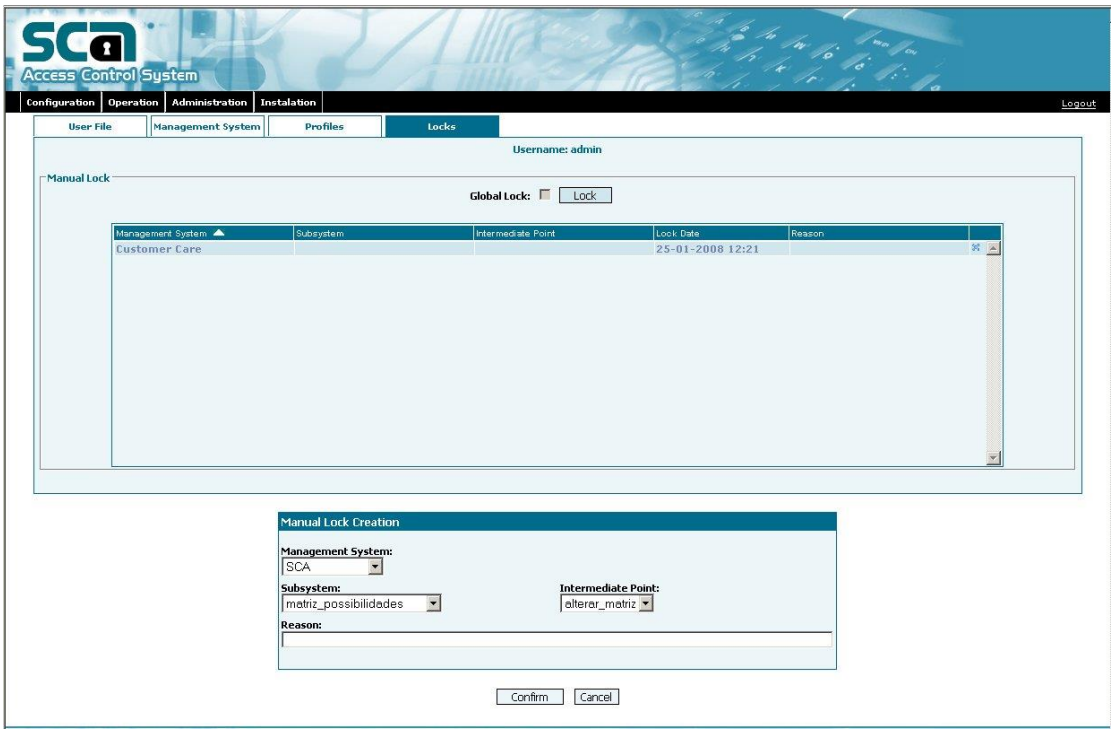
Remove – this removes the lock corresponding to the selected context

Exit – returns to the users list page

Add Locks by Context

The locks by context can be at the levels of management system, subsystem or intermediate point.

Figure 217. Add locks by context

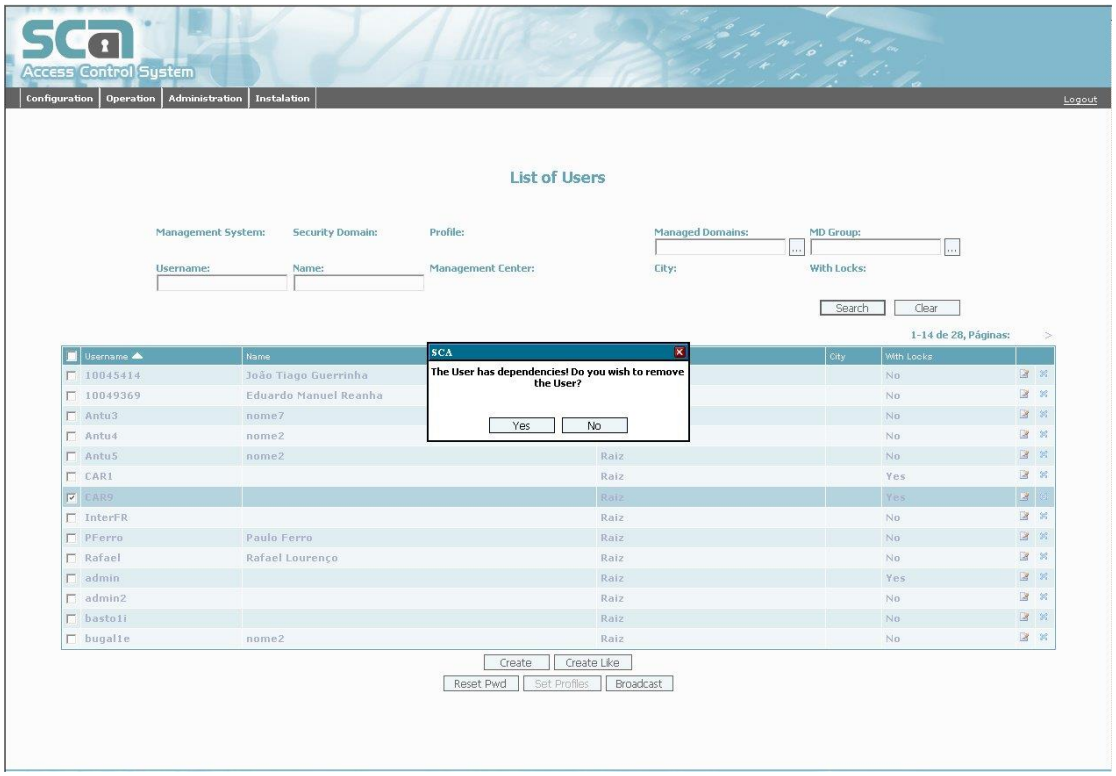


The Confirm and Cancel buttons respectively confirm or cancel the alterations made and lead back to the previous page.

Remove User

To remove a user, simply press the remove button on the right of the wanted user register (Figure 218). This command, once confirmed in the confirmation screen, deletes the user registration along with all the existing associations to management systems, profiles and locks.

Figure 218. Remove user



User Details

The Details button in the User homepage (Figure 214) allows access to the four panels described above as well as to the History panel, though only for consultation purposes. The only action that can be taken apart from navigation between the panels is to exit and return to the user homepage.

History

The Details option offers another panel in addition to the ones previously described. It is called History and allows you to consult the records of a user's sessions in each authorized system, whether in a detailed or compressed form.

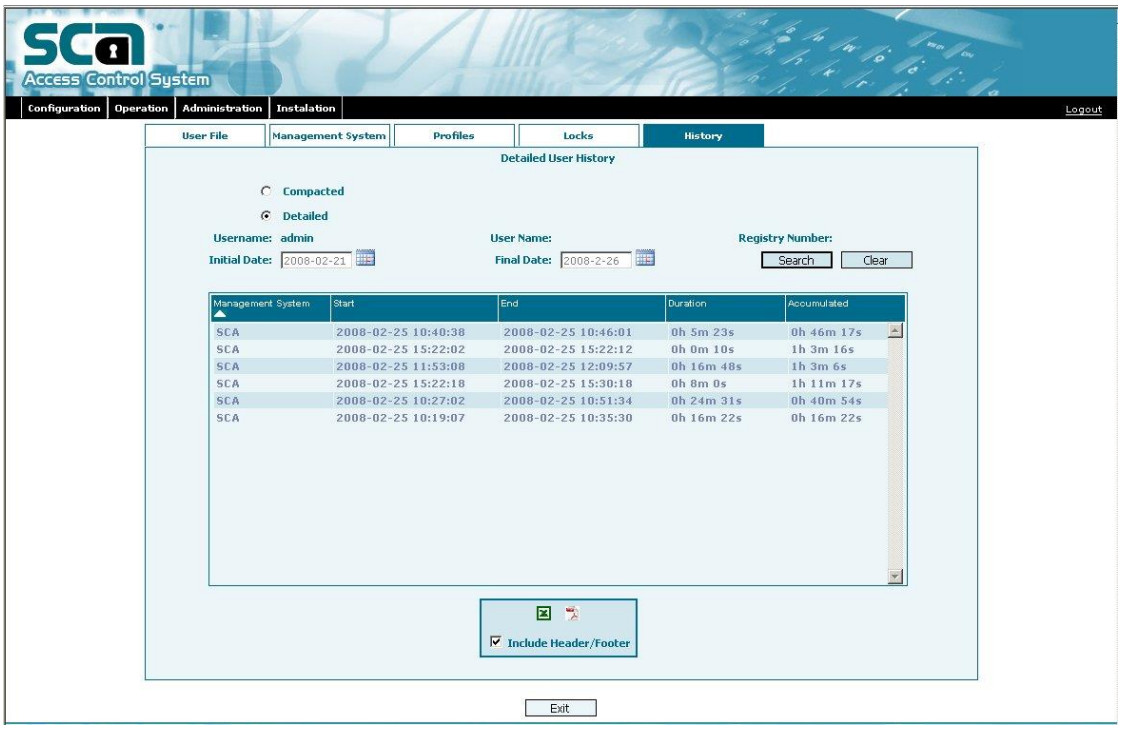
A radio button allows you to commute between the detailed or compressed form in the same panel.

Both types of historical reports allow the extraction to PDF or Excel files.

Detailed Sessions History

The detailed history allows you to see the sessions that a user has had throughout a selected period of time. The data presented are: management system, date of the beginning of the session, date of the end of the session, duration of the session and accumulated session time.

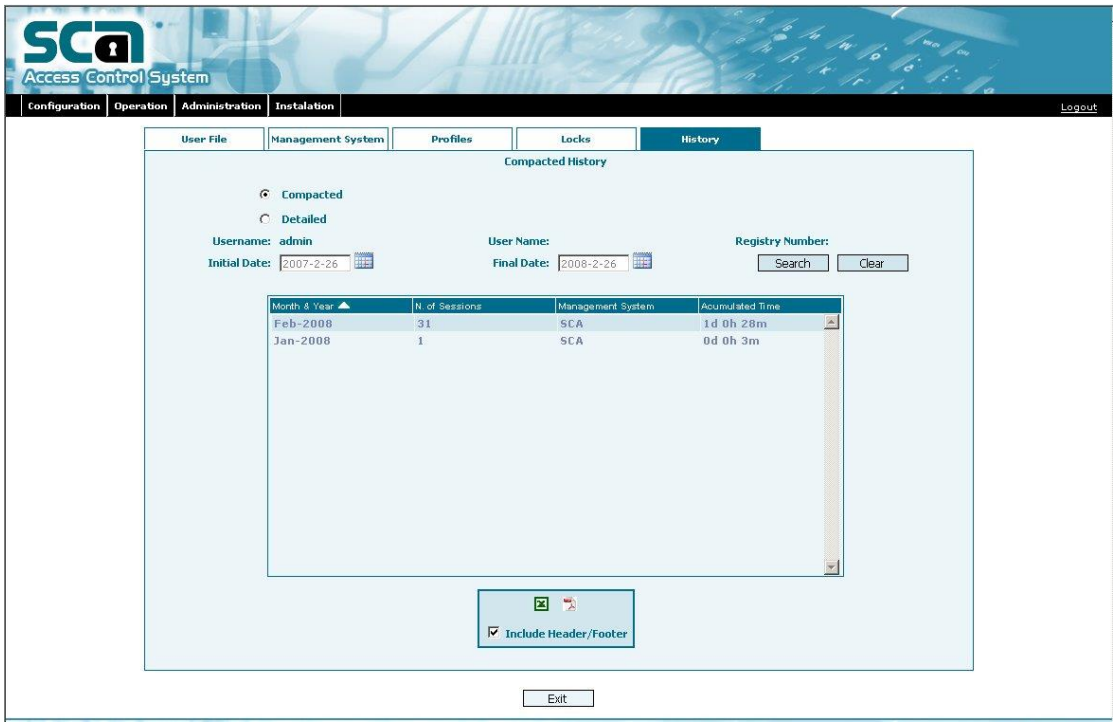
Figure 219. Detailed history of user sessions



Compressed Sessions History

The Compressed history allows you to consult the total number of sessions and the accumulated monthly session time in a given management system, between two given dates.

Figure 220. Compressed history of user sessions

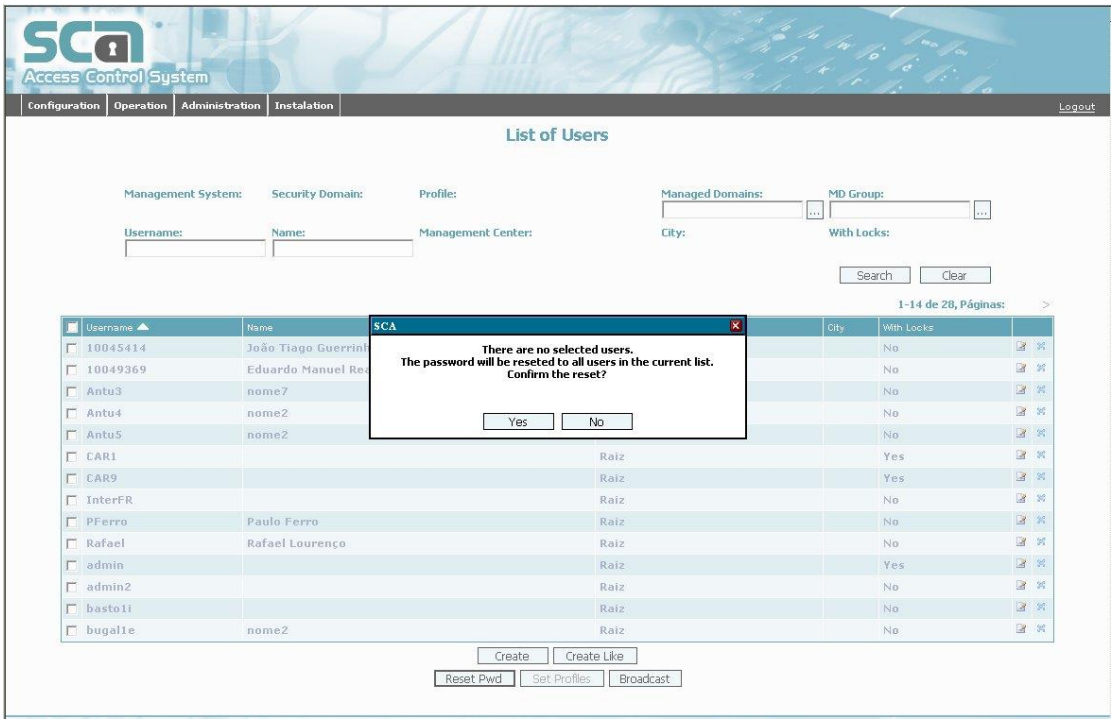


Reset Password

This action results in the change of password to the default value as defined in the SCA database. After due confirmation, it is applied to all users selected through activation of the check box to the left of each registration or in the case of any user selected to all users filtered in the current list. The system will demand confirmation, previously informing that the password will be reset to either the selected user or all filtered users.

All users whose passwords have been reset will automatically have to alter it on their first login, which should also be done within the stipulated time limit (“Global Settings” section).

Figure 221. Confirmation of the Reset Password command



Assign Profiles

The result of this action is to assign profiles, domains and groups to all the users currently filtered or the users which are selected through their check boxes only.

The prerequisite of this function is that the current users belong to the same management system. If this filter option has not been used the button 'Assign Profiles' will not be available.

The process of assigning profiles, managed domains and groups to a set of users follows the same sequence as described in "Assign Profiles to a User" section, knowing that the presented information is restricted to that which is common to all users, whether it is about profiles, domains or groups.

In this case, when viewing a group's content ("View Group Details" section) the window displaying the group details will highlight with a bolder color the managed domains that are common or will remain common to all users, and a softer color will be used to show those not authorized for all users, according to the attributions in the possibilities matrix, or for those that are part of managed domains families who are not assigned to the present management system.

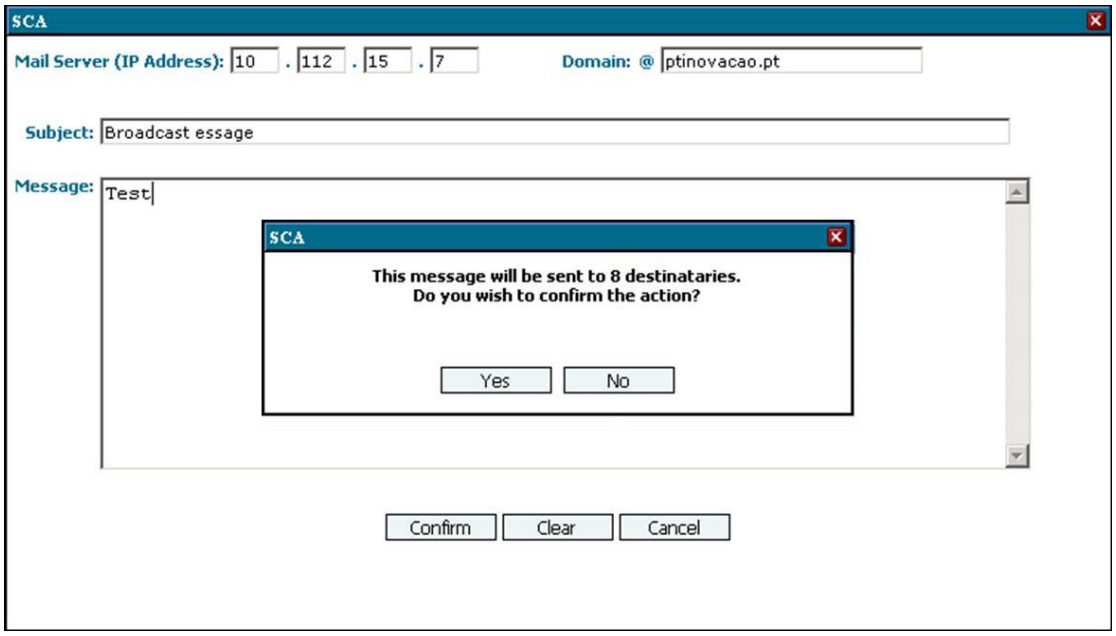
Broadcast

As a result of this action, an e-mail message is sent by SMTP to all users or to a selected set of users. This tool should be used judiciously and only when it is deemed important to send a message or public announcement to part or all the universe of the users registered in the SCA.

Before using the broadcast function you should define the universe of users by means of the use of the available filters or the check boxes attached to each user.

Clicking the Broadcast button will open a new window for introduction of the address of the mail server, the domain, and also the subject and the actual message. The mail server and the domain are memorized and on subsequent occasion these fields will automatically be filled in, although you can change them.

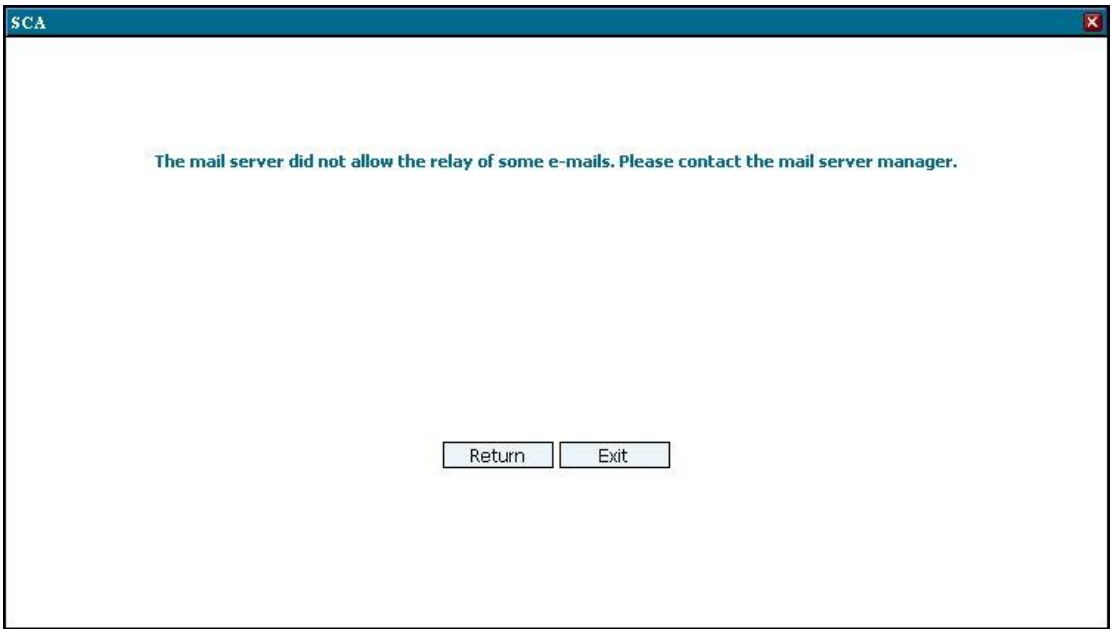
Figure 222. Window to write and confirm a broadcast message



When the message is confirmed, the system lets you know how many recipients it will be sent to, and then only after a final confirmation will it be sent. The number of recipients is calculated on the basis of those selected users that have an e-mail address assigned to them.

Note: If the machine from which the SCA application is running is not authorized to send e-mails to domains other than the company's, the mail server will detect these external addresses and send back a failure notification. In this case the message is not sent to any recipient. This measure is taken by the mail server and not by the SCA application. To get around this situation the mail server administrator could be asked to authorize the SCA server to send mails to other domains.

Figure 223. Failure notification from the mail server



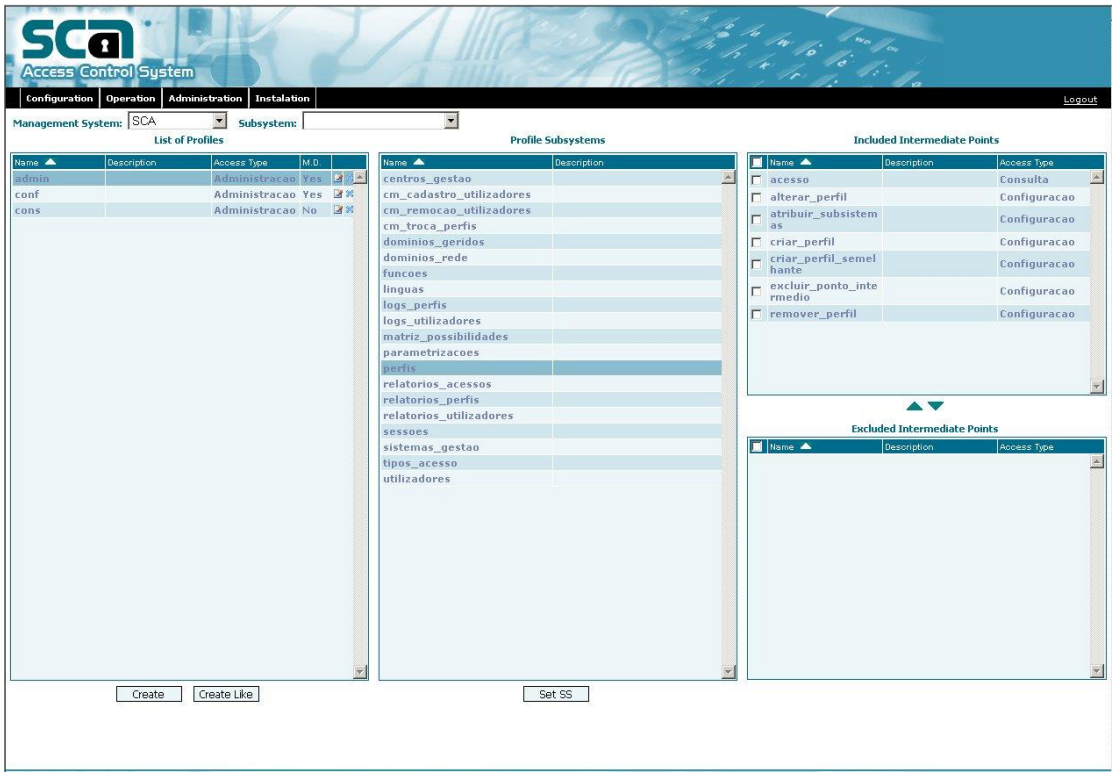
Profiles

Choosing the Profiles option opens up a page where, after selecting a management system, all the profiles created for that system are listed. Besides its name, description of access type, there is an indication of whether or not it is possible to assign managed domains for the profile in question. Provided that at least one profile subsystem has the same characteristic the indication given is 'yes'.

If you select a given profile you can view the constituent subsystems. By selecting a subsystem you can view the constituent intermediate points and also exclude or include intermediate points in that profile.

Additionally you can view only the profiles which contain a subsystem of a management system also. So, you must select the system and the subsystem that you want at the top of the list.

Figure 224. List of profiles for a management system



Following actions are possible:

Create – create a new profile for the selected management system

Create Like – create a new profile similar to the one previously selected, except that you have to give it a new name. This profile will have the same structure in terms of subsystems, intermediate points and access type as the original. Alteration to the profile's constitution can be done, but only after the profile has been saved first

Modify – this alters the profile (e.g. identification, access type

Remove – this removes a profile

Assign SS – this adds or removes subsystem(s) to/from a profile

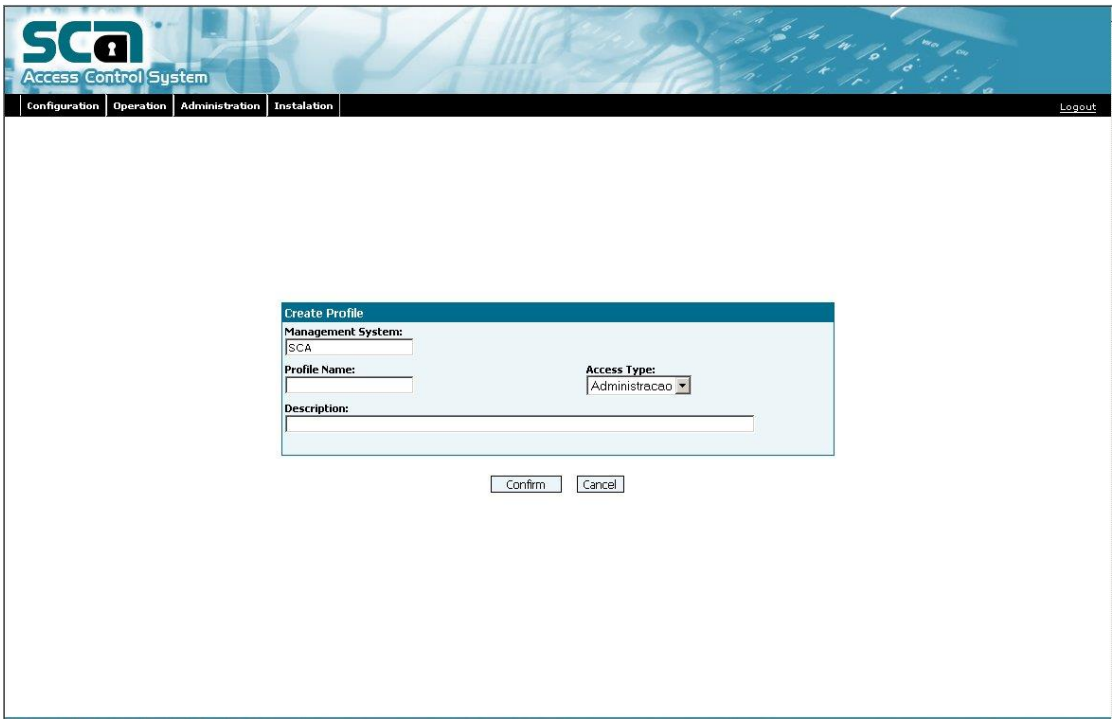
▼ - exclude an intermediate point

▲ - include an intermediate point

Create / Create Like / Modify Profile

These actions open a page where you can indicate the new profile and respective access type.

Figure 225. Profile identification screen



The Confirm and Cancel buttons respectively confirm or cancel changes made and take you back to the previous page.

Description of the fields of the profile identification form:

Table 50. Profile identification

Field	M/O	Description
Management System	M	Name given to the Management System, non editable
Profile Name	M	Name given to the Profile
Description	O	Description of the Profile
Access Type	M	Access type allowed

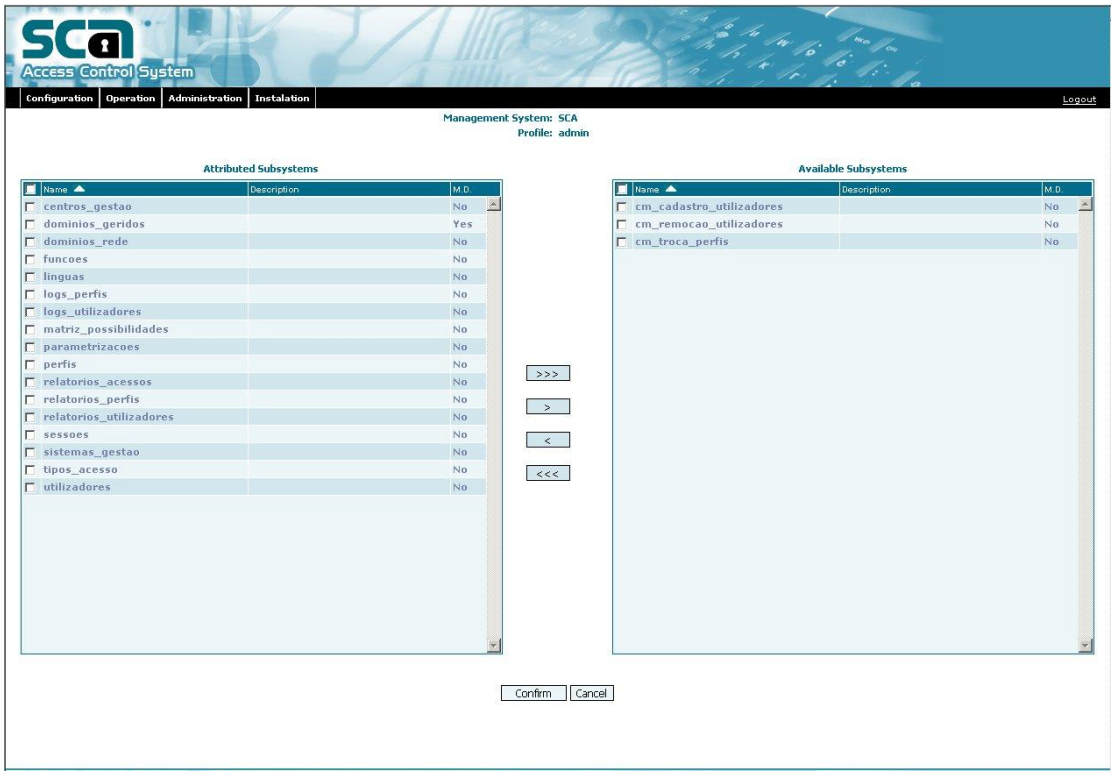
Removing a Profile

To remove a profile you simply have to press remove button on the right of the wanted profile. Removal can only be carried out if the given profile is not currently assigned to any user.

Assign Subsystems to the profile

For a given selected profile this action opens a new page with two lists of subsystems: the left-hand-side displays the subsystems already assigned to the profile and on the right-hand-side all the available subsystems. Both lists show the subsystems that belong to the previously selected managements system.

Figure 226. Assign subsystems to a profile



Possible actions are:

'>' or '<' – transfers the selected subsystems from one list to the other

'>>>' and '<<<' – transfers all the subsystems from one list to the other

Confirm – validates the changes carried out between the two lists, and returns to the page containing the list of profiles of a given management system

Cancel - this cancels the changes carried out between the two lists, and returns to the page containing the list of profiles of a given management system

To select the subsystems that you want move from one list to another one, you must use the check boxes attached to each subsystem or a check box in the line of the title which allows selecting all subsystems of the list.

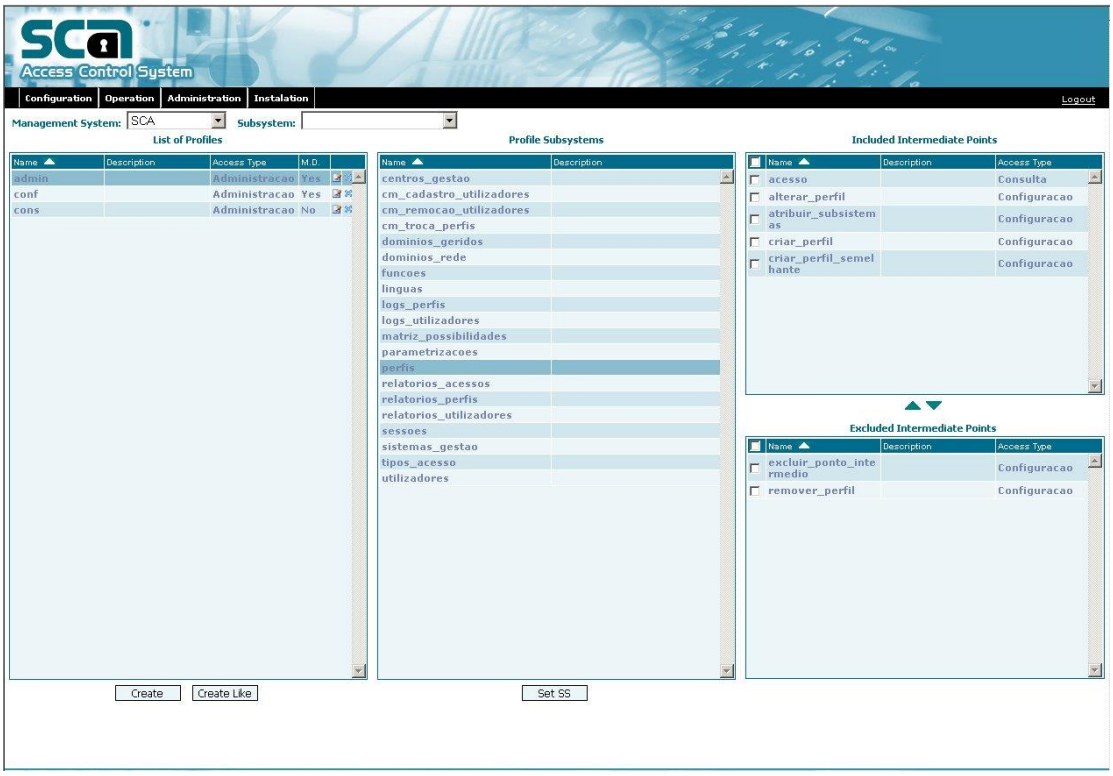
Exclude/Include Intermediate Points in a Profile

These two actions are carried out in the page which shows the profiles of a given management system after selecting a profile and a subsystem.

By default, when a subsystem is included in a profile, all its intermediate points are included. If you wish to configure exceptions to the rule you should select the desired intermediate points and, using the buttons and, transfer them from one list to the other.

To select intermediate points to move from one list to another one, you must use the check boxes attached to each line or a check box in the line of the title which allows selecting all intermediate points of the list.

Figure 227. Include/Exclude intermediate points in a profile



Bulk Operations

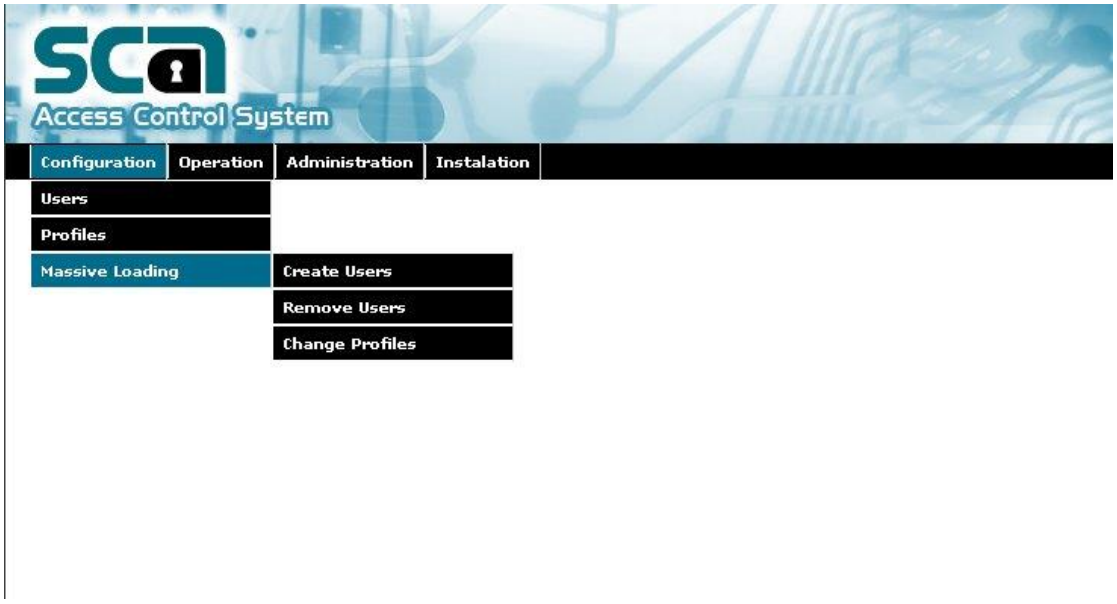
This option leads to three features, all of which require the input of a text file with conveniently formatted data referring to an amount of identical operations to be processed:

Create Users – This creates users in a massive way and associates them with a given management system and a given profile

Remove Users – This eliminates the association of users to a given management system, and can even delete them from the system database if they do not have any access privileges in any other management system

Change Profiles – this swaps one user profile for another. In addition, it allows the deletion or addition of profiles to the user as well as the assignment of managed domains to a given user profile

Figure 228. Menu options for bulk operations



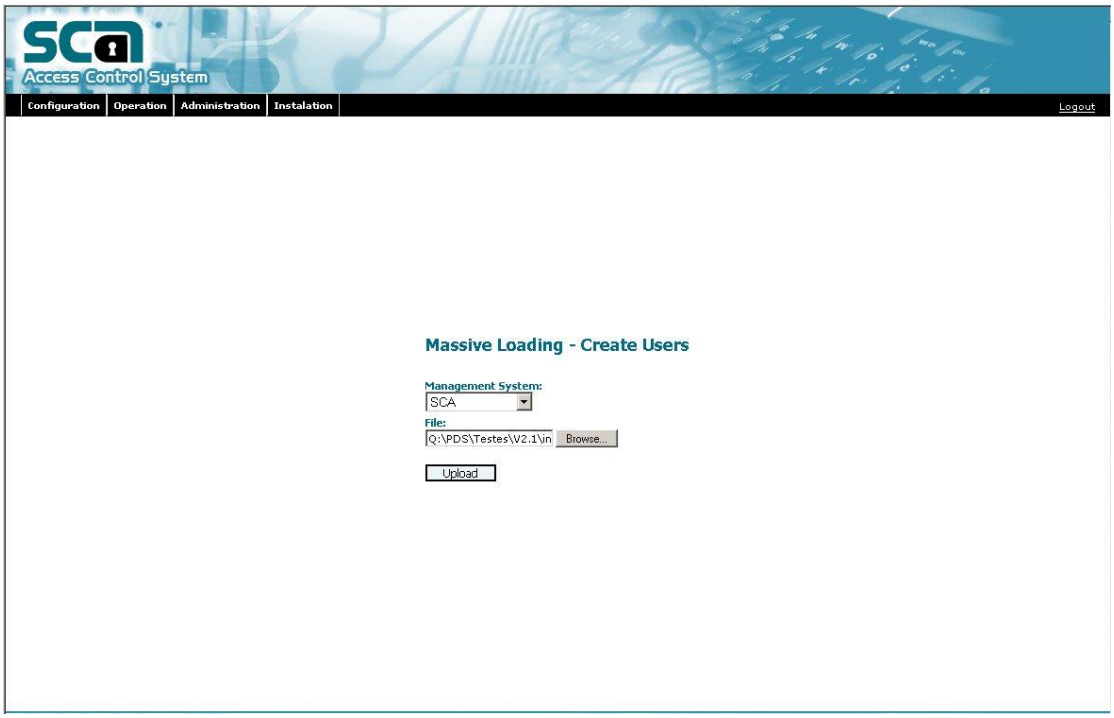
Create Users

Choosing the option Create Users opens up a page where the target management system is to be identified as well as the file for data processing.

The result of this bulk operation corresponds to the creation of the respective users in the SCA database and the assignment to a management system and chosen profile. Of course, the profile indicated in the file of processing must be a valid profile in the required management system.

All users created this way will automatically have to change their password on their first login, which should be within the stipulated time limit (by default 60 days), after which they will be locked out.

Figure 229. Identification of data file for processing



This page has two buttons:

Browse… – this opens up a new window where it is possible to select the path and the name of the file containing the data to be processed

Upload – this begins the processing of the file data

The result of the processing is shown in a new window, either to confirm that the file has been successfully downloaded or to indicate the lines where errors occurred and that were therefore not processed (Figure 230 and Figure 231).

Figure 230. Report of successful file processing

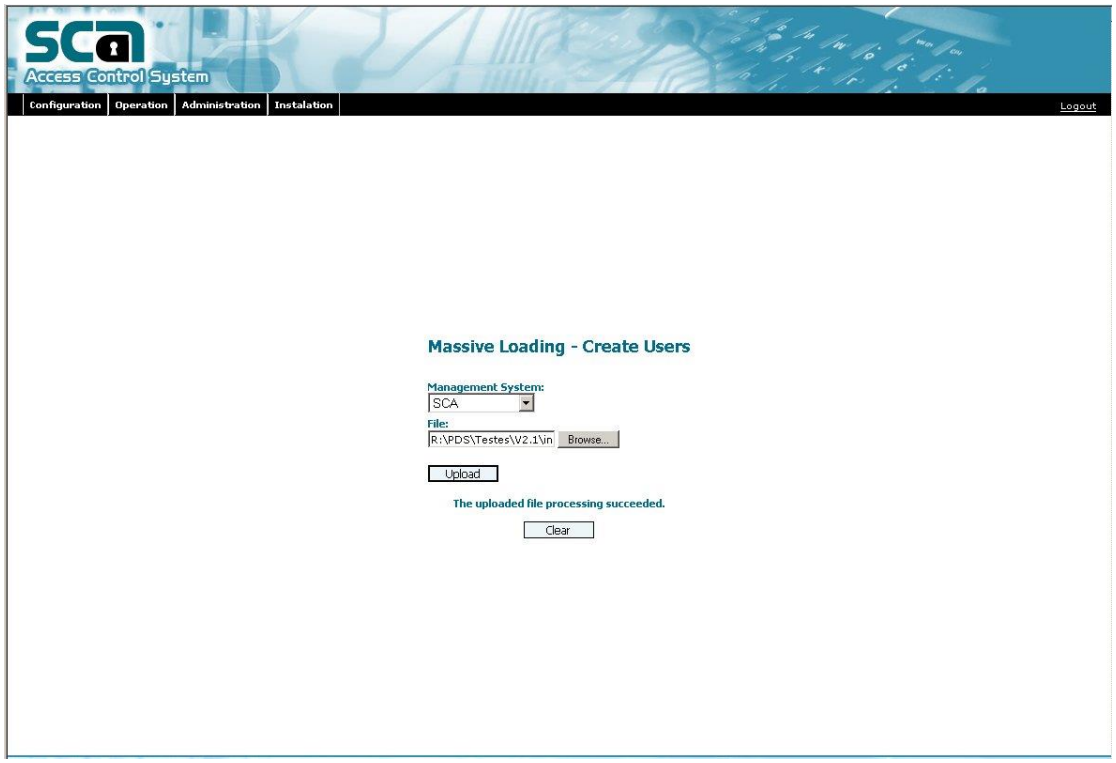
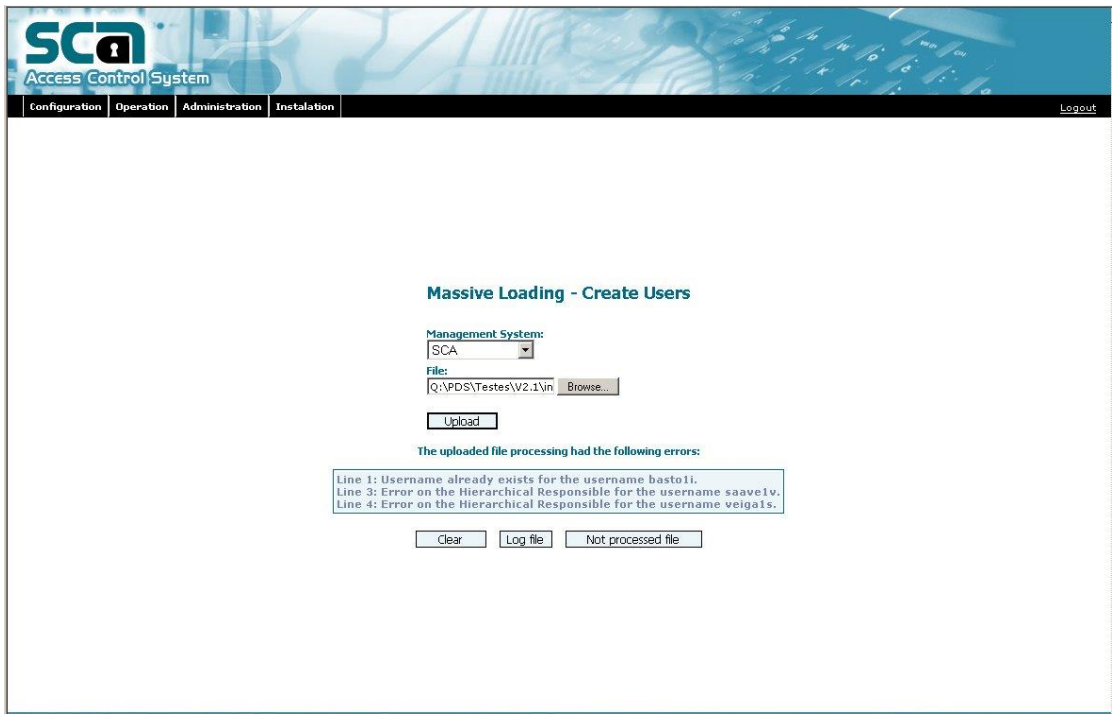


Figure 231. Report of errors in the file processing



If errors have occurred, the unprocessed lines in the original file are put into another file whose name (generated by default) is made up of the name of the original file together with the date and time of the download and with the extension “np”. Besides this, messages containing errors are kept in a log file, whose name (generated by default) is made up of the name of the original file together with the date and time of the download and with the extension log.

In the window showing errors there are three buttons:

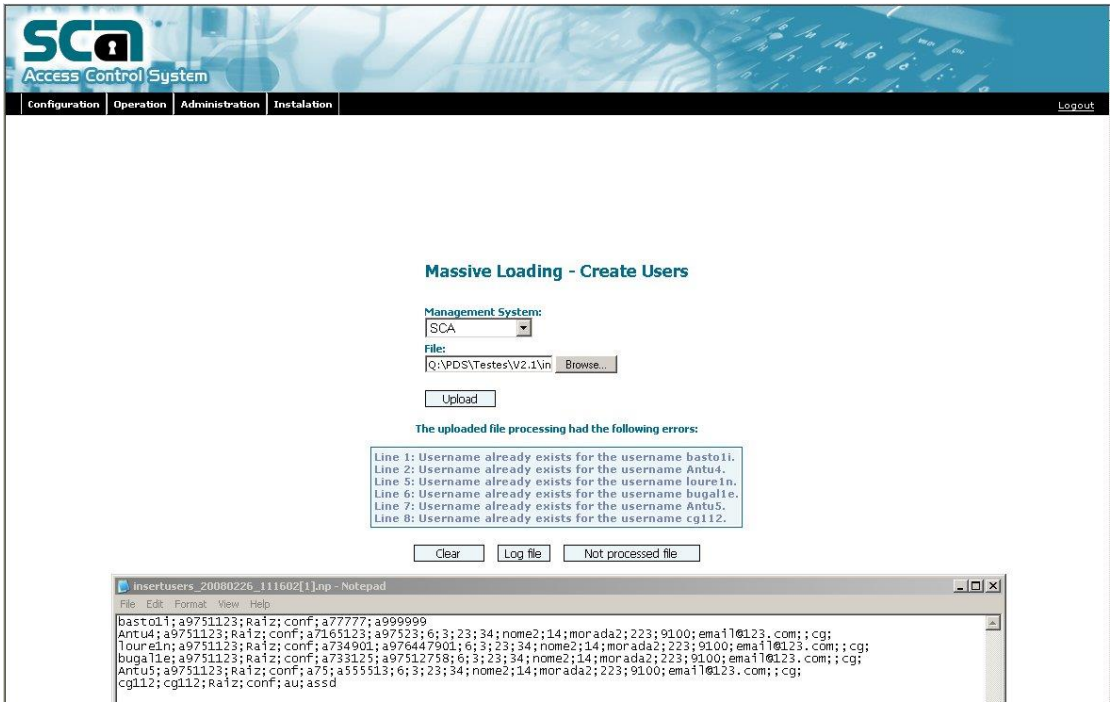
Clear – this clears the result of the previous processing, and this returns you to the window for choosing a file to process

Log file – this calls a download screen allowing you to consult or store the file containing the errors

Non-processed data file – calls a download screen allowing you to consult or store the file containing the non-processed material

The storage place recommended for the download of files is the same as that for the originals, but the user can alter this place as well as the name of the resulting files.

Figure 232. Viewing the file with the non-processed data



Format of the file for mass user registration:

This file must contain all the data that are obligatory for each user, and optionally, the rest, separated by a semi-colon (;). Listed below are the fields in the order they should appear in the file.

* Username	varchar(12)
* Password	varchar(16)

* Acronym of management center	varchar(20+)	can be chained to all or some of the higher management center acronyms if the terminal acronym is not unique
* Profile name	varchar(50)	
** Identity number	varchar(15)	
** Tax number	varchar(16)	
** Registry number	varchar(12)	
Max login attempt	number(1)	
Max simultaneous sessions	number(2)	
Max time per session	number(4)	in minutes
Max idle time	number(3)	in minutes
User name	varchar(50)	
Address	varchar(50)	
Telephone	number(15)	
Mobile phone	number(15)	
E-mail	varchar(50)	
Location	varchar(30)	
Hierarchical superior	varchar(12)	username of hierarchical superior
Job title	varchar(50)	

* this indicates that it is a mandatory field in all installations.

** this indicates that it may be a mandatory field in some installations.

Preferred language, despite being an obligatory category, is not supplied in the file. In Mass Operations the preferred language is considered to be the default language and can be altered online after the mass operation in particular cases.

Also the Network Domain field is not included in the file despite being a required attribute. In a bulk operation, does not make sense that the security domain is different from 'local', and it is this value that is assigned by default.

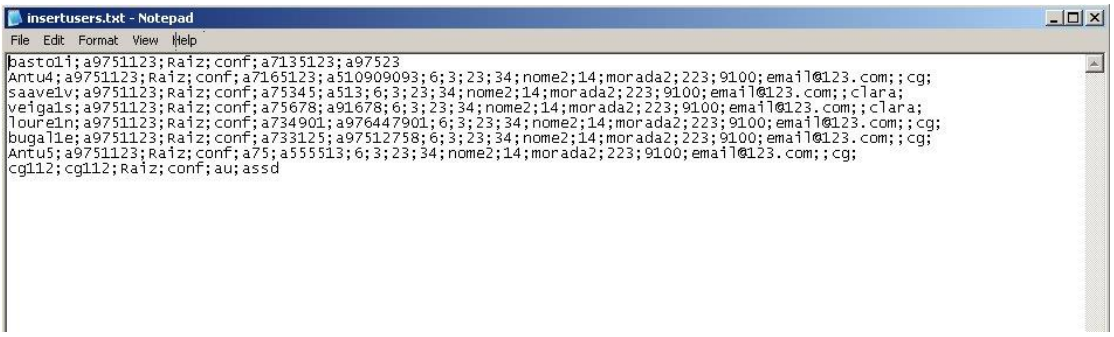
Examples of records:

E0323;95637052468;Vivo.VivoRJ;P108;138238037;95637052468;Operator;

E032311;34967790801;Raíz; P01;7323733737; 34967790801

If you not indicate a field, you should simply mark the tab, as the first registration. You can also omit the void field separators of the line does not contain any more not void field, as se second registration.

Figure 233. Example of a user's registration file



Remove Users

By choosing the option Remove Users, a page is opened where the management system is identified as well as the file containing data to be processed (Figure 229).

The result of this command might correspond to:

- **Removal of the User** – if the user does not have any other access privileges to any other management system besides the one indicated.
- **Elimination of the access privileges** to the indicated management system if the user is authorized for other systems.

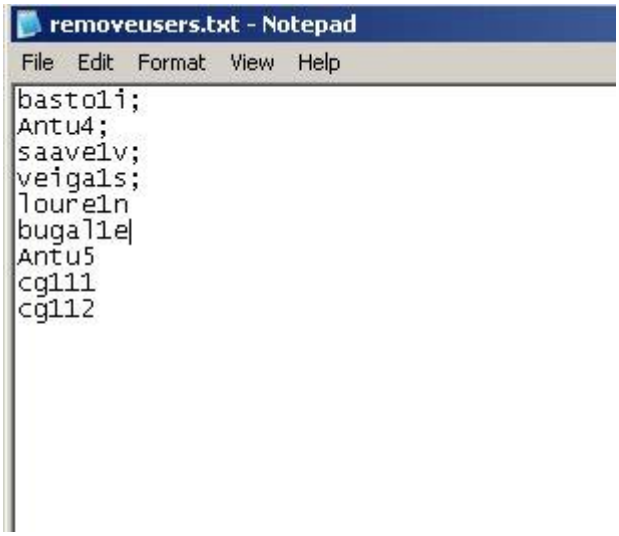
The bulk operations, viewing and downloads of the files either of error or of non-processed data, is the same in all the functionality of Users Register, so we advise you to read the respective paragraph ("Create Users" section).

File format for the removal of users

This file contains only the login of users you wish to remove.

Username - varchar(12)

Figure 234. Example of a file for the removal of users



Change Profiles

By choosing the option Change Profiles, a page is opened where the management system is identified as well as the file containing data to be processed (Figure 229).

The result of this command might correspond to:

- Change of one profile for another– the user stop having the first profile mentioned and adopt the second instead;
- Removal of a user profile - if the second profile isn't mentioned in the user record, he just stops being associated to the mentioned profile.
- Addition of a new profile - if the first profile isn't mentioned in the user record, the result is the adding of the second mentioned profile, that is, one additional profile has been assigned to the user.

Attribution of a managed domain to the user with a given profile – a managed domain can be joined to the profile in the third field, set in the record as an additional fourth field after the user identification and the two profiles.

The bulk operations, viewing and downloads of the files either of error or of non-processed data, is the same in all the functionality of Users Register, so we advise you to read the respective paragraph ("Create Users" section).

File format for Changes Profiles

This file is composed of the following fields:

* Username	varchar(12)
Name of the profile to remove	varchar(50)
Name of tithe profile to assign	varchar(50)
Managed domain to assign	varchar(80+) – this should be a concatenation of the acronym of the managed domains family with the acronym o the managed domain, separated by '.'. If the acronym of the managed domain is not unique, it can be included

with the acronyms(s) of the higher-level domains in the hierarchy to assure its uniqueness.

* The obligatory fields are the username and at least one profile.

Examples of records:

E032313;P51;P50 (changes profile P51 for P50)

E032313;;P40 (adds profile P40)

E032313;P01; (removes profile P01)

E032313;;P02; Reasons.Contingency (adds profile P02 with the managed domain Contingency of the DG Reasons)

E032313;P50;P51;FDG_Dealers.D1.D11 (changes profile P50 for P51 and assigns the managed domain D1.D11 of the familyFDG_Dealers)

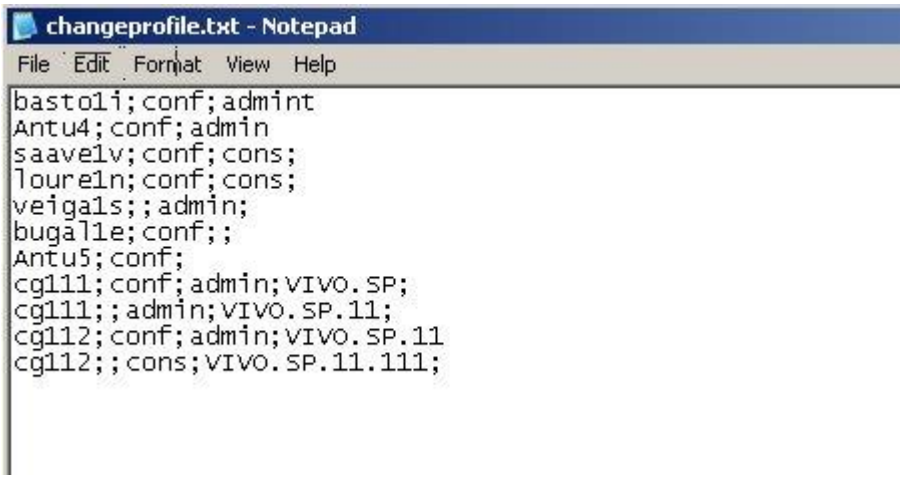
Even though the user might have more than one profile or more than one managed domain this feature is atomic, that is, it only allows:

- changing one profile for another
- removing one profile
- adding one profile
- adding one managed domain to one given user profile

Should you wish to assign or remove more than one profile for the same user, these atomic actions simply have to be repeated in the same file. In the same way repeating in the file the attribution of a domain as many times as the number of managed domains you wish to assign can carry out the attribution of several managed domains in the same profile.

N.B.: This feature does not permit to un-assign managed domains. The solution for this is the removal of a profile and the reassigning of the same one, together with the attribution of the desired managed domains.

Figure 235. Example of a file for changes profiles



Operation Menu

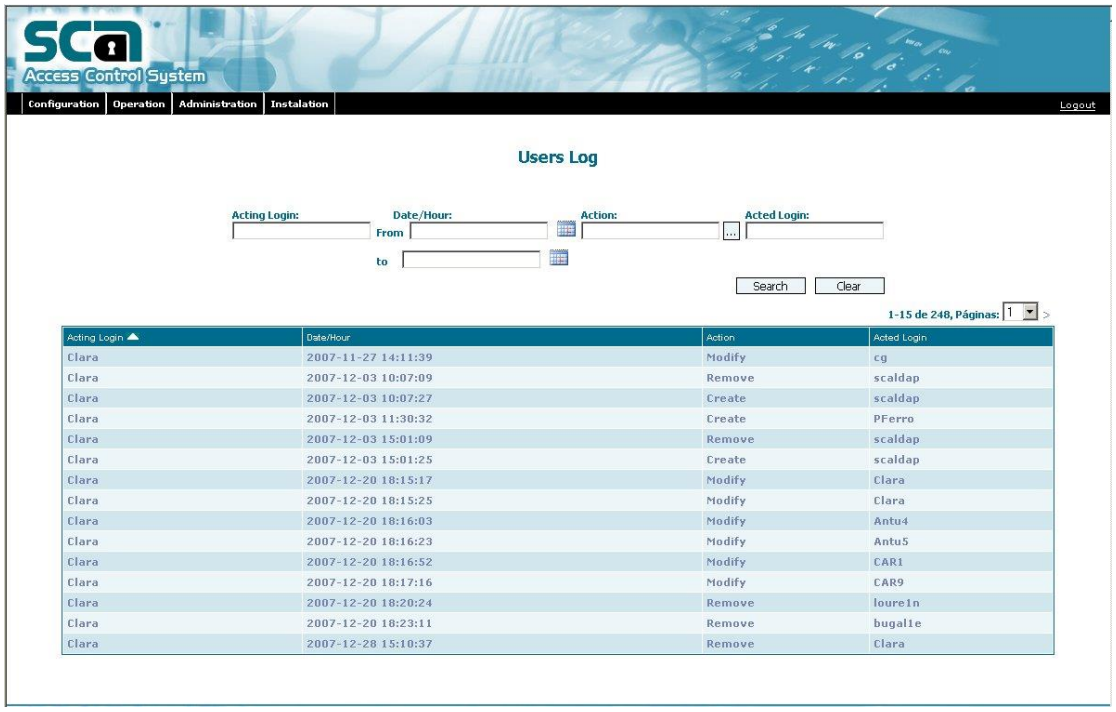
This menu consists of the options Logs, Reports, Bulk Operations and Sessions, whose operations are described below.

Logs

This option gives access to two types of logs:

- **Log of actions on Users** – this registers all actions of creation, modification and removal of users. Each register is composed of the acting user's username, the date/time, the type of action carried out and the action's target user's username.
- **Log of actions on Profiles** – this registers all actions of creation, modification and removal of Profiles, as well as the alteration of their structure in terms of subsystems and intermediate points. Each register consists of the acting user's username, the date/time, the type of action carried out, the name of the profile acted on and additional information that could refer to the name of the subsystem or intermediate point which has been included/excluded.

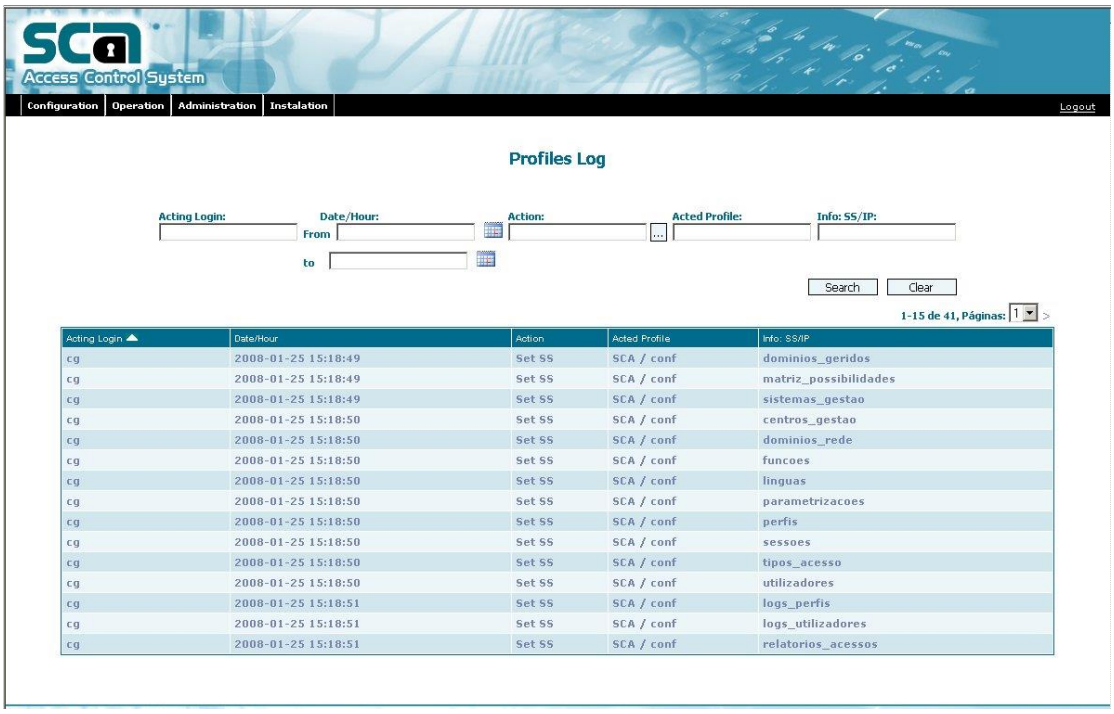
Figure 236. Log of action on users



Viewing the log of registered actions can be restricted to the filters placed in the box under each column header, which can be made of a sub-set of characters to search for in this column, or by a date defining the time frame under analysis. The button with a magnifying glass is used to activate all filters while the button with the eraser/rubber clears al current filters.

By clicking on the title of each column the kind of ordering can be determined or changed. For this, a symbol next to the title shows the chosen type of ordering.

Figure 237. Log of actions over profiles



Reports

This option permits to access to three types of reports:

- **Users Report** – this lists the users who meet certain filtering criteria. The filtering criteria are the management center, the management system, subsystem, intermediate point, profile, managed domain, managed domains group and time windows of the last login
- **Profiles Report** – this lists the profiles of a given management system or those which include a given function such as a subsystem or an intermediate point
- **Logins Report** – this lists the average of logins per hour in a given management system and this allows knowing the daily average profile and the more charged hour. In this report, you can see a graph of the distribution of logins during the day

All types of reports can be exported in Pdf and Excel formats, and in this case with the option of including or not the headers and footers in losses of pages.

Users Report

According to the information inserted into the filtering criteria fields this report can list:

- all users registered in the SCA
- all users of a given management system
- all users with privileges in a given subsystem
- all users with permission to access a given intermediate point
- all users belonging to a given management center
- all users with a given profile
- all users with access to one or more managed domains

- all users with access to one or more assigned groups
- all users who agreed to a management system in a given time window
- several others lists that can be obtained by combining the various available criteria

Besides the variety of filters provided in this report, there is still the possibility to choose the columns to be included in the list, the order and the types of ordination.

Figure 238. Choice of criteria and columns for users report

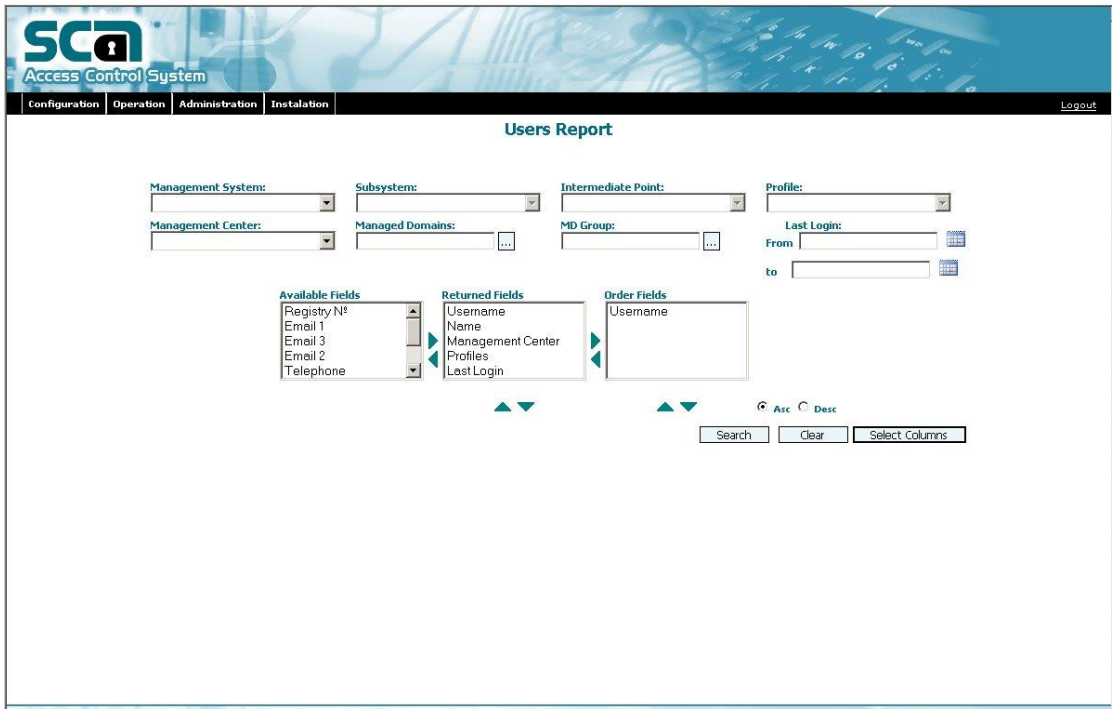
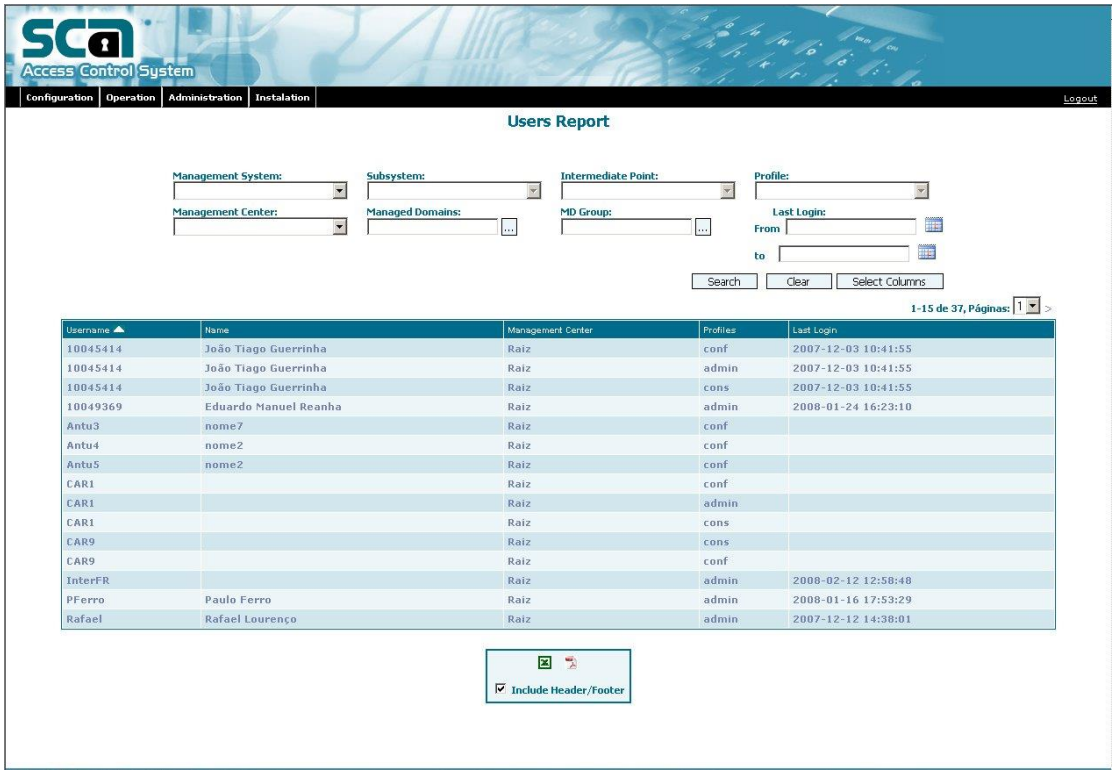


Figure 239. Users report



Username	Name	Management Center	Profiles	Last Login
10045414	João Tiago Guerrinha	Raiz	conf	2007-12-03 10:41:55
10045414	João Tiago Guerrinha	Raiz	admin	2007-12-03 10:41:55
10045414	João Tiago Guerrinha	Raiz	cons	2007-12-03 10:41:55
10049369	Eduardo Manuel Reanha	Raiz	admin	2008-01-24 16:23:10
Antu3	nome7	Raiz	conf	
Antu4	nome2	Raiz	conf	
Antu5	nome2	Raiz	conf	
CAR1		Raiz	conf	
CAR1		Raiz	admin	
CAR1		Raiz	cons	
CAR9		Raiz	cons	
CAR9		Raiz	conf	
InterFR		Raiz	admin	2008-02-12 12:58:48
PFerro	Paulo Ferro	Raiz	admin	2008-01-16 17:53:29
Rafael	Rafael Lourenço	Raiz	admin	2007-12-12 14:38:01

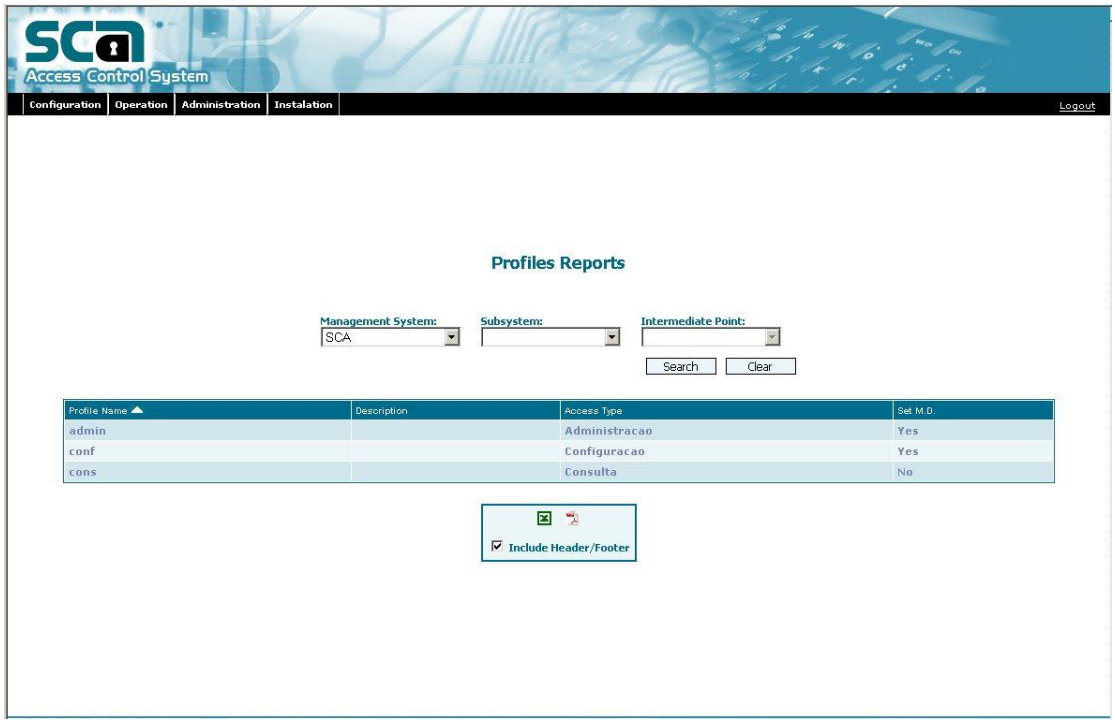
Profiles Report

According to the information inserted into the filtering criteria fields, this report can list:

- all profiles in a given management system;
- all profiles that includes a given subsystem;
- all profiles with a given intermediate point.

The report displays for each profile the name, description, access type and whether or not it accepts assignment of managed domains.

Figure 240. Profiles report



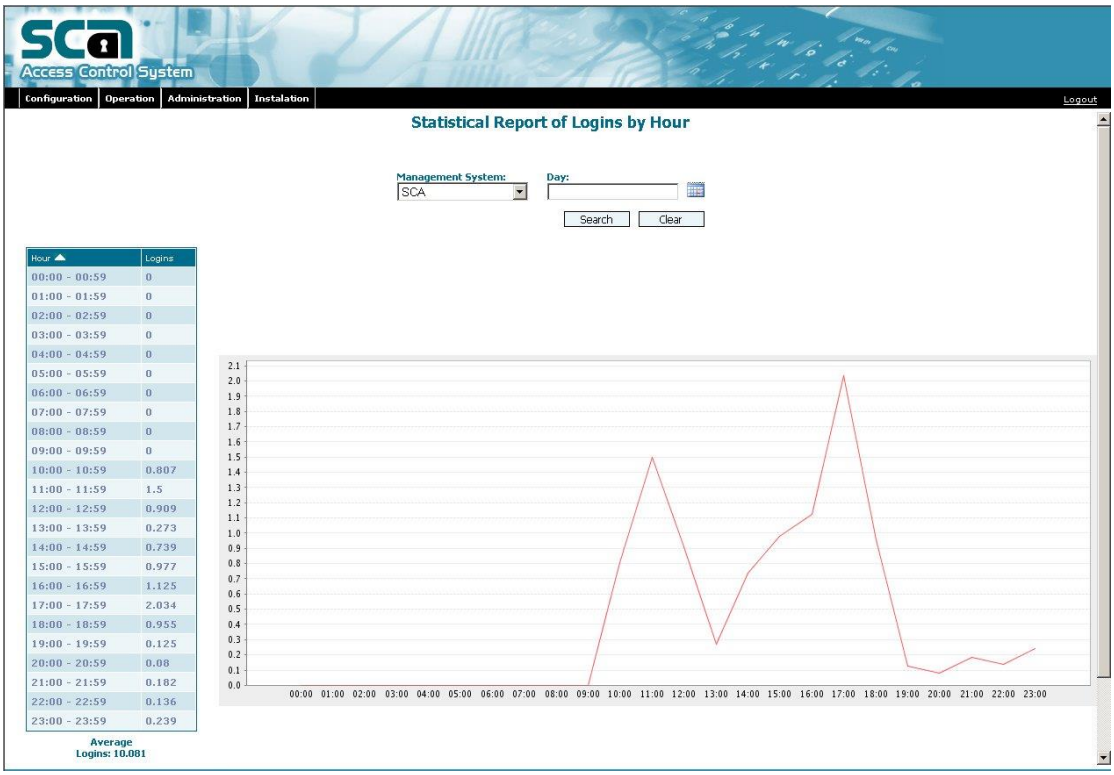
Logins Report

This report provides two types of possibilities:

- to a particular day, it shows the number of logins with success, distributed by the 24 hourly;
- to the set of log data, it calculates the average number of logins per hour.

This report will also provide the respective graph.

Figure 241. Logins report



Sessions

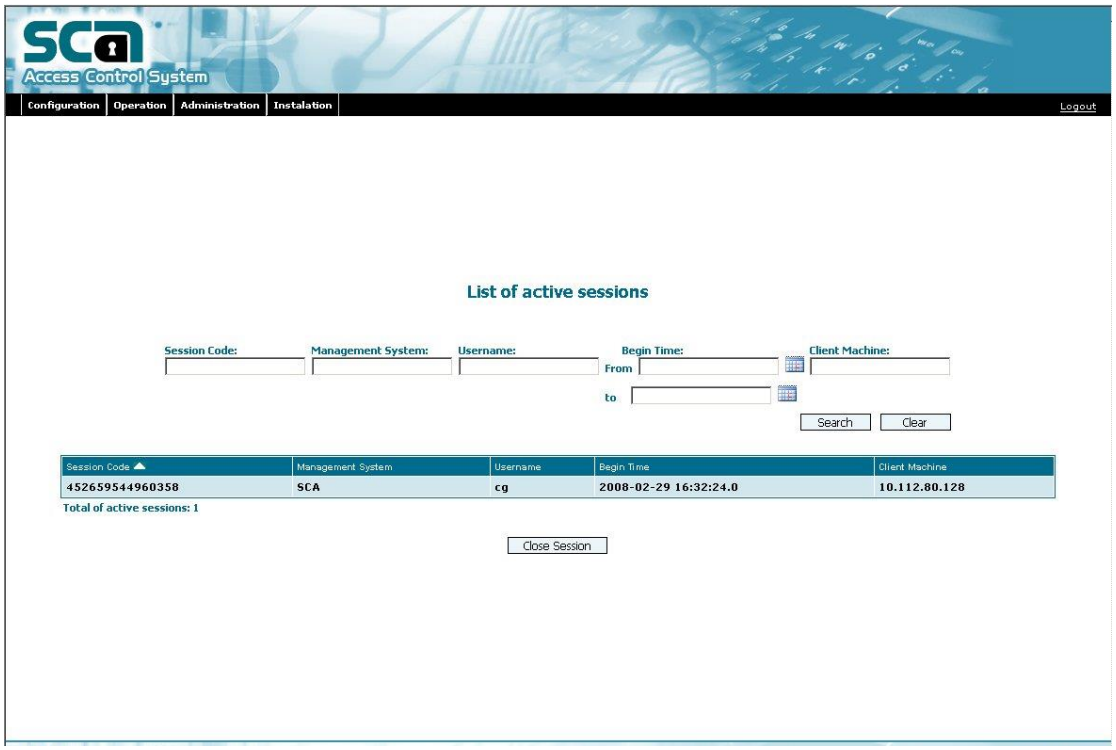
Choosing the option Sessions opens a page where you can view all the open sessions, either on the SCA itself or on any SCA client applications.

Each session is identified by the session code, management system, username, date and time of the beginning of the session and the name of the client terminal. Each of these characteristics can be used as a filter, either alone or in combination, in order to limit the sessions you wish to consult. For example, you can see only the sessions of a given management system, of a sole user, beginning between given periods of time, etc.

The session code can be the same for more than one management session. This happens when the user logs into a portal and from there can access various systems.

The current SCA session is highlighted in the open sessions.

Figure 242. Consulting the SCA open sessions



At the foot of the window there is a button that allows you to close a previously selected session.

The administrative closing down of a session frees the SCA charts of these records, thus reducing the number of open sessions for the same user. However, this action does not eliminate a session from the web server, as this connection has to be terminated by the web session itself.

The administrative closing down is useful to free up locked sessions. However, it should be used responsibly as its misuse could cause the shutdown (in SCA) of an ongoing session, which will then cease to have a connection with the SCA and will begin to show diverse errors.

The system will not allow a current SCA session to close itself down.

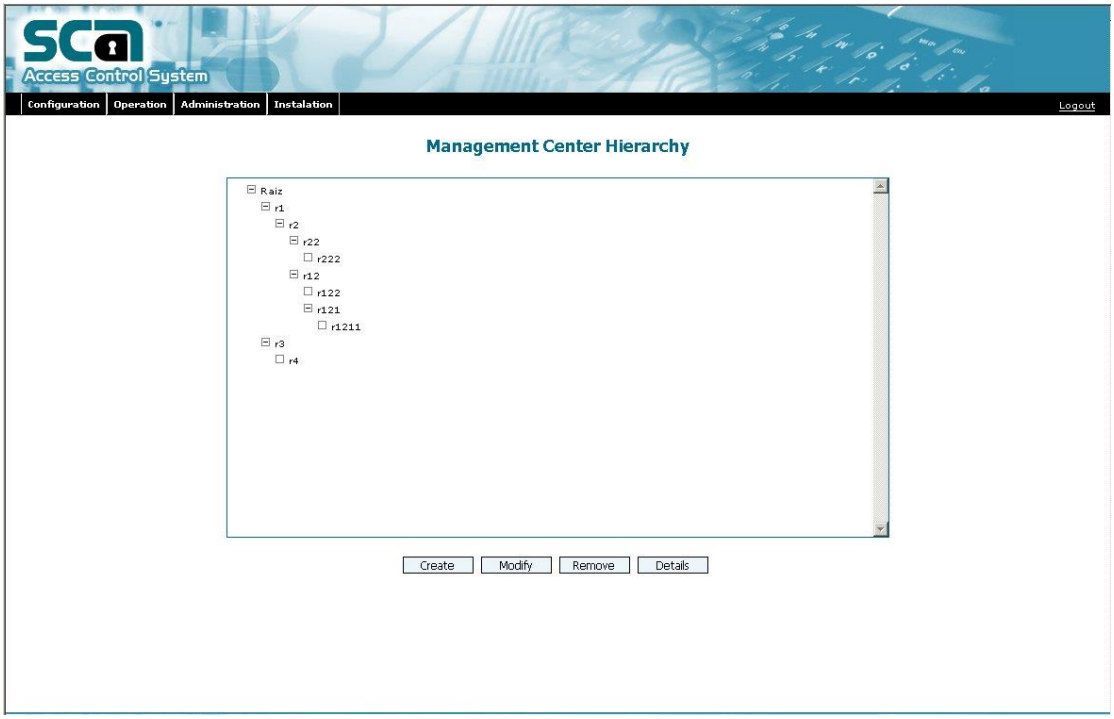
Administration Menu

This menu comprises the options Management Centers, Possibilities Matrix, Settings and Job Titles, as described below.

Management Centers

Choosing the option Management Centers opens a new page displaying the hierarchy of the management centers.

Figure 243. Hierarchy of the management centers



These are the possible commands:

Create – this creates a new management center.

Modify – this alters the characteristics of the management center.

Remove – this removes a management center.

Details – this allows you to view the characteristics of the management center.

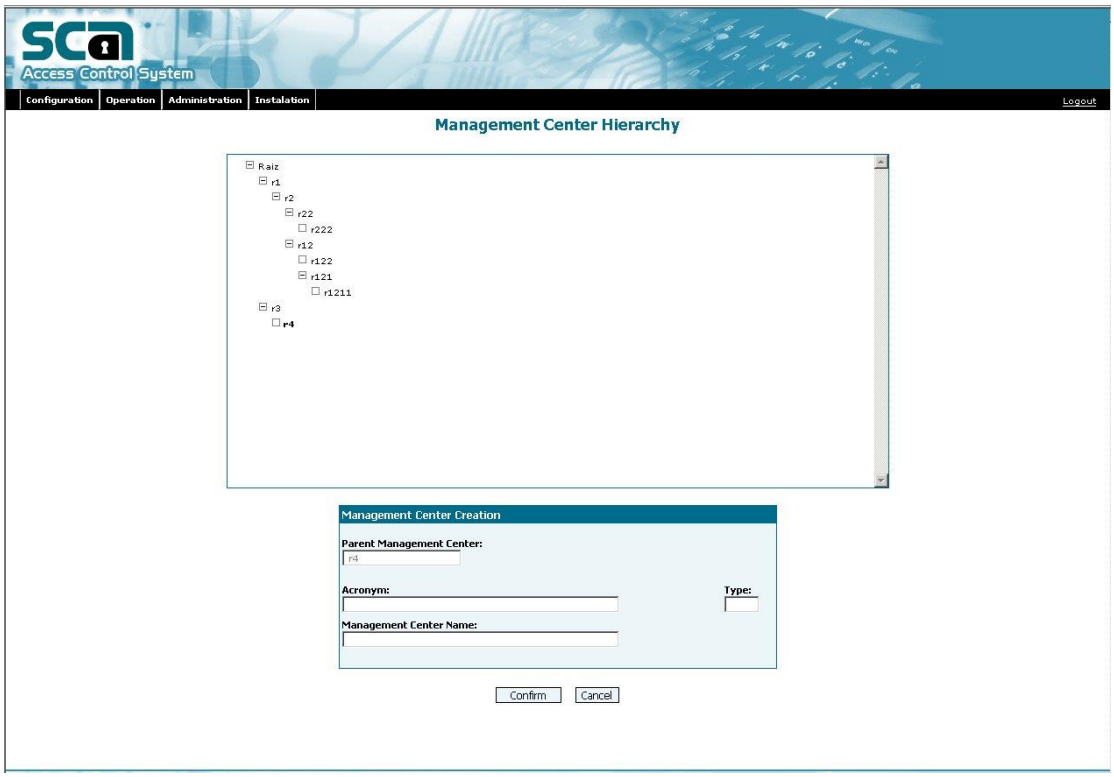
'+', '-' – this opens or closes a branch of the management centers tree.

Create Management Center

By default there is a management center with the name of 'Root' that corresponds to the root of the tree diagram. This name can be customized by using the Modify option, according to the hierarchical structure that you wish to display in the diagram. For example, the 'Root' can be changed to 'PTIN', 'VIVO', etc.

To create a new management center you should select the parent center under which you intend to insert the new center and then pressing the button Create. A new frame will automatically appear on the same page where you can insert the necessary details of the new center.

Figure 244. Creating a management center



The Confirm and Cancel buttons confirm or cancel respectively any modifications and then close the input frame.

Description of the fields in the management center identification form:

Table 51. Management center identification

Field	M/O/A	Description
Parent Management Center	A	Acronym of the management center previously selected in the tree
Acronym of Management Center	M	Abbreviation of the management center – this is the one shown in the tree
Name of the Management Center	O	Full name of management center
Type of Management Center	O	Optional list of a list of types of management centers (e.g., main department, section, store, etc.). This is not a pre-written list so you are free to fill in the details that you wish.

Modify Management Center

This is identical to the Create command, with the only difference that instead of selecting the parent management center, choose the management center intended to be modified.

Remove Management Center

To remove a management center, simply select it in the tree and press the Remove button.

Restrictions to the remove command:

- only removes a management center that isn't associated with users.
- only removes a management center that have no other centers depending on it in the hierarchy.

Details of the Management Center

This action allows you to consult the characteristics of any given management center. A screen appears which is identical to that used for Create and Modify but with no other action except Exit.

Possibilities Matrix

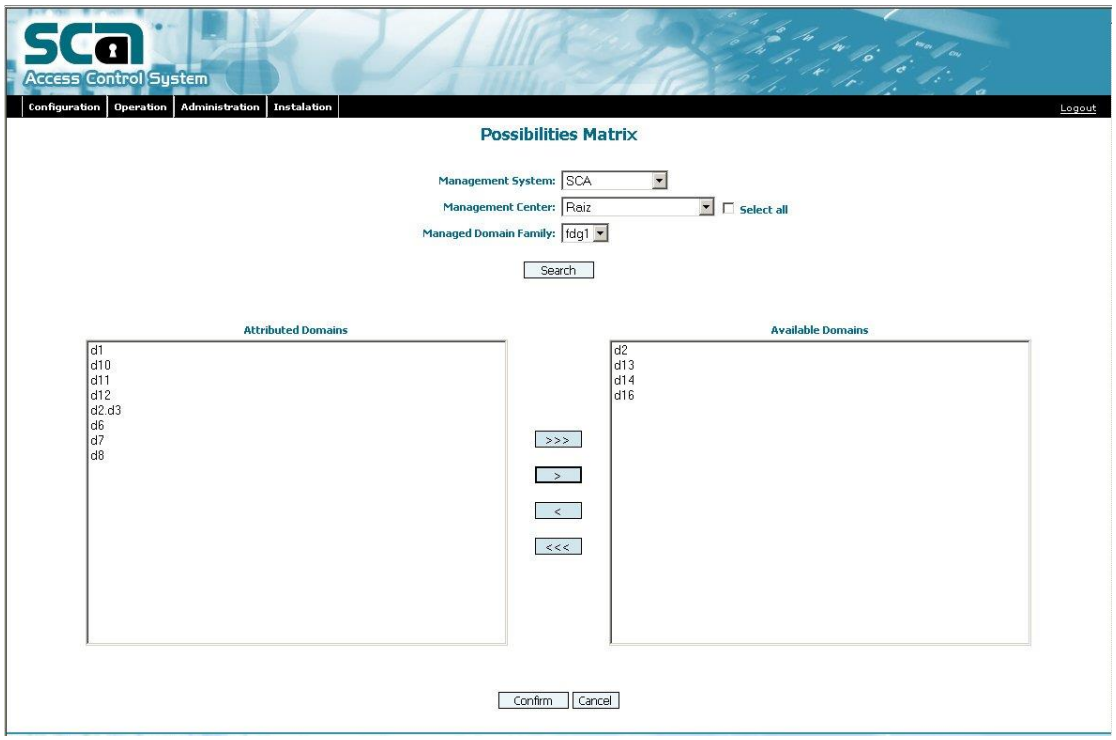
The option Possibilities Matrix allows you to establish relations between management centers and managed domains or, in other words, it allows you to define/restrict the managed domains to which the users in a given management center

have potential access, when assigning managed domains to a user profile (in the case of a profile which allows the assigning of managed domains).

In this display, first select the management system and the managed domains family to configure or simply consult for the possible interconnections between management centers and domains. A button on the right of the management center allows you to choose whether to apply it to all of them or only to one.

Assigning or un-assigning managed domains is carried out by moving items from one list to the other, showing the domains assigned to the selected management center (or all) on the left, and on the right the available domains. To select multiple items to move from one list to the other, use the controls SHIFT + mouse (selecting various items in a row) and use CTRL + mouse to pick several single items.

Figure 245. Possibilities matrix



When all the management centers are selected, the assigned domains correspond to the match of domains assigned to each center individually. If there is no match, the list on the left appears empty, which doesn't mean that there is no domain assigned individually to the management centers.

Possible commands are:

'>' or '<' – move the selected domains from one list to the other, for which SHIFT + mouse and CTRL + mouse can be used for multiple items.

'>>>' and '<<<' – transfer all domains from one list to the other.

Confirm – validates the changes made between the two lists. This button is only active if there are changes to validate or cancel.

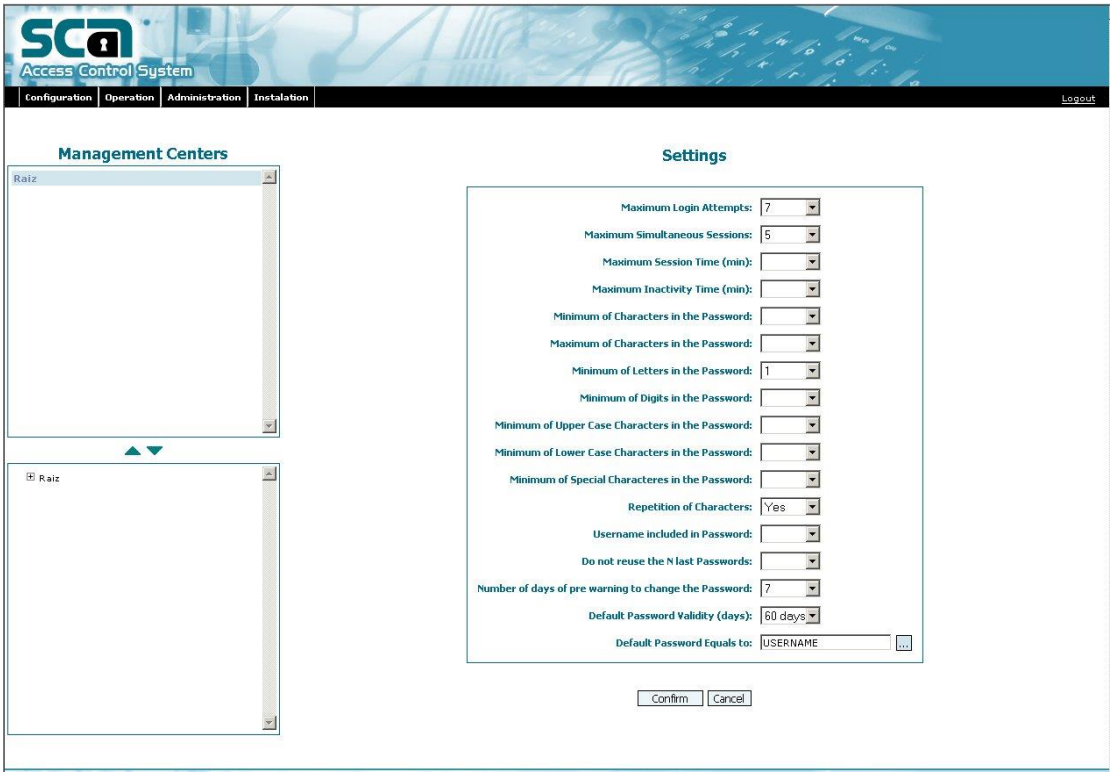
Cancel – cancel all changes made between the two lists. This button is only active if there are changes to validate or cancel.

Global Settings

By choosing the option Global Settings, it is possible to define, consult or modify the list of characteristics that are applicable to all users of a given management center. If the Root management center is selected, the characteristics displayed are those that apply to all users of the SCA unless they have more restricted configurations determined by their own management center or other centers at a higher level than the Root center.

Some of these characteristics can also be redefined in the user attributes form. In this way the Settings which are valid in the first instance are those defined for the user, followed by the management center which he/she belongs to and then successively those settings which have been defined for the centers which are hierarchically superior, up as far as the Root.

Figure 246. Global settings



Consult Global Settings

To consult the list of characteristics applicable to one or more management centers, select the needed items in the tree of the management centers and move them one by one to the list named Management Centers. If several are selected, it may not be possible to see all the information in the case, for example of there being differences for the same parameter between the selected centers. In this case a check box in front of the respective field tells that there are definitions that are not common to all the selected management.

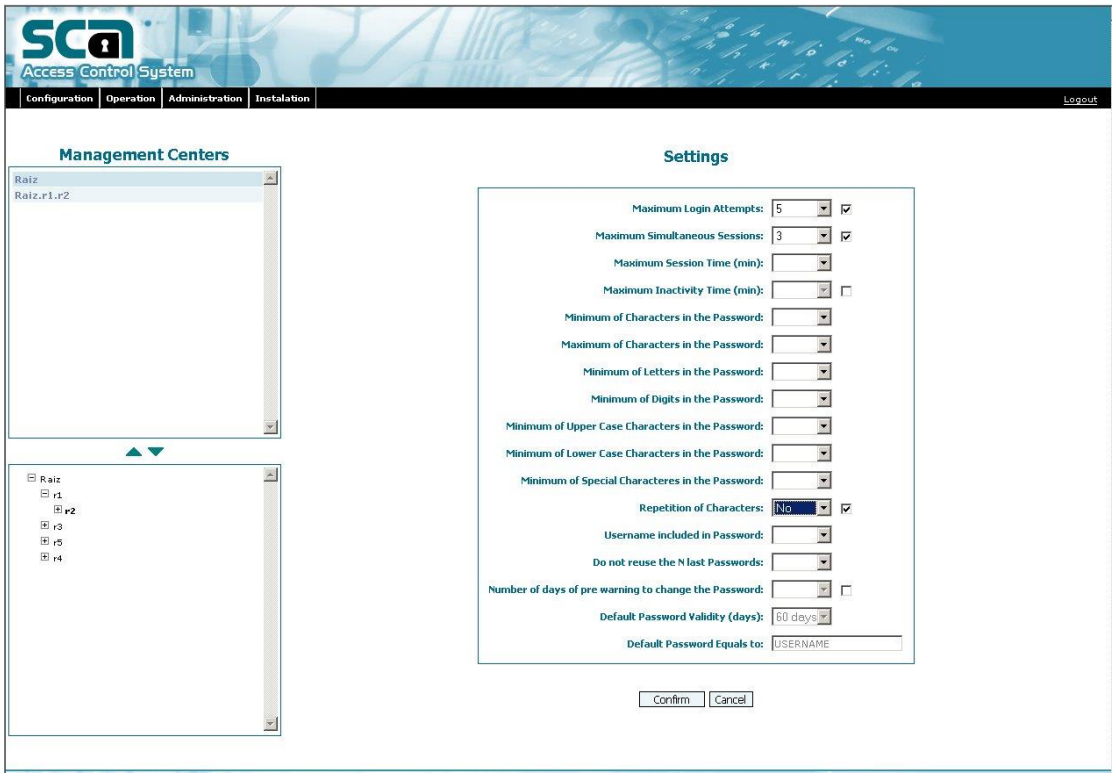
Define/Modify Global Settings

The process of defining for the first time or modifying the settings only differs if values already exist for a given parameter that is not the same for all the selected management centers. In that case, to re-define the value of the parameter for the whole group of selected centers, use the check box in front of the required field, to access the field where the new value can be inserted. This function can be used to specify which parameters are to be re-written in the database and which are to remain unaltered.

The last two settings, which refer to the validity and value of the default password, are defined only for the root management center.

The buttons Confirm and Cancel validate or cancel the actions taken.

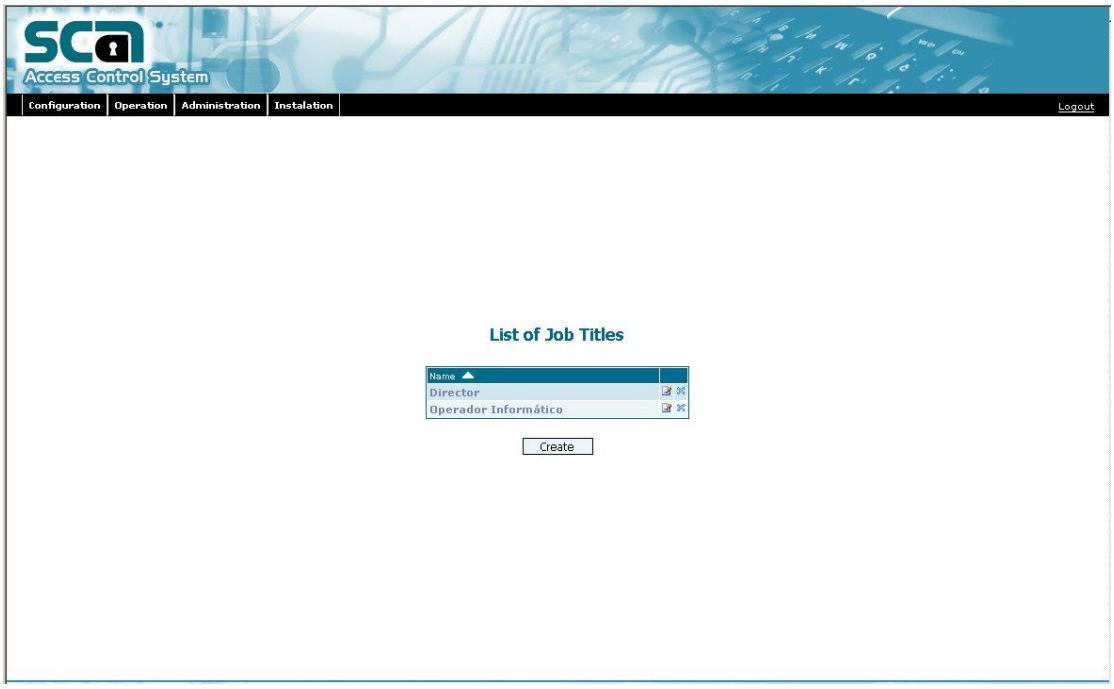
Figure 247. Define or modify global settings



Job Titles

By choosing the option Job Titles, all the job titles (or positions) already defined in the SCA are listed.

Figure 248. List of job titles / positions registered in the SCA



The possible commands are:

Create – creates a record of a new job title.

Modify – alters the name of a given job title.

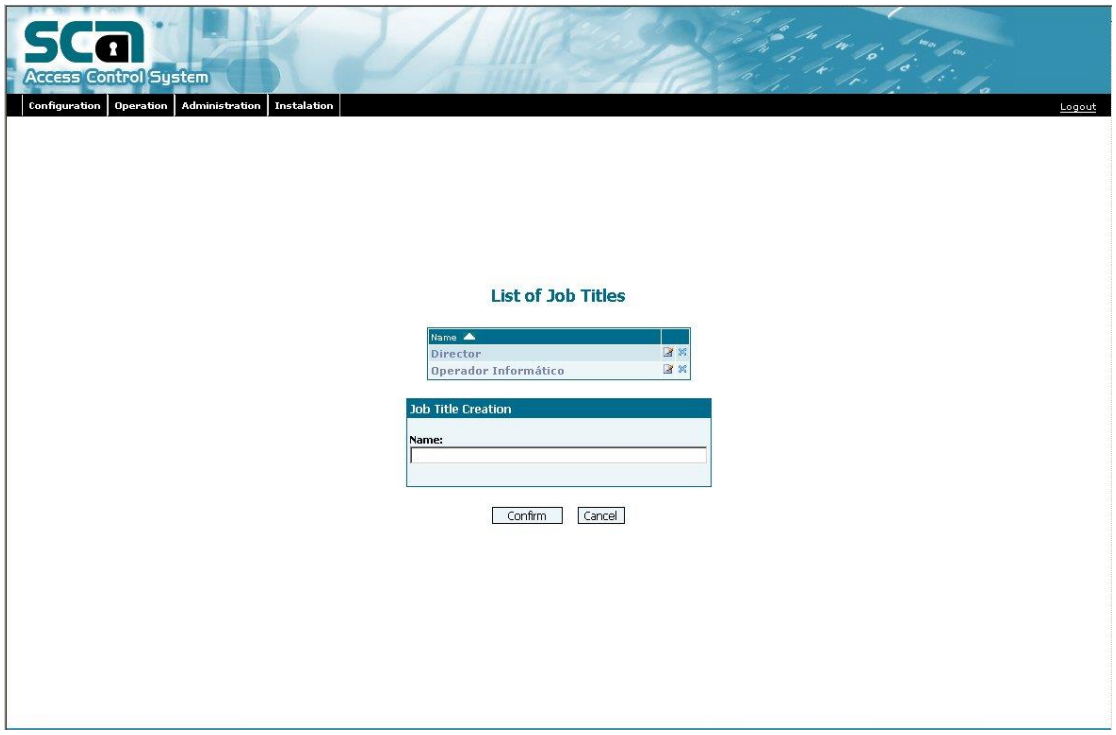
Remove – removes a job title from the SCA.

Details – allows viewing all the information about a job title. For that you must click the left button of the mouse on top of the job name.

Create / Modify Job Title

These two actions allow defining or modifying the name of the job.

Figure 249. Create/modify Job title



The Confirm and Cancel buttons confirm or respectively cancel any modifications made and then close the add information window.

Description of the Job title identifications fields:

Table 52. Job title

Field	M/O	Description
Name	M	Common name of the position/Job title, e.g. Operator

Remove Job Title

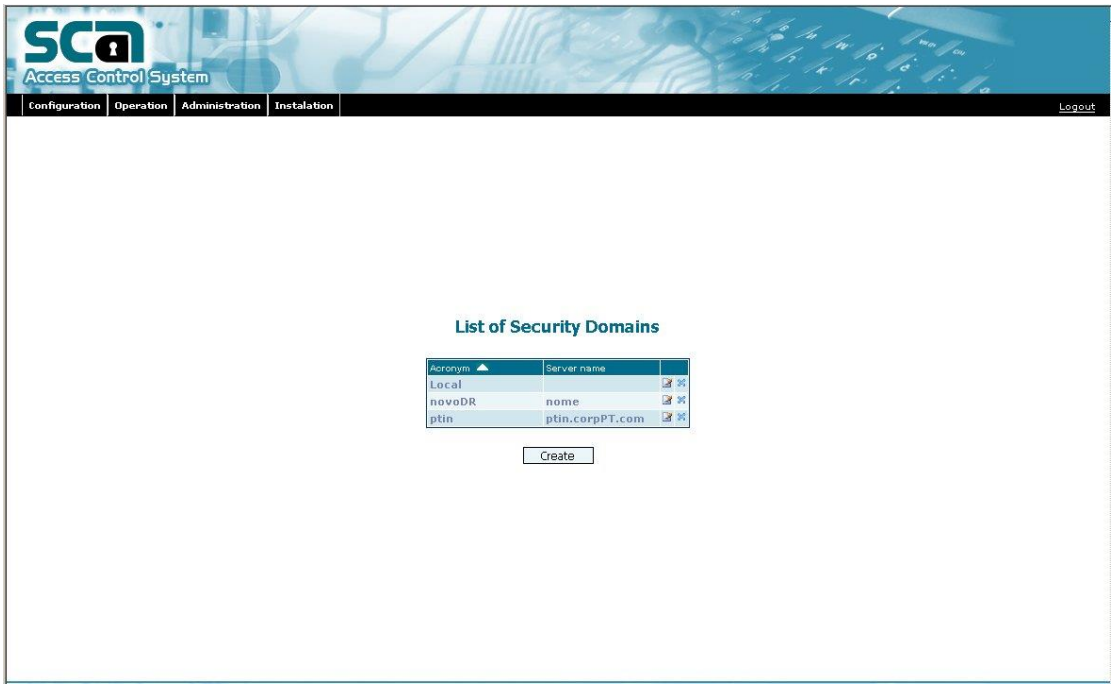
This action removes a job title provided it isn't assigned to any user. Simply press the remove button on the right of the required job register and then confirm the request in the confirmation window that appears.

Security Domains

By choosing the option **Security Domains**, all the security domains already defined in the SCA are listed.

By default there is always the local security domain, created during the SCA installation. This field cannot be removed because it is associated with the Manufacturer user, which also cannot be moved from the application.

Figure 250. List of security domains registered in the SCA



Four buttons provide access to the following actions:

Create – registers a new security domain.

Modify – modifies the attributes of a security domain.

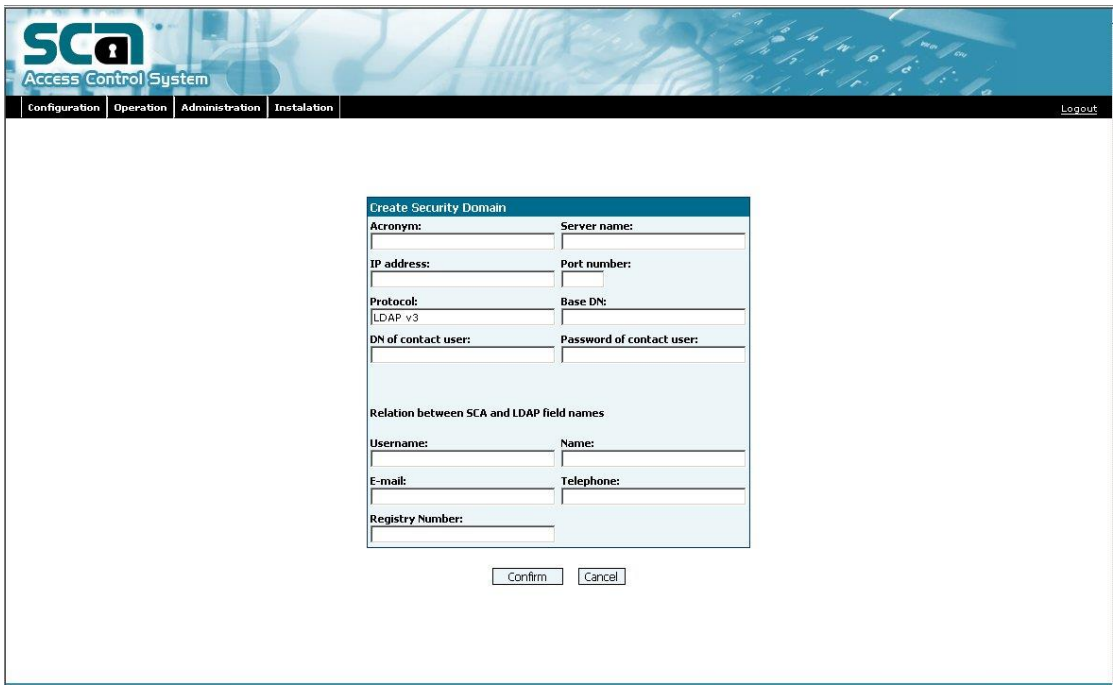
Remove – removes a security domain from the SCA.

Details – this allows consultation of all the information of the security domain. You must click the left button of the mouse on top on any field of the required registration.

Create/Modify Security Domain

These two commands provide access to a new page where you can define or modify the security domain characteristics.

Figure 251. Create/modify security domain



The Confirm and Cancel buttons confirm or cancel respectively any modifications and then close the input frame.

Description of the Security domain Identification Fields:

Table 53. Security domain

Field	M/O	Description
Acronym	M	Acronym of the security domain
Name of the Server	M	Name of the security domain server.
IP Address	M	IP Address of the security domain server.
Port Number	M	Port of access to the server by LDAP (e.g.: 389).
Protocol	M	Used protocol of communication (e.g. LDAP V3,....)
DN base	M	Distinguished Name of the server.
DN of the contact user	M	Distinguished Name of the contact user in the repository of the security domain.
Password of the contact user	M	Password of the contact user in the repository of the security domain.
Username	M	Name of the Username attribute in the security domain.
Name	O	Name of the Name attribute in the security domain.
E-mail	O	Name of e-mail attribute in the security domain.
Telephone	O	Name of the Telephone attribute in the security domain.
Registry Number	O	Name of the Registry Number in the security domain.

The filled last five attributes determine that every time users are imported from this domain their attributes will be imported ("User Attributes" section). The Username is the only attribute that is always imported, so is the only mandatory of these five attributes.

Remove Security Domain

This action removes a security domain which has no associated user. Simply press the remove button on the right of the required register and then confirm the request in the confirmation window.

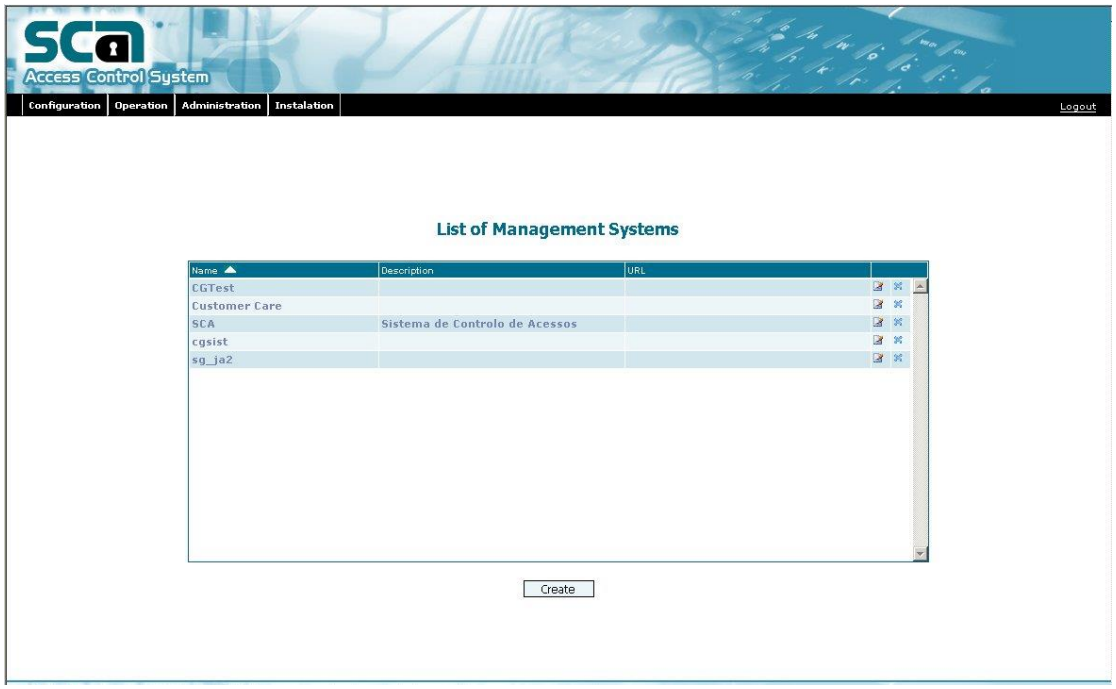
Installation Menu

This menu is made of the options Management Systems, Managed Domains, Access Types and Languages, which are described below.

Management Systems

By choosing the option Management Systems, a page shows where all the systems configured for the SCA are listed. Besides the name and description, the URL access to the system is also given.

Figure 252. List of the management systems registered in the SCA



Four buttons provide access to the following actions:

Create – registers a new management system in the SCA.

Modify – modifies the information associated with a management system.

Remove – removes a management system from the SCA.

Details – this allows consultation of all the information of a management system. You must click the left button of the mouse on top of any field of the required registration.

Create/Modify Management System

These actions provide access to a page containing four panels, each one showing a specific type of information associated with the management system:

Management System – identification attributes and way of access to the system;

Subsystems – lists the subsystems and intermediate points of the system;

Languages – lists the languages for the user's access to the system

MD Families – displays the managed domains families associated to the management system.

Each panel has its own validation (Confirm) and cancellation (Exit) buttons so that you can validate the new or modified information in one panel and cancel any modifications made in another panel.

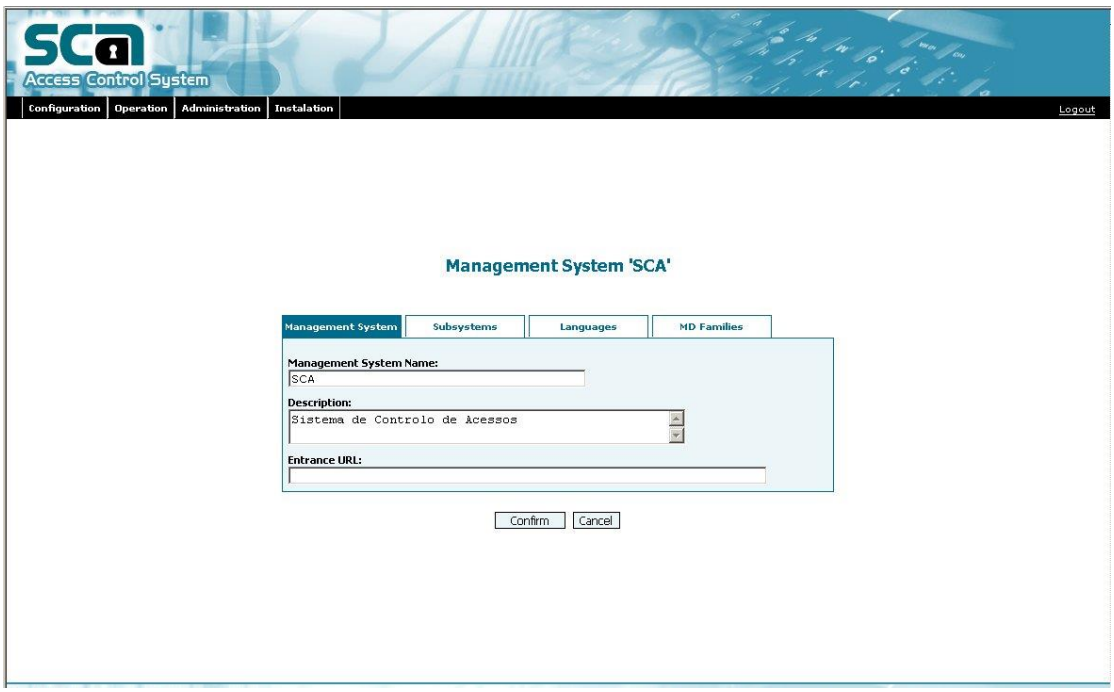
When creating a management system, the only panel that is obligatory to complete is the first (the one containing identification and way of access). Until this panel has not been validated, all the rest remain unavailable, that is, any attempt to change panels by clicking on its tab has no effect.

When you modify a management system, all the panels are active and user can navigate between them freely.

Management System

This panel displays the set of attributes that both identify and characterize the management system.

Figure 253. Management system identification page



The Confirm and Cancel buttons confirm or cancel respectively any changes made.

Description of the Management System Identification Fields:

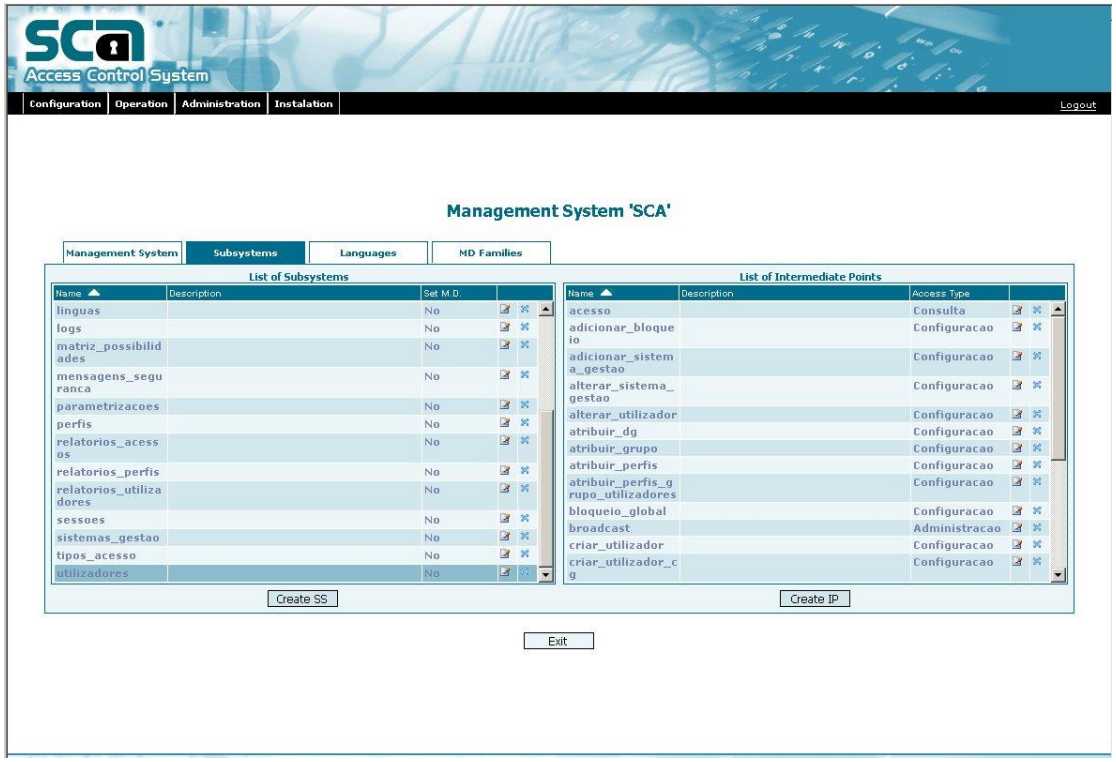
Table 54. Management system

Field	M/O	Description
Name of the Management System	M	Name of the management system
Description	O	Description of the management system
URL	O	Web address of the management system

Subsystems

This panel displays the list of the subsystems pertaining to the management system and, for each of them, a list of the intermediate points and respective access type.

Figure 254. List of SS and intermediate points of a management system



Possible actions are:

Create SS – creates a new subsystem for the current management system.

Modify SS – alters the identification characteristics of a subsystem.

Remove SS – removes a subsystem from the current management system.

Create IP – creates a new intermediate point in the current subsystem.

Modify IP – alters the access and identification characteristics of an intermediate point.

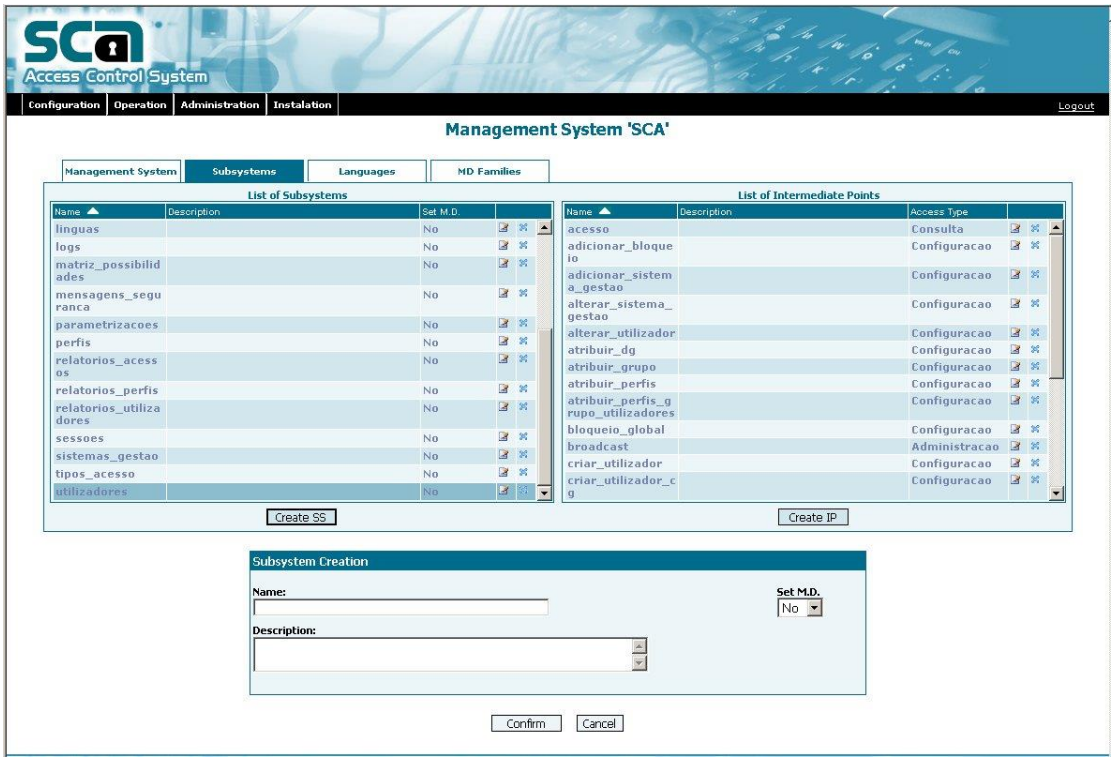
Remove IP – removes an intermediate point from the current subsystem.

Exit – returns to the list of all configured management systems.

Create/Modify Subsystem

These actions add a new window to the previous list of subsystems and intermediate points, in which you can define or modify the name and description of a subsystem as well as indicate whether a subsystem requires managed domains to be assigned.

Figure 255. Create/Modify subsystem



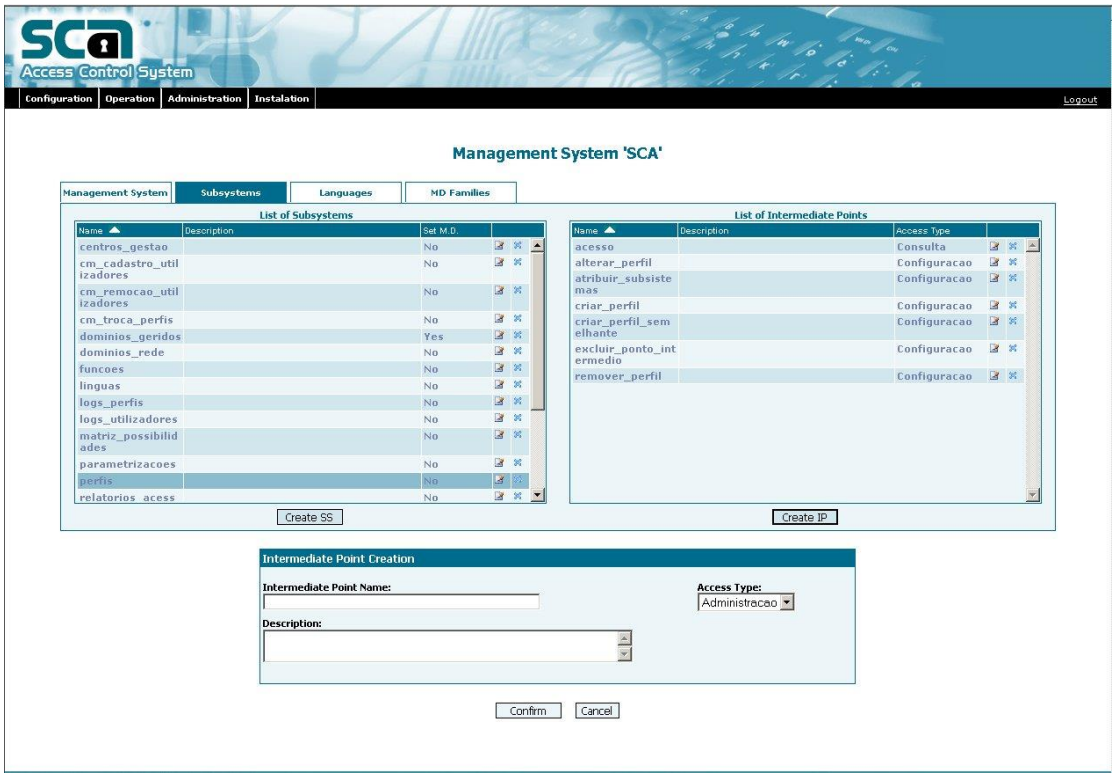
Remove Subsystem

This action removes a subsystem from the current management system. Just press the remove button on the right of the wanted subsystem and then confirm the request in the confirmation window. The existence of any entities associated (profiles, subsystems, languages, access type, etc.) will not prevent the removal if the operation is confirmed.

Create/Modify Intermediate Point

These actions add a new frame to the previous list of subsystems and intermediate points, in which you can define or modify the name and description of the intermediate point as well as minimum access type required.

Figure 256. Create/Modify intermediate point of a subsystem



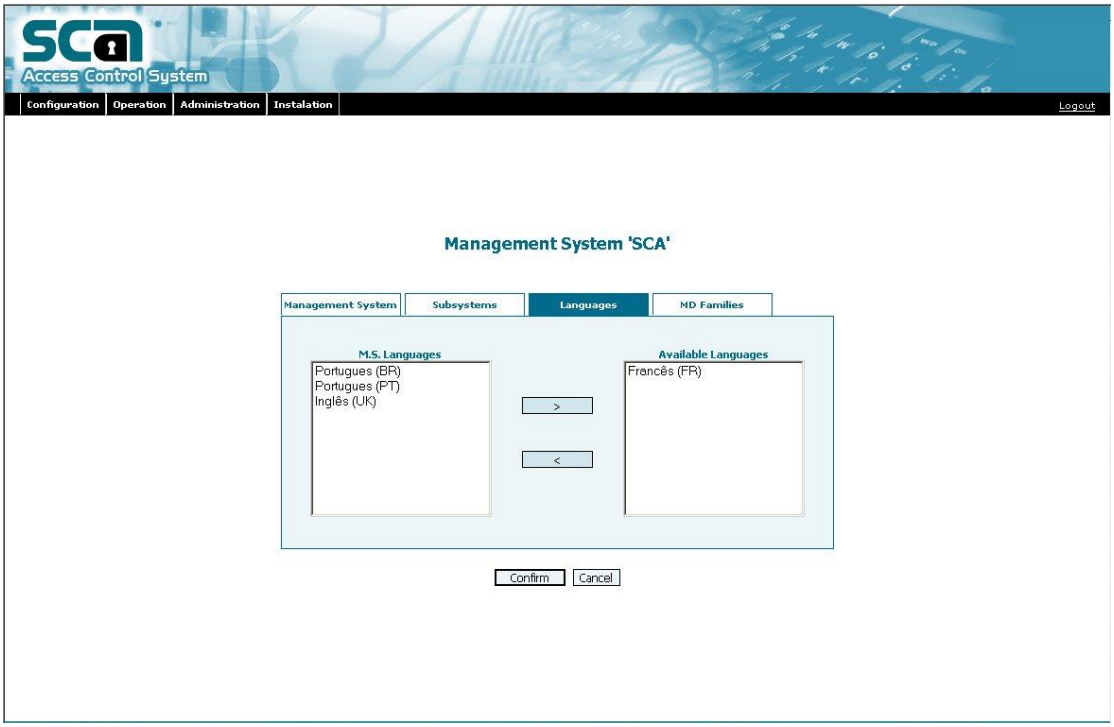
Remove Intermediate Point

This action removes an intermediate point from the current subsystem. Just press the remove button on the right of the wanted intermediate point and then confirm the request in the confirmation window.

Languages

This panel displays two Lists: on the left are the languages assigned to the management system and on the right are the available languages.

Figure 257. Assigning languages to the management system



Possible actions are:

'>' or '<' – move the languages selected from one list to the other; use the keys SHIFT + mouse and CTRL + mouse for multiple item selection.

Confirm – validates the changes made between the two lists and returns you to the page showing the management system list.

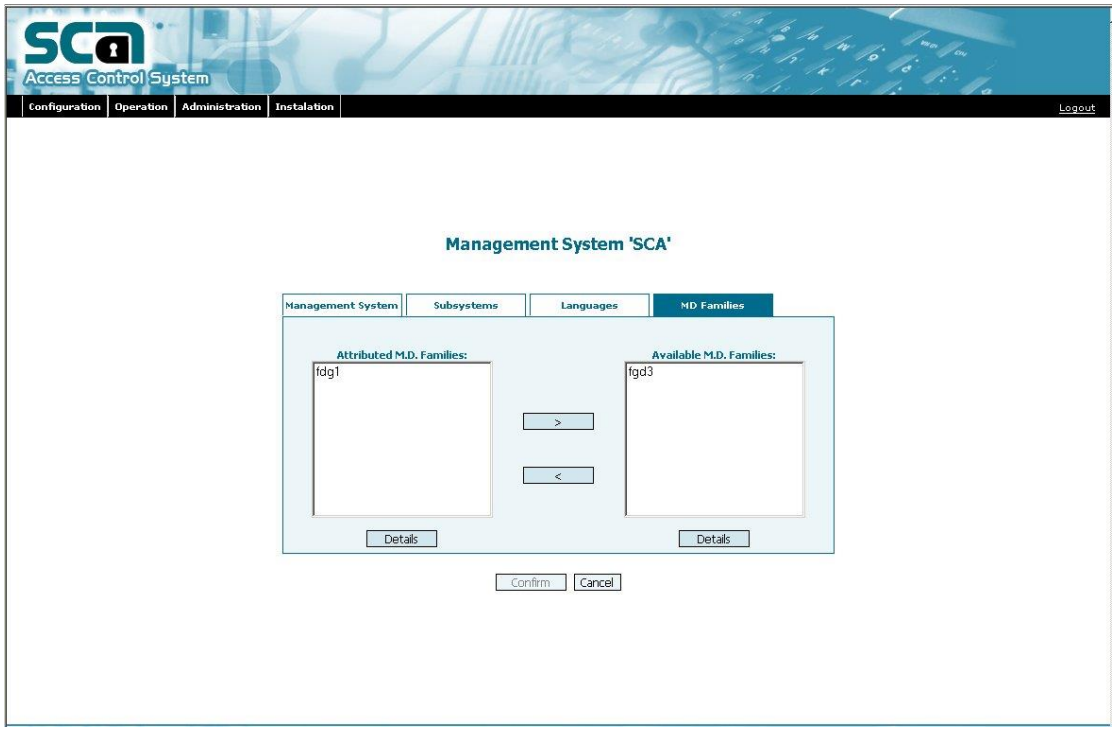
Cancel – cancels any changes made between the two lists and returns you to the page showing the management system list

MD Families

This panel displays two lists of the managed domains families: on the left are the families assigned to the management system and on the right are the available families.

If there are not shareable managed domains families assigned to the system in question these are displayed in a separate list, also on the left. This list is inaccessible, as all the not shareable managed domains families and only be assigned or removed in the management system itself, and can only be viewed in the SCA.

Figure 258. Assign MD families to the management system



Possible actions are:

'>' or '<' – move the selected managed domains families from one list to the other; use the keys SHIFT + mouse and CTRL + mouse for multiple item selection.

Details – shows the managed domains of a given family.

Confirm – validates the changes made between the two lists and returns to the page showing the management system list.

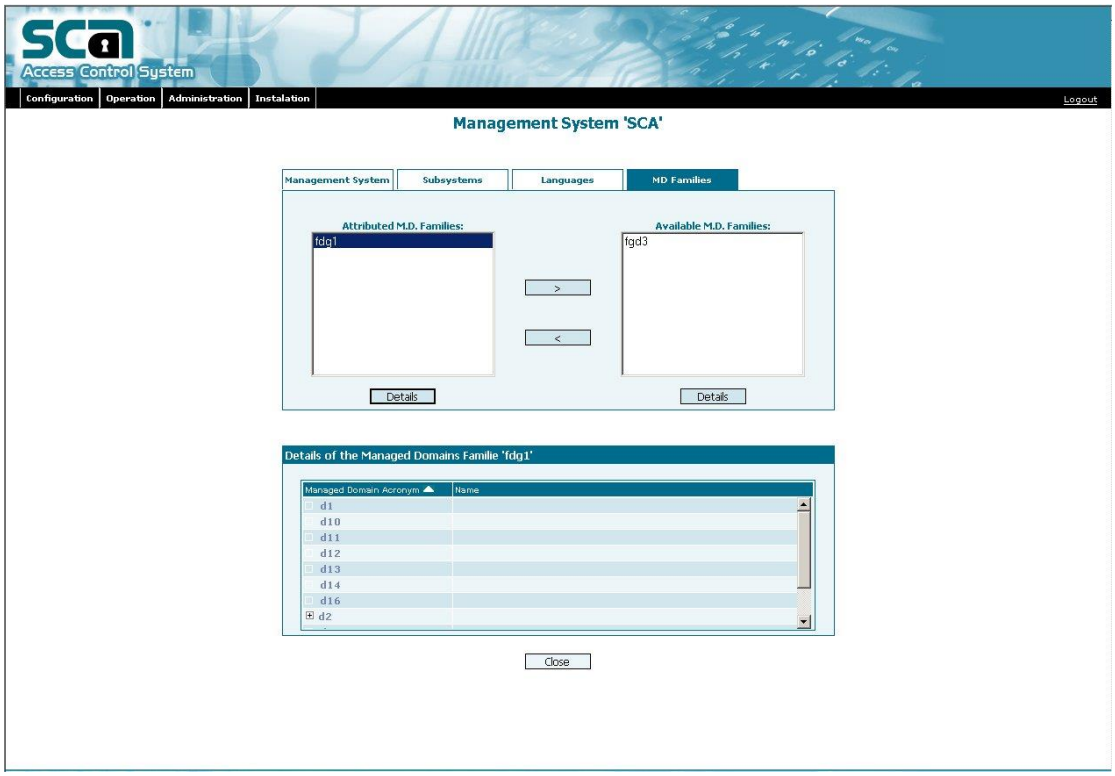
Cancel – cancels any changes made between the two lists and returns you to the page showing the management system list.

View Details of a Managed Domains Family

On the page where managed domains families are assigned to management systems, selecting an MD family in any of the lists and then pressing the Details button will show a window where you can view that family's managed domains.

The way to view the managed domains is fragmentary, e.g. the managed domains which belong to the same level are displayed on the list. If a domain has got dependent ones, pressing the sign '+' behind the acronym will cause his expansion and it displays the domains which belong to level below. As the levels of the tree are opened, the followed way is shown at the top of the details window.

Figure 259. View managed domains of a given MD family



Remove Management System

To remove a management system, simply press the remove button on the page which displays the management system list (Figure 250). This action, after due confirmation in the confirmation window, is only carried out if there are no associations with (users, profiles, etc.) in the management system. The association of any users with the management system prevent their removal, while the existence of any other entities associated (profiles, subsystems, languages, access type, etc.) will not prevent the removal if the operation is confirmed.

Managed Domains

Choosing the option **Managed Domains** gives access to a page with two panels:

MD Families – to list and configure the managed domains families;

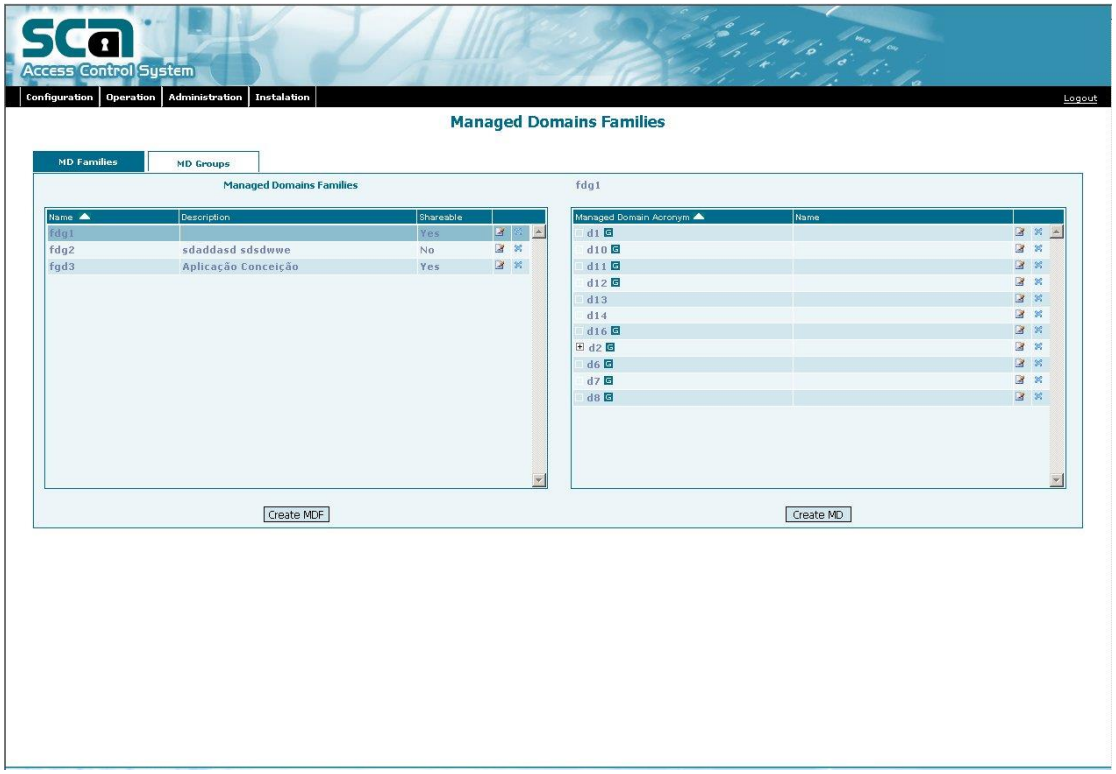
MD Groups – to list and configure managed domains groups, whether these are made up of managed domains from one or several families.

MD Families

In this panel appear all the managed domains families registered in the SCA, and a respective list of managed domains for each of them. Apart from the name and description of each family there is information about whether it is shareable with other managements systems.

This concept of sharing is only possible for the managed domains families created in the SCA, as opposed to those that are created in the context of an application (management system) and stored in the SCA repository.

Figure 260. List of managed domains families



Selecting a managed domains family shows on the right the hierarchy of its managed domains. The way to view the hierarchy of managed domains is fragmentary, e.g. the managed domains are displayed on the list of the managed domains families which belong to the same level. If a domain is independent, pressing the sign '+' behind the acronym the level will expand and move to show the domains of the level below. As the levels of the tree are opened, the path followed is shown at the top of the window.

By placing the mouse over this symbol you can see the information about the groups to which it belongs.

Possible actions are:

Create MDF – creates a new managed domains family.

Modify MDF – modifies the information associated to a managed domains family.

Remove MDF – removes a managed domains family.

Create MD – creates a managed domain.

Modify MD – modifies a managed domain.

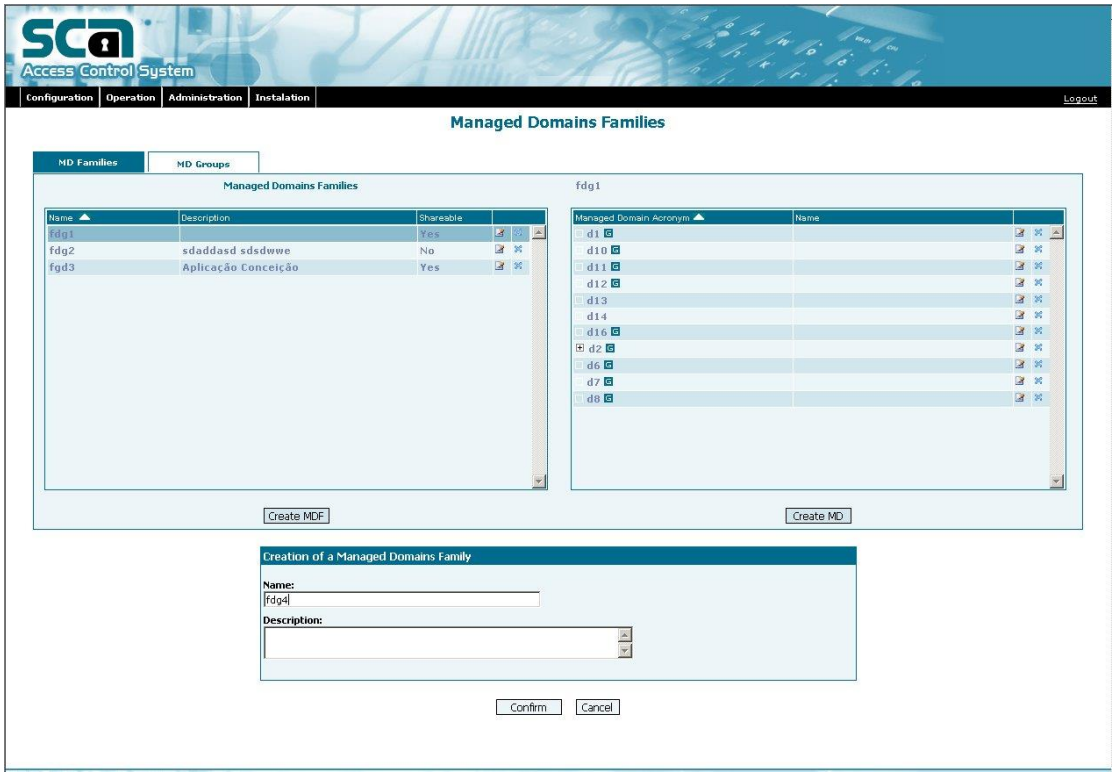
Remove MD – removes a managed domain.

Create/Modify MD Family

These actions take you to a new page where a new window appears for you to define or modify the name and description of a managed domains family.

The symbol for a shared family by various management systems is automatically set to 'Yes' and is not alterable. The only not-shareable families are the ones created in the management systems themselves and made known to the SCA for storage purposes and to assign to the users.

Figure 261. Create/Modify a MD family



The Confirm and Cancel buttons confirm or cancel respectively the changes made and close the insert window.

Description of the fields in the MD family identification form:

Table 55. MD family

Field	M/O	Description
Managed Domains Family Name	M	Name of managed domains family
Description	O	Description of the managed domains family

Remove MD Family

This action removes a managed domains family. Simply press the remove button on the right of the wanted family and confirm the request in the confirmation window.

Restrictions to the Remove command:

Only remove a managed domains family that does not contain any managed domains;

Only remove a managed domains family that isn't associated with any management system.

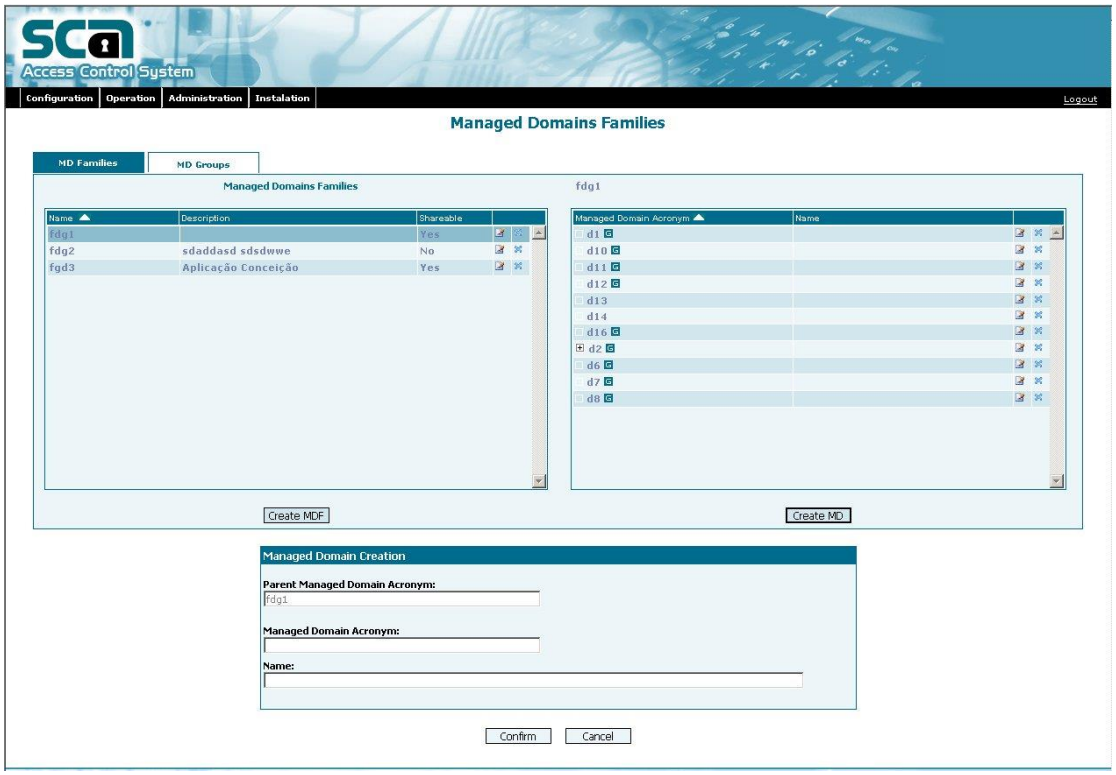
Only remove a managed domains family that is sharable.

Create/Modify Managed Domain

To create a managed domain you must open the level where you want to put the new domain. If you wish to modify information about the MD, press the edit button associated with the register.

These actions open a new page with a new window in which you can define or modify the acronym and the name of the managed domain.

Figure 262. Create/Modify a managed domain



The Confirm and Cancel buttons confirm or cancel respectively the changes made and close the insert window.

Description of the file identification fields of a managed domain:

Table 56. Managed domain

Field	M/O/A	Description
Managed Domain Acronym	M	Abbreviated name of a managed domain, this being what is displayed in the MD tree
Managed Domain Name	O	Full name of a managed domain
Upper Level Managed Domain Acronym	A	Parent managed domain. This cannot be changed

Remove Managed Domain

This action removes a managed domain. Simply press the remove button on the right of the wanted managed domain and confirm the request in the confirmation window.

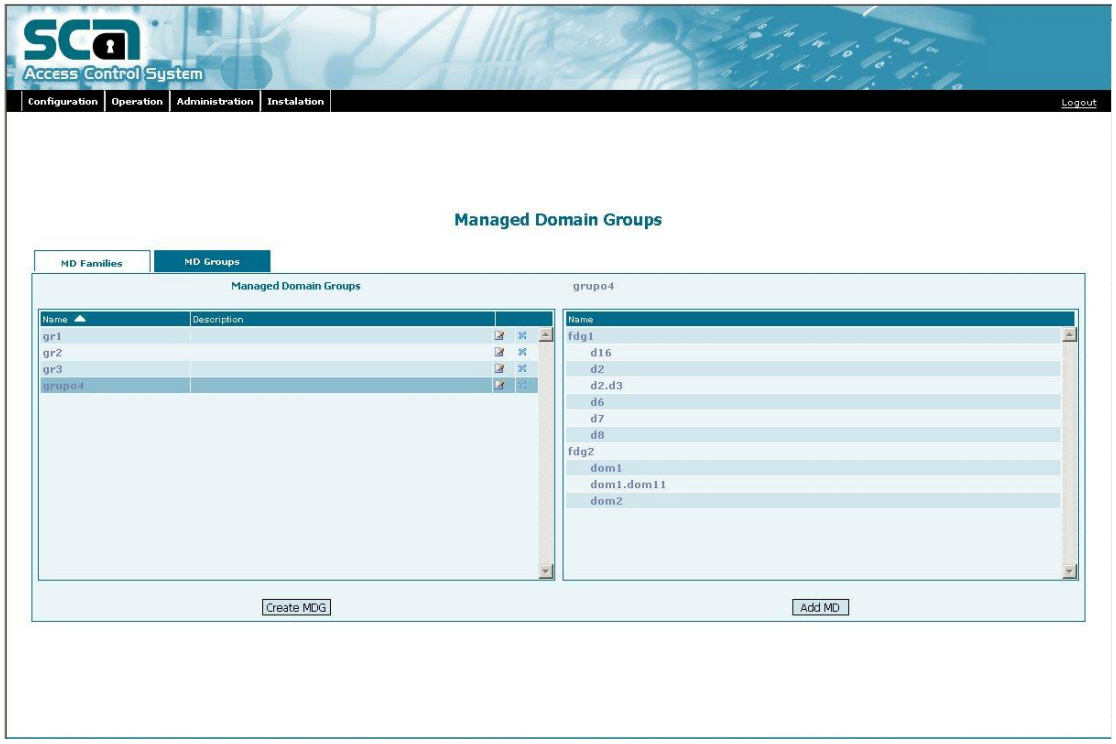
Restrictions to the Remove command:

- Only remove a managed domain that isn't associated with any users.
- Only remove a managed domain that does not have any managed domains hierarchically dependent on it.

MD Groups

In this panel are displayed all managed domains groups registered in the SCA and for each one selected the respective structure in terms of managed domains, organized by families is also displayed on the right side.

Figure 263. List of managed domains groups



Possible actions are:

Create MDG – creates a new MD group.

Modify MDG – modifies information associated to an MD group.

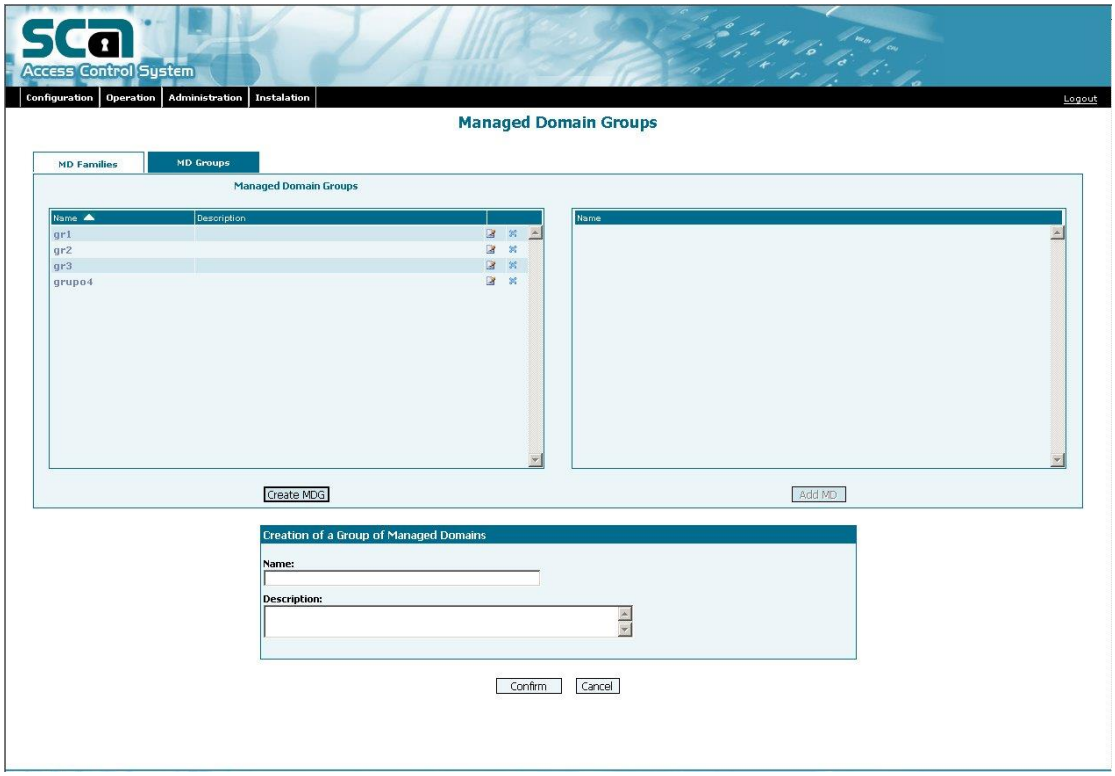
Remove MDG – removes an MD group.

Assign MDs – alters de composition of a group, by assigning or de-assigning managed domains to the selected group.

Create/Modify MD Group

These actions open a new page to define or modify the name and description of the MD group.

Figure 264. Create/Modify managed domains group



The Confirm and Cancel buttons confirm or cancel respectively the made changes and close the insert window.

Description of the fields of the identification form of the MD group:

Table 57. MD group

Field	M/O	Description
Managed Domains Group Name	M	Name of the managed domains group
Description	O	Description of the managed domains group

Remove MD Group

This action removes an MD group. Simply press the remove button on the right of the wanted MD group and confirm the request in the confirmation window.

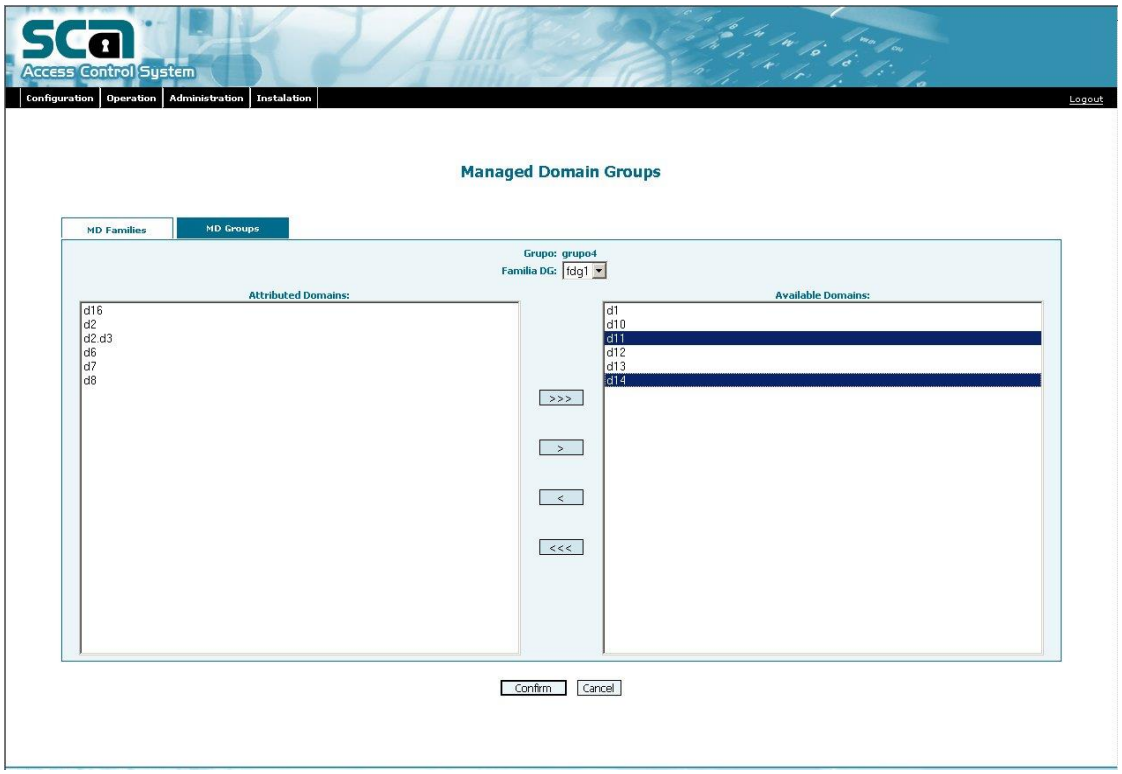
Restrictions on the remove process:

- Only possible to remove an MD group that isn't assigned to a user.

Assign MDs

This action opens a page where two lists are displayed for each MD selected at the top: the one on the left shows the managed domains already assigned to the group, arranged in their respective families; the one on the right shows the list of existing managed domains families, available to be assigned to the group.

Figure 265. Assign managed domains to a group



Possible actions are:

'>' or '<' – to move the selected domains from one list to the other; use the keys SHIFT + mouse and CTRL + mouse for multiple item selection.

'>>>' and '<<<' – to move all the domains from one list to the other.

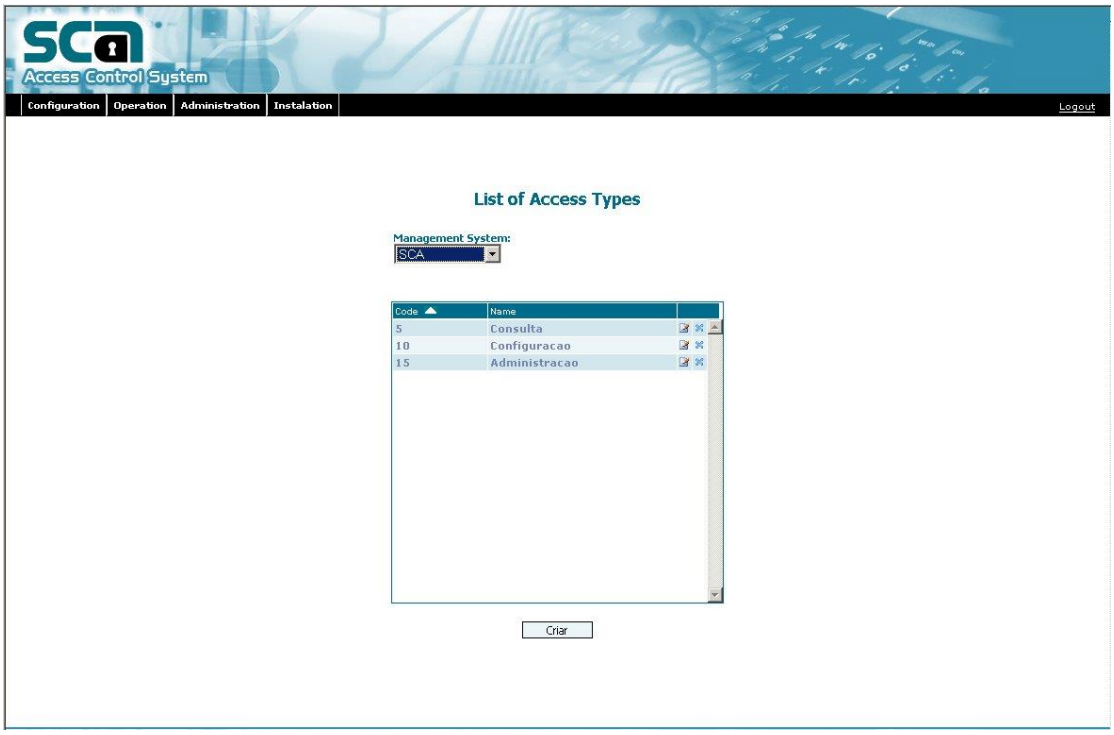
Confirm – validates the changes made between the two lists and returns to the previous page.

Cancel – cancels the changes made between the two lists and returns to the previous page.

Access Types

By choosing the Access Types option you are shown a page listing all access types already defined in the SCA for one given management system.

Figure 266. List of the access types by management system



Possible actions are:

Create – creates a new access type.

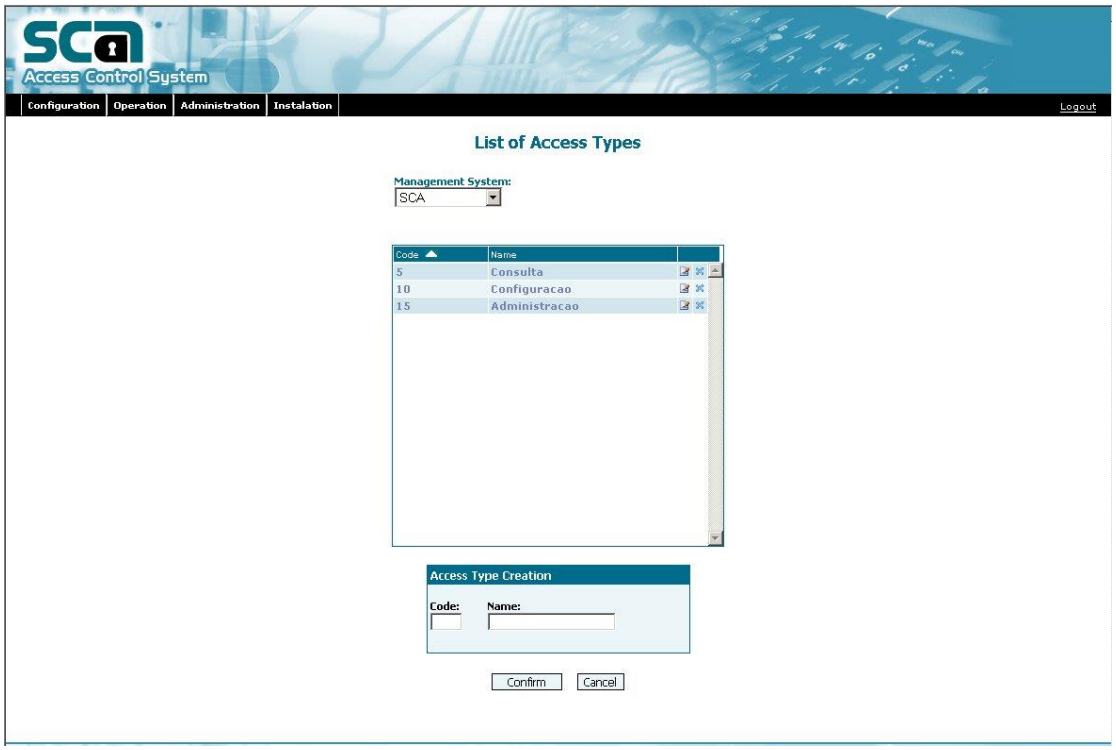
Modify – modifies the name of the access type.

Remove – removes an access type.

Create/Modify Access Type

These actions open a page with a window to define or modify the access type.

Figure 267. Create/Modify Access type



The Confirm and Cancel buttons confirm or cancel respectively the changes made and close the insert window.

Description of the fields of the identification form for the access type:

Table 58. Access type

Field	M/O	Description
Code	M	Numerical identification code for the access type. The higher the code the higher the access privileges.
Name	O	Name associated to the access type, e.g.: viewing, administration, etc.

Remove Access Type

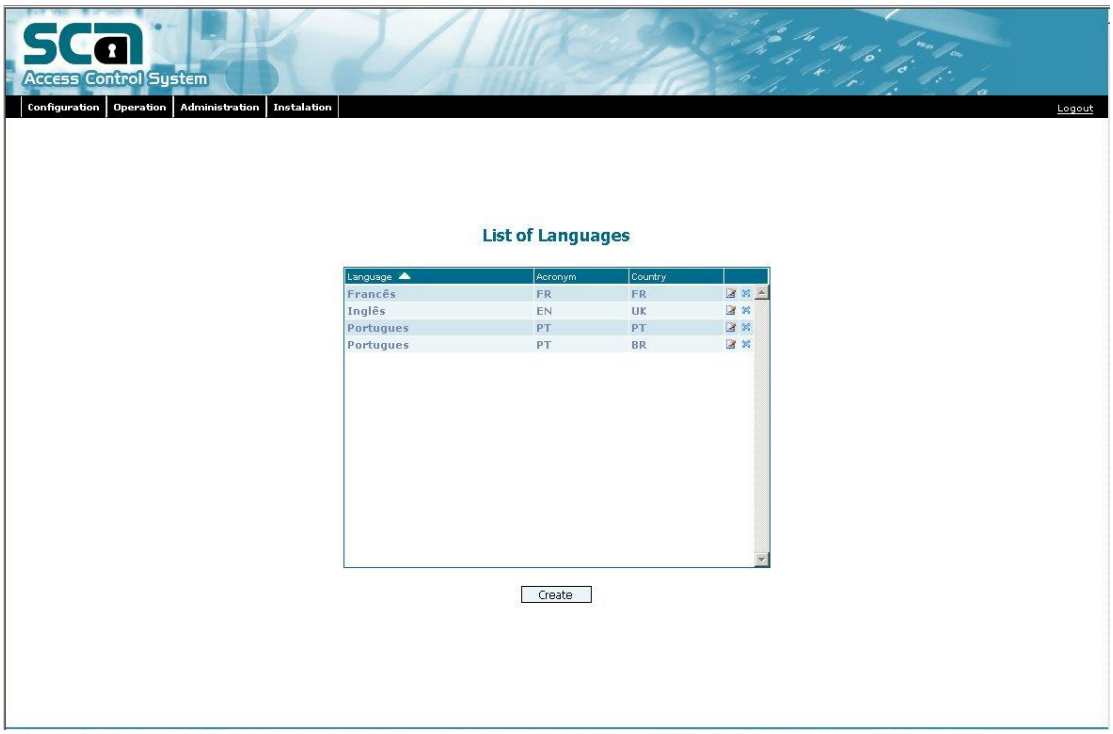
This action removes an access type provided if it isn't assigned to a profile or any Intermediate point. Simply press the remove button on the right of the wanted access type and confirm the request in the confirmation window that pops up.

Languages

- **Cisco Template**

By choosing the option Languages you are shown a page where all the languages defined in the SCA are listed.

Figure 268. List of the languages registered in the SCA



Possible actions are:

Create – creates the register of a new language.

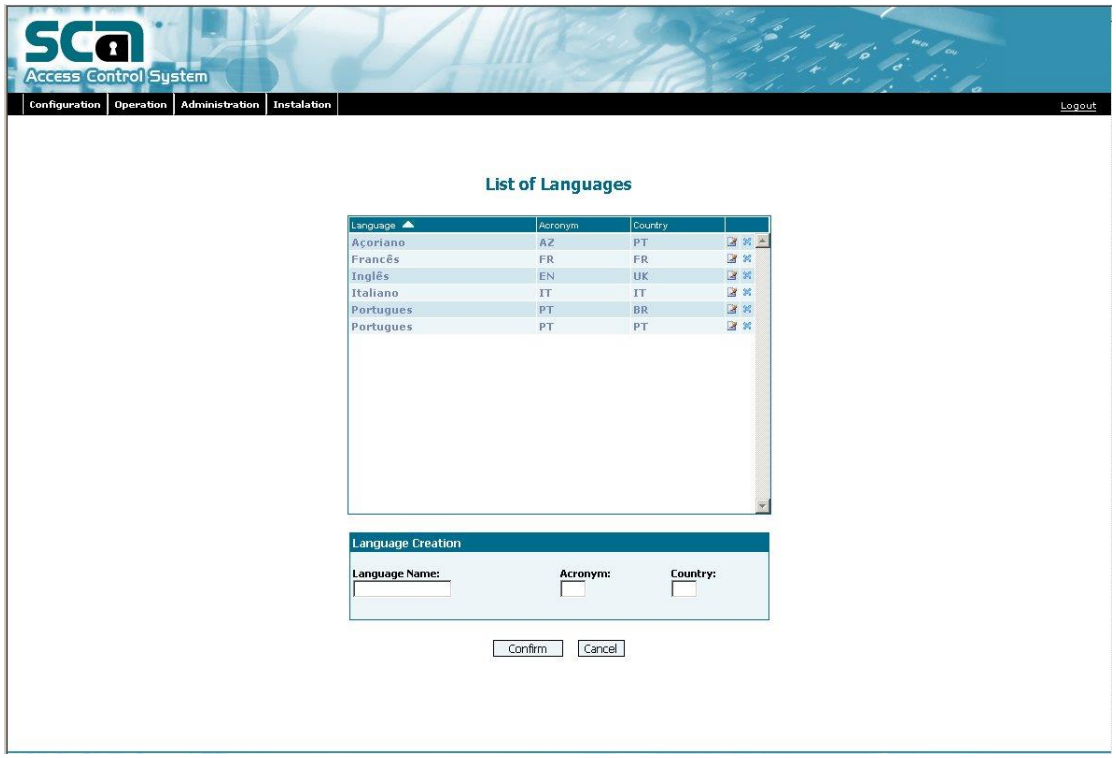
Modify – modifies the information associated to a language.

Remove – removes a language from the SCA.

Create/Modify Language

These two actions open up a page where a new window appears allowing you to define or modify the language characteristics.

Figure 269. Create/Modify language



The Confirm and Cancel buttons confirm or cancel respectively the changes made and close the insert window.

Description of the fields of the language identification form:

Table 59. Language identification

Field	M/O	Description
Language Name	M	Usual name of the language, e.g.: “Portuguese”
Acronym	M	Short name associated to the language, e.g.: “PT”.
Country	O	Acronym of the country where the language is spoken, e.g.: “PT”.

Remove Language

This action removes a language provided it isn’t assigned to a management system or a user as the language of preference. Simply press the remove button on the right of the wanted language and confirm the request in the confirmation window that pops up.

Subsystems and Intermediate Points of the SCA

This chapter explains all about the subsystems, intermediate points and access types defined for the administration application of the SCA. This data is static, considering the client cannot alter it.

The configuration of these elements is done prior to the creation of the SCA's users and their respective access rights. It must be done by a special user, called "Builder", identified on the application since the first moments of the pre-exploitation phase, i.e. while the application is prepared to be deployed on the client's systems. This "Builder" will have to register on the SCA the SCA management system itself and all of its subsystems, before creating the user profiles, the first users, and assign the adequate access rights to the future operational users of the SCA system.

Access Types

According to the specific needs of the SCA, three access types have been identified, described her in growing privilege order:

- **Viewing**: profiles with this access type can only view the available information on the administration application. No changes are permitted.
- **Configuration**: profiles with this access type can perform normal configuration operations, like management of profiles and users.
- **Administration**: with this access type, the users are able to perform administration tasks like the definition of management centers or the modification in the possibilities matrix and general parameters.

Pseudo-Access Type of the "Builder"

This could be considered as a fourth and maximum level access type, as it actually corresponds to the privilege associated with the "Builder" user. However, this access type cannot be configured nor assigned to any intermediate point or profile. There are in fact intermediate points that can only be accessed to by the "Builder", but as they will never be associated to any profile, there is no need to register them on the system. These are identified internally as virtual intermediate points, subject to a particular access control procedure: instead of being validated against the required access right, the comparison is done with the current "Builder" user.

Subsystems and Intermediate Points

Considering the Web technology used by the SCA administration application, all the subsystems must include an "access" intermediate point to control the access to the main page from which the program features are reached, themselves controlled by the other intermediate points.

The following tables show all the SCA's subsystems, their intermediate points and corresponding required minimal access rights levels. Note that the intermediate points requiring "Builder" access type only exist in theory, and they do not need to be registered.

Subsystem: users

Table 60. Users subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing the users information
criar_utilizador	Configuration	Create user
criar_utilizador_semelhante	Configuration	Create similar user
criar_utilizador_cg	Configuration	Create user of any management system
alterar_utilizador	Configuration	Modify user
remover_utilizador	Configuration	Remove user
adicionar_sistema_gestao	Configuration	Add management system to user
alterar_sistema_gestao	Configuration	Update the association between management system and user
retirar_sistema_gestao	Configuration	Remove management system from user
atribuir_perfis	Configuration	Add and remove user's profiles
atribuir_dg	Configuration	Add and remove managed systems from user
excesso_tentativas	Configuration	Reset a user's failed attempts counter
bloqueio_global	Configuration	Lock or unlock a user
adicionar_bloqueio	Configuration	Create a lock to a user
retirar_bloqueio	Configuration	Remove a lock to a user

desbloquear_login	Configuration	Unlock user who has a expired login
desbloquear_password	Configuration	Unlock user who has a expired password
reset_password	Configuration	Reset password of a group of users
broadcast	Configuration	Send an e-mail to a users group
atribuir_grupo	Configuration	Assign managed domains groups to a user or a group of users
atribuir_perfis_grupo_utilizadores	Configuration	Assign profiles, managed domains and managed domains groups to a users group

N.B.: The intermediate points criar_utilizador and criar_utilizador_cg actually correspond to the same intermediate point within the application. The difference between them is the list of management centers available to assign to a new user, i.e. if the current user has been assigned the first of these two intermediate points, he will only be able to assign his own management center or one hierarchically depending on that one to the new user, whereas if he has been assigned the second intermediate point he will be able to assign any management center to the new user. He actually can have been assigned both of them.

Subsystem: perfis

Table 61. Perfis subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing the profile information
criar_perfil	Configuration	Create a profile
criar_perfil_semelhante	Configuration	Create a profile like another that already exists
alterar_perfil	Configuration	Modify a profile
remover_perfil	Configuration	Delete a profile
atribuir_subsistemas	Configuration	Add/remove subsystem to/from a profile
excluir_ponto_intermedio	Configuration	Include/exclude intermediate points to/from a profile

Subsystem: cm_cadastro_utilizadores

Table 62. cm_cadastro_utilizadores subsystem

Name	Access Type	Description
acesso	Configuration	It allows the mass introduction of users by loading a file with the necessary data

Subsystem: cm_remocao_utilizadores

Table 63. cm_remocao_utilizadores subsystem

Name	Access Type	Description
acesso	Configuration	It allows the mass removal of the users by loading a file with the necessary data

Subsystem: cm_troca_perfis

Table 64. cm_troca_perfis subsystem

Name	Access Type	Description
acesso	Configuration	It allows the Exchange of profiles to mass users through the upload of a file with the necessary data

Subsystem: logs_utilizadores

Table 65. logs_utilizadores subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing the user logs

Subsystem: logs_perfis

Table 66. logs_perfis subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing the profile logs

Subsystem: relatorios_utilizadores

Table 67. relatorios_utilizadores subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing the users reports

Subsystem: relatorios_perfis

Table 68. relatorios_perfis subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing the profiles reports

Subsystem: relatorios_acessos

Table 69. relatorios_acessos subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing the Access reports

Subsystem: sessoes

Table 70. sessoes subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing of open sessions and relative information
fechar_sessao	Administration	Close session

Subsystem: centros_gestao

Table 71. centros_gestao subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing information about the management centers
criar_centro_gestao	Administration	Create a management center
alterar_centro_gestao	Administration	Modify a management center
remover_centro_gestao	Administration	Delete a management center

Subsystem: matriz_possibilidades

Table 72. matriz_possibilidades subsystem

Name	Access Type	Description
Acesso	Viewing	Allows viewing information about the possibilities matrix
alterar_matriz	Administration	Modify the possibilities matrix

Subsystem: parametrizacoes

Table 73. parametrizacoes subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing settings
alterar_parametrizacoes	Administration	Modify settings

Subsystem: funcoes

Table 74. funcoes subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing user's position and duties
criar_funcao	Administration	Create new position / duty / job title
alterar_funcao	Administration	Modify position / duty
remover_funcao	Administration	Delete position / duty

Subsystem: dominios_rede

Table 75. dominios_rede subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing information about security domains
criar_dominio_rede	Administration	Create security domain
alterar_dominio_rede	Administration	Modify security domain
remover_dominio_rede	Administration	Remove security domain

Subsystem: sistemas_gestao

Table 76. sistemas_gestao subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing information about management systems
criar_sistema_gestao	Builder	Create management system
alterar_sistema_gestao	Builder	Modify management system
remover_sistema_gestao	Builder	Delete management system
adicionar_lingua	Builder	Add language to a management system
retirar_lingua	Builder	Delete language from management system
criar_subsistema	Builder	Create subsystem
alterar_subsistema	Builder	Modify subsystem
remover_subsistema	Builder	Delete subsystem
criar_ponto_intermedio	Builder	Create intermediate point
alterar_ponto_intermedio	Builder	Modify intermediate point
remover_ponto_intermedio	Builder	Delete intermediate point
adicionar_familia_dg	Builder	Add managed domains family to a management system
retirar_familia_dg	Builder	Remove managed domains family from a management system

Subsystem: dominios_geridos

Table 77. dominios_geridos subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing information about managed domains families
criar_familia_dg	Builder	Create managed domains family
alterar_familia_dg	Builder	Modify managed domains family
remover_familia_dg	Builder	Delete managed domains family
criar_dominio_gerido	Builder	Create managed domain
alterar_dominio_gerido	Builder	Modify managed domain
remover_dominio_gerido	Builder	Delete managed domain
criar_grupo	Administration	Create managed domains group
alterar_grupo	Administration	Modify managed domains group
remover_grupo	Administration	Delete managed domains group
atribuir_dg_grupo	Administration	Assign managed domains to managed domains group

Subsystem: tipos_acesso

Table 78. tipos_acesso subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing information about the access types
criar_tipo_acesso	Builder	Create access type
alterar_tipo_acesso	Builder	Modify access type
remover_tipo_acesso	Builder	Delete access type

Subsystem: linguas

Table 79. linguas subsystem

Name	Access Type	Description
acesso	Viewing	Allows viewing information about available languages
criar_lingua	Builder	Create language
alterar_lingua	Builder	Modify language
remover_lingua	Builder	Delete language

SCA Profiles

The SCA application is prepared with three basic user profiles, one for each access type. The client is free to use, modify or delete these profiles, or even create new ones.

This chapter describes the profiles and their associated subsystems. The access to a subsystem implies viewing its information pages, but does not necessarily require the access to the intermediate points of the system. This is the case with intermediate points that are only available to the “Builder”, or those requiring a higher level of access rights than the ones corresponding to the profile of the current user.

Table 80. SCA profiles

Name	Description	Subsystems
Administration (Administração)	Profile of users with extended configuration responsibilities at top organizational level: configuration of management centers, possibilities matrix and global settings.	All
Configuration (Configuração)	Profile of users with configuration responsibilities at operational level: profiles management, users management and their access rights.	All
Viewing (Consulta)	Profile of users only with viewing access rights.	All

"Builder" User

Requirements for the "Builder" User

The general requirements for the “Builder” user are the following:

- The “Builder” user should not be visible to the SCA administration application
- Not being a normal user, the “Builder” should be able to access the administration application, either directly or through a portal, after normal authentication on the login screen.
- It is not possible to perform auto-destructive operations, i.e. the “Builder” cannot delete himself or reduce his own access rights.

Implemented Solution for the "Builder" user

The central idea of the solution is to consider the “Builder” as an identified user. If this user is given the ID code 0 (zero), the application can assume he is the “Builder” and give him full and unrestricted access rights to the application.

There is no risk to create another “Builder” user, as the sequence of ID codes for users created with the administration application start with 1 (one).

All the users must be part of a management center (constraint associated to the table of users), and the same applies to the “Builder” user who is part of the management center with ID 1 (one), corresponding to the root of the management centers tree.

If the “Builder” is expected to access the administration application through the portal, the user with ID code 0 has also to be associated with the SCA management system in the appropriate database table. Supposing that the SCA application is initially registered in the database, this should be also with ID code 1 (one), for consistency reasons.

Making the distinction of the “Builder” user by an intrinsic parameter (here the user ID code), instead of by the association to any special profile of a given application, makes it easy to provide a similar mechanism to the other

applications. Anticipating the need for a user of the “Builder” type for all applications sharing the portal, this mechanism allows the existence of a “Builder” user as universal as the access control itself.

Summarizing, the initial database requisites for the SCA application to work with the concept of a “Builder” user are:

- A management center with ID code 1.
- A user with ID code 0. This user is the one with “Builder” privileges.
- A management system with ID code 1 (preferably). This system is the SCA application.
- An association between the user with ID code 0 and the SCA administration application.

Implementing Access Control in the SCA application

The simplest but also the most important change to do in the SCA application is the differentiated handling of normal users and the “Builder” user. Therefore, each time the access to an intermediate point is tested, the “Builder” user will always succeed whereas other users will have to be validated by calling the access control API.

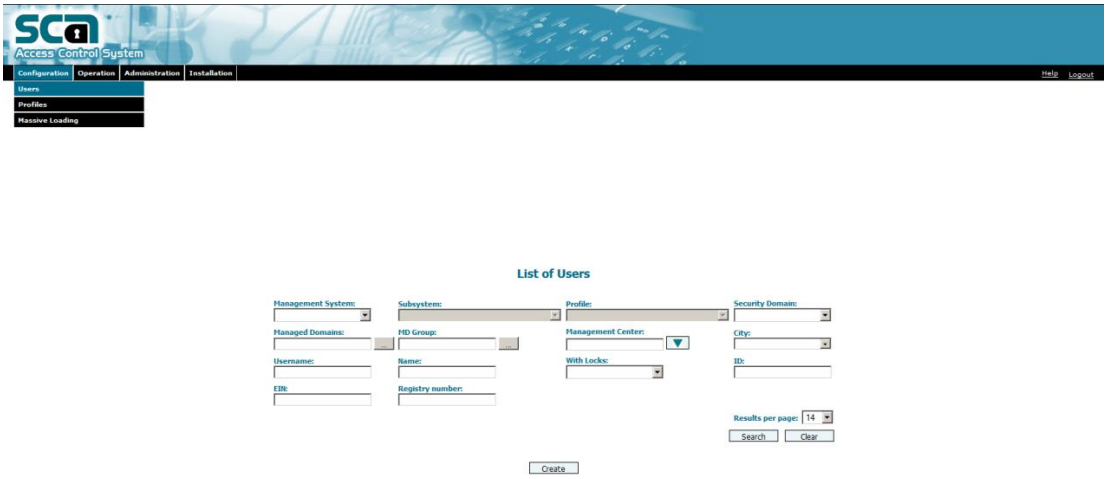
It also is necessary for the “Builder” user to be invisible to the administration application users.

About the intermediate points that are only accessible by the “Builder” user, no change in the application is needed, as those intermediate points are not registered in the database. Therefore, these intermediate points can never be assigned to any normal user. In particular, the SCA management system will be visible, having no risk for it to be modified or deleted by a “normal” user as only the “Builder” can perform this type of operations.

User profile example

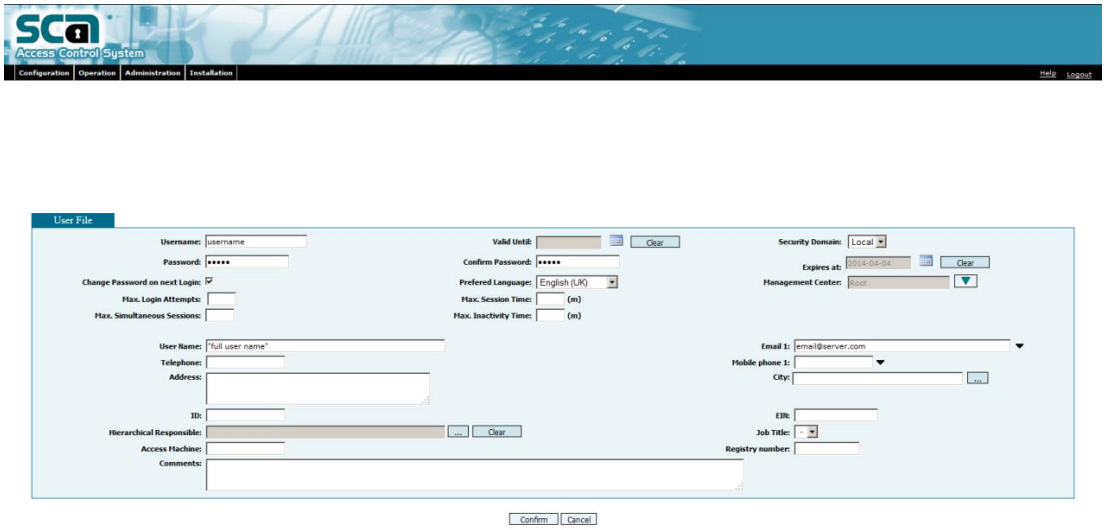
Select Configuration→Users, in order to view the list of registered users (**Figure 270**).

Figure 270. List of Users



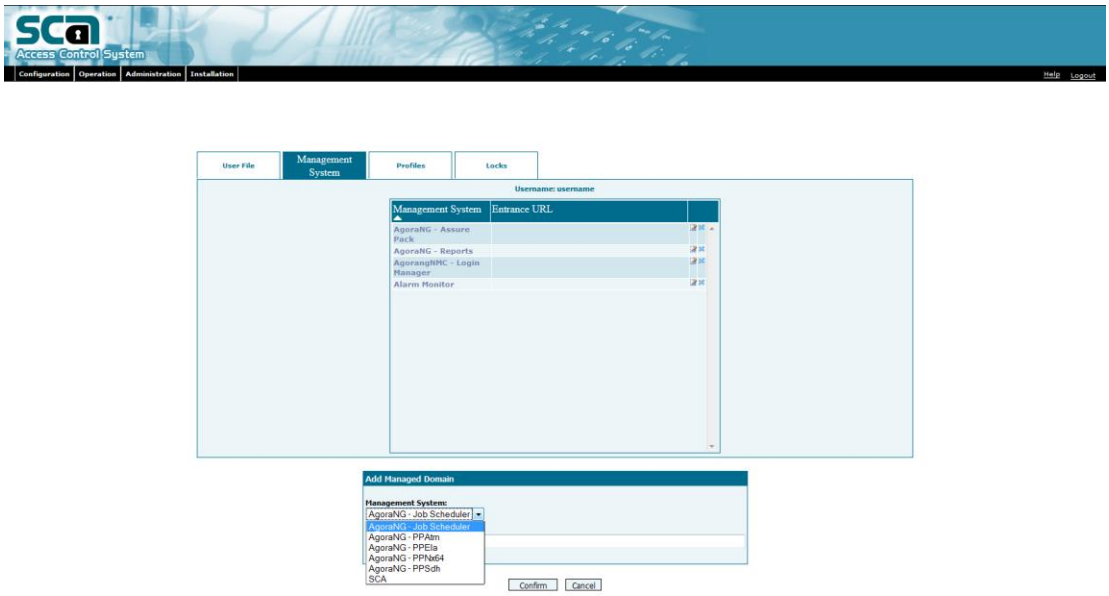
Select User Files, in order to view the user list details (**Figure 271**).

Figure 271. User file



Select Management System, in order to see and add user managed domains (**Figure 272**).

Figure 272. Management System



Select Profiles, in order to see and add user, domain and global profiles (**Figure 273**, **Figure 274** and **Figure 275**).

Figure 273. User Profiles

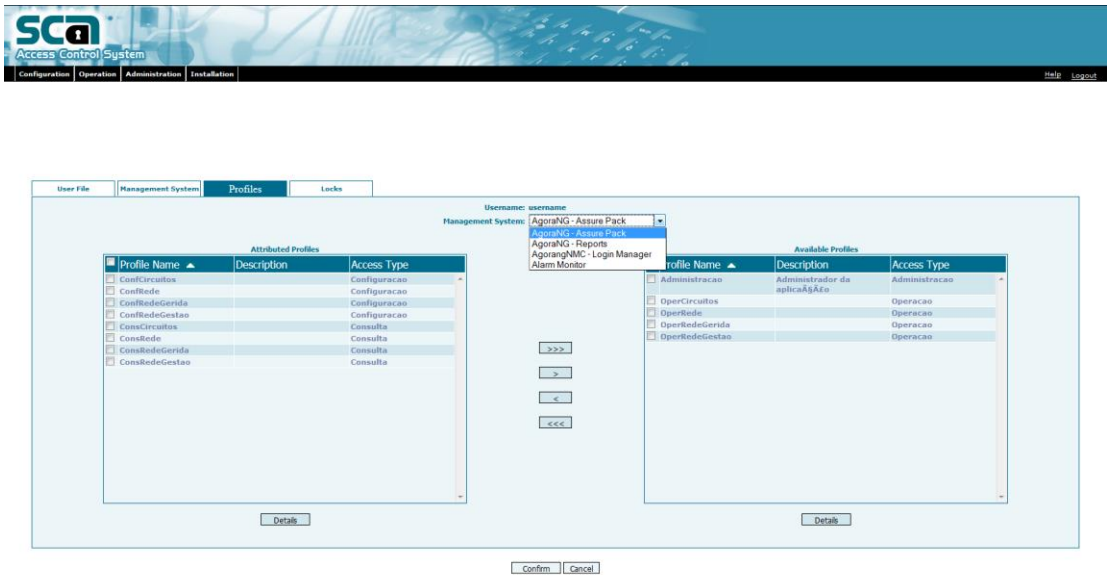


Figure 274. Domain Profiles

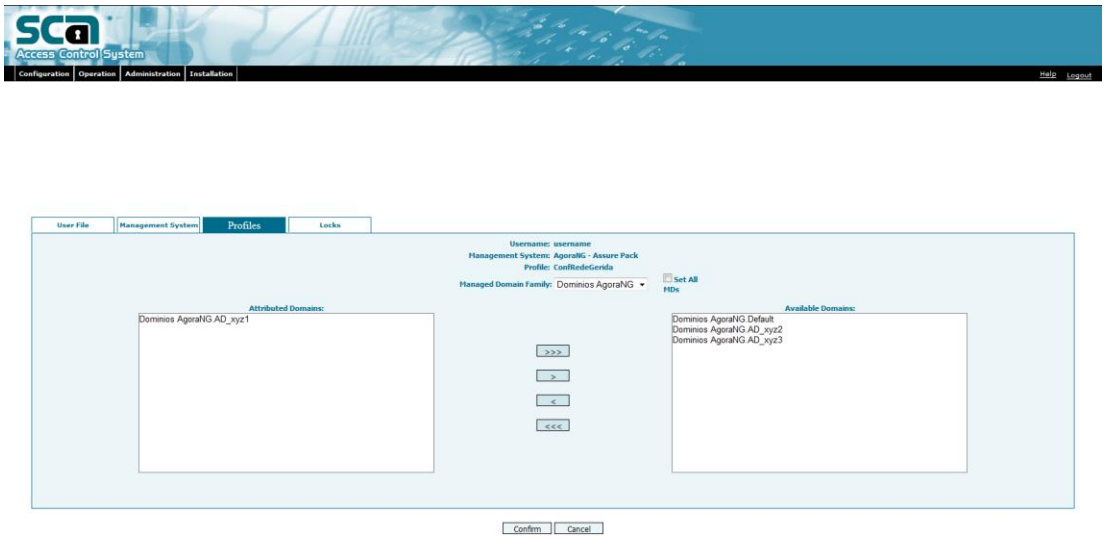
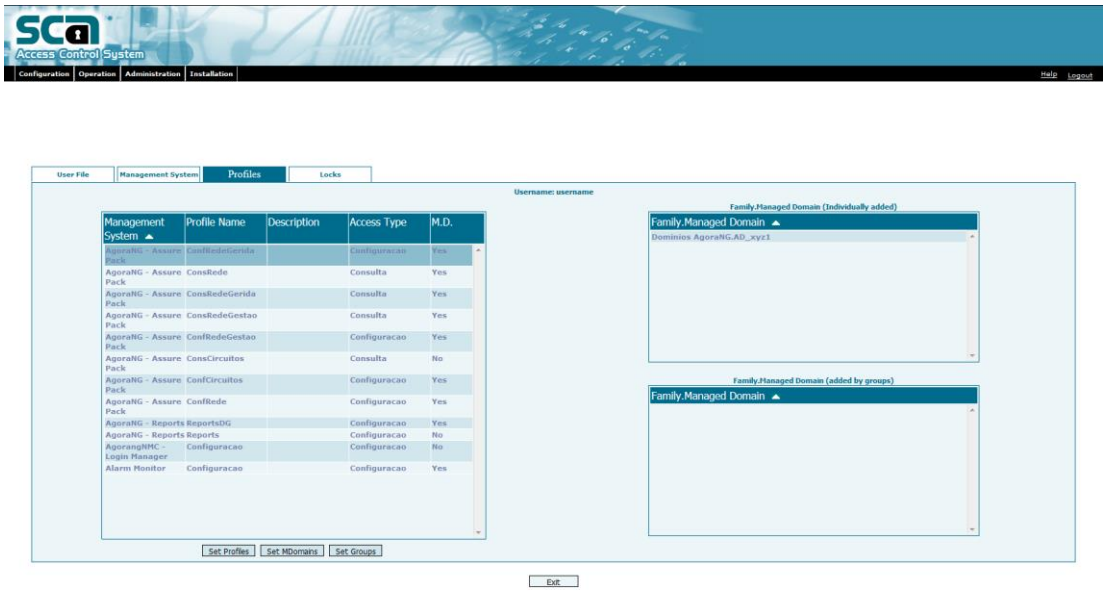
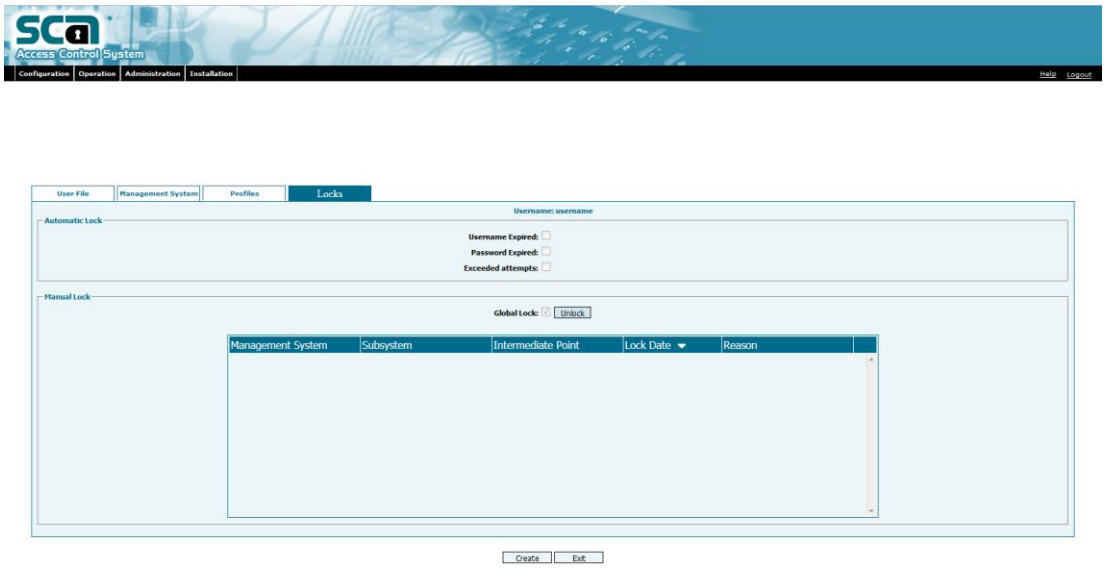


Figure 275. Profiles



Select Locks, in order to see and configure manual and automatic user locks (**Figure 276**).

Figure 276. Lock



Glossary of Abbreviations and Terms

ACL	Access Control List
AM	Alarm Monitor
CMN	Termination Point/Intermediate Point
CORBA	Common Object Request Broker Architecture
CSV	File extension of type Comma Separated Values
DB	Database
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
GPON	Gigabit Passive Optical Network
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
ICN	Management Centralized Network
ICNAP	ICN Access Point
IP	“Internet Protocol”
IP	Intermediate Point
IP	Internet Protocol
IP	Internet Protocol
IP	Internet Protocol
J2EE	JavaTM 2 Platform, Enterprise Edition (J2EETM)
JAR	Java ARchive
JBOSS	JavaBeans Open Source Software
JDBC	Java Database Connectivity
JDK	Java Development Kit
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LSB	Linux Standard Base
M/O/A	Mandatory/Optional/Automatic
MC	Management Center
MD	Managed Domain
MDF	Managed Domains Family
MDG	Managed Domains Group
MPLS	Multiprotocol Label Switching
MS	Management System
ND	Network Domain

NE	Network Element
NE	Network Equipment
NE	Network Element
OCF	OpenBSD/FreeBSD Cryptographic Framework
OMCI	ONT Management and Control Interface
OS	Operation System
OS	Operating System
OS	Operational System
OS	Operation System
PAW	Pending Alarms Window
PGA	Program Global Area
PL-SQL	Procedural Language/Structured Query Language
PP	Provision Pack
PT	Portugal Telecom
QoS	Quality of service
RHEL	Red Hat Enterprise Linux
RIN	PT Computer Network
RPM	Red Hat Package Manager
SCA	"Sistema de Controlo de Acessos", Access Control System
SCA	Service Component Architecture
SD	Security Domain
SGA	System Global Area
SID	Security Identifier
SNMP	“Simple Network Management Protocol”
SNMP	Simple Network Management Protocol
SNMP	Simple Network Management Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SS	Subsystem
SSH	Secure Shell
STONITH	Shoot The Other Node In The Head
TCP	“Transport Control Protocol”
TCP	Transport Control Protocol
TCP	Transmission Control Protocol
TCP	Transport Control Protocol
TMN	“Telecommunications Management Network”
TMN	Telecommunications Management Network
TP/IP	Termination Point / Intermediate Point

UDP	User Datagram Protocol
URL	Uniform Resource Locator
WWW	“World Wide Web”
WWW	World Wide Web
XML	Extensible Markup Language
YUM	Yellowdog Updater, Modified