A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Manager

Installation and Service Manual

Service Documentation

03/2025

A31003-H34B0-S101-02-7620

Notices

Trademarks

Contents

1 Important Notices

1.1 About This Book

This manual provides overview information and instructions for installing, testing and servicing the OpenScape 4000 Manager.

The audience for this book are the installation specialists, customer engineers, second level support, system engineers, and customer administrators who install, maintain, service, administer the OpenScape 4000 Manager.

1.1.1 Prerequisite Knowledge

The person installing and servicing the OpenScape 4000 Manager must have the following basic knowledge:

- Telephony and trunking knowledge
- OpenScape 4000 system knowledge
- LAN-based communications
- Client and server architecture
- Workstation and server hardware repair procedures

1.1.2 Organizational Structure

This manual contains the following chapters:

Chapter 2, "Introduction", provides an overview of the OpenScape 4000 Manager hardware and software.

Chapter 3, "Preparing and Installing the OpenScape 4000 Manager Server", describes the procedures that must be performed before and during the installation of OpenScape 4000 Manager.

Chapter 4, "Setting Up Systems and Users with OpenScape 4000 Manager", provides the instructions for installing the different types of software associated with the OpenScape 4000 Manager server.

Chapter 5, "Servicing and Maintaining the OpenScape 4000 Manager Server", provides OpenScape 4000 Manager service and maintenance procedures.

Chapter 6, "OpenScape 4000 SNMP Management", describes the installation, configuration and basic administration of the OpenScape 4000 SNMP Proxy Agent and the special scripts used to filter alarm messages.

Chapter 7, "SNMP Features/Extensions", describes the requirements and the architecture of OpenScape 4000 Manager and Assistant.

Chapter 8. "Troubleshooting", provides instructions for troubleshooting SNMP.

This manual also includes an Abbreviations list.

1.1.3 Notational Conventions and Symbols Used

This manual uses the following symbols and conventions:

NOTICE: Notes and explanatory information are presented in this manner.

Customer impact statements and explanatory information of particular importance are presented in this manner.

Safety information: DANGER, WARNING or Caution Hazard information. See Section 1.2, "Data Protection and Data Security" for details.

1.1.4 Related Publications

Related publications include the following manuals and guides:

- OpenScape 4000 Manager V10, Batch Generator - Direct Access, Administrator Documentation, P31003-H34A0-M130-xx-76A9
- OpenScape 4000 Manager V10, Configuration Management, Administrator Documentation, P31003-H34A0-M111-xx-76A9
- OpenScape 4000 Manager V10, Feature Description, P31003-H34A0-F100-xx-7618
- OpenScape 4000 Manager V10, Import/Export Interface (XIE) API, Service Documentation, P31003-H34A0-S100-xx-7620
- OpenScape 4000 Manager V10, License Management Tool - Access Management, Administrator Documentation, P31003-H34A0-M132-xx-76A9
- OpenScape 4000 Manager V10, Performance Planning Tool, Planning Guide, P31003-H34A0-P101-xx-76A9
- OpenScape 4000 Manager V10, PM Calculation Rules and Examples, Administrator Documentation, P31003-H34A0-M136-xx-76A9
- OpenScape 4000 Manager V10, Software Activation, Administrator Documentation, P31003-H34A0-M133-xx-76A9
- OpenScape 4000 Manager V10, Webmin Base Administration, Administrator Documentation, P31003-H34A0-M132-xx-76A9
- OpenScape 4000 Manager V10, Data Sheet, P31002-H34A0-D100-xx-7629
- OpenScape 4000 V10, Volume 3, Feature Usage Examples P31003-H31A0-S104-xx-7620

1.1.5 Documentation Feedback

When you call or write, be sure to include the following information. This will help identify which document you are having problems with.

- **Title:** OpenScape 4000 Manager, Version 10, Installation and Service Manual
- **Order Number:** A31003-H34A0-S101-02-7620

1.1.5.1 For U.S. only

To report a problem with this document, call your next level of support:

- Customers should call the Customer Support Center (CSC).

- Unify employees should call the Interactive Customer Engagement Team (i-CET) or complete a Documentation Feedback Form on the LiveLink Product Documentation page.

1.1.5.2 Countries other than U.S.

Please provide feedback on this document as follows:

- Submit a trouble ticket via the Service NOW portal, or
- Use the Document Feedback form that you can access from the front page of the HTML version of this document.

1.2 Data Protection and Data Security

This system processes and uses personal data for purposes such as call detail recording, displays, and customer data acquisition.

In Germany, the processing and use of such data is subject to various regulations, including those of the Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG). For other countries, please follow the appropriate national laws.

The aim of data protection is to protect the rights of individuals from being adversely affected by use of their personal data.

In addition, the aim of data protection is to prevent the misuse of data when it is processed and to ensure that one's own interests and the interests of other parties which need to be protected are not affected.

The customer is responsible for ensuring that the system is installed, operated and maintained in accordance with all applicable labor laws and regulations and all laws and regulations relating to data protection, privacy and safe labor environment.

Employees of our company are bound to safeguard trade secrets and personal data under the terms of the company's work rules.

In order to ensure that the statutory requirements are consistently met during service – whether on-site or remote – you should always observe the following rules. You will not only protect the interests of your and our customers, you will also avoid personal consequences.

A conscientious and responsible approach helps protect data and ensure privacy:

- Ensure that only authorized persons have access to customer data.
- Take full advantage of password assignment options; Never give passwords to an unauthorized person orally or in writing.
- Ensure that no unauthorized person is able to process (store, modify, transmit, disable, delete) or use customer data in any way.
- Prevent unauthorized persons from gaining access to storage media, such as backup CDs or log printouts. This applies to service calls as well as to storage and transport.
- Ensure that storage media which are no longer required are completely destroyed. Ensure that no sensitive documents are left unprotected.

Work closely with your customer contact; this promotes trust and reduces your workload.

2 Introduction

This chapter provides an overview of the OpenScape 4000 Manager and its components.

2.1 General Description

Within the context of OpenScape Management and the new OpenScape/ HiPath convergence architecture, the OpenScape 4000 Manager is the element manager dedicated to the administration and serviceability of the OpenScape 4000 IP communication platform, either in standalone mode (referred to as OpenScape 4000 Assistant in such cases), or in networks with other OpenScape/HiPath 4000 IP communication platforms, and associated products.

With HiPath User Management V3, it is possible to connect two different Managers.

OpenScape 4000 Manager and OpenScape 4000 Assistant can be differentiated as follows (see also the diagram in Figure 3):

- OpenScape 4000 Manager -- Network version for small, medium and large networks; resides on an external server (refer to Section 2.1.1)
- OpenScape 4000 Assistant -- Local version, resides on the ADP of a OpenScape 4000 IP communication platform

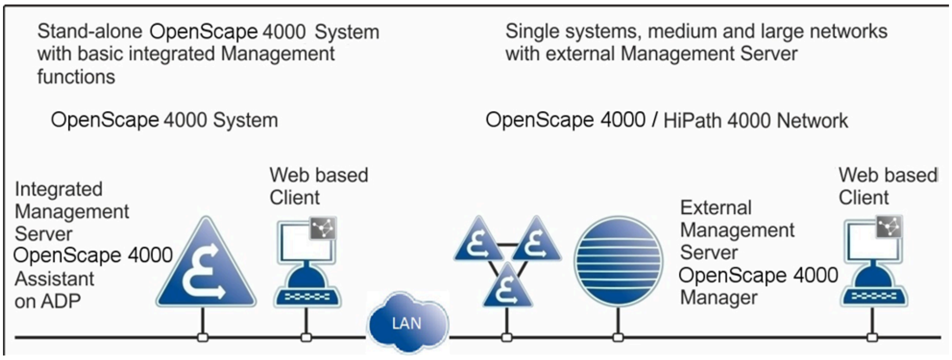

Stand-alone OpenScape 4000 System with basic integrated Management functions
Single systems, medium and large networks with external Management Server
OpenScape 4000 System
OpenScape 4000 / HiPath 4000 Network
Integrated Management Server OpenScape 4000 Assistant on ADP
Web based Client
LAN
External Management Server OpenScape 4000 Manager
Web based Client

Figure 1: OpenScape 4000 Manager vs. OpenScape 4000 Assistant

2.1.1 OpenScape 4000 Manager (External Server)

The OpenScape 4000 Manager provides extended management functionality for standalone OpenScape 4000 IP communication platforms and networks of these platforms. The features of the OpenScape 4000 Manager add functionality, simplify tasks, or both.

OpenScape Manager V10R1 will be offered for Unify proprietary hardware EcoServer and for VMware/ESX>. In both cases, due to the enhanced demand, a 1TB SSD is required.

The OpenScape 4000 Manager package features the following applications:

- CM-Network

  This feature provides advanced Configuration Management functionality in small, medium, and large networks, including node-to-node moves and network dial plan handling. Trunk-related administration is possible by launching the CM-Basic application in the OpenScape 4000 system itself (Assistant). In this way, approximately 85% of AMOs are accessible via the web-based interface, the rest being accessible using the integrated ComWin application.

- PM-Network

  The network-level Performance Management package measures and evaluates trunk traffic network-wide. PM-Net replaces the PM-Charts product associated with HDMS.
- PM-Enhanced

  Using PM-Network as a basis, PM-E measures and evaluates the communication behavior of users and user groups. PM-E also measures the load on specific components of OpenScape 4000 systems, with limited features network-wide for all measurement objects.
- PM-ASC (Attendant Supervisor Console)

  This feature is only for measurement of ASC statistics from an attendant console.
- COL-Network

  When installed for an OpenScape/HiPath 4000 network, this application serves as a central CDR collection function for the entire network. The data collected are used by Accounting Management and Performance Management.
- Import/Export API (XIE)

  This is the data import/export interface. The API provides external applications access to the OpenScape 4000 Manager data and allows data import and export to/from the OpenScape 4000 Manager.
- SNMP

  The SNMP Agent is a gateway function that is required for connection to third-party umbrella management systems.

2.2 OpenScape 4000 Manager Hardware

The OpenScape4000 Manager is offered as a Hardware/Software Appliance similar to the OS4K system. The OpenScape EcoServer (S30122-K7760-X) can be used as platform or, alternatively, as a VM in a VMware environment.

For the required resources on VM, please see the table in chapter 5.5.2 "OpenScape 4000 Manager V10R1", of the OpenScape Solution Set V10, OpenScape Virtual Machine Resourcing and Configuration Guide, Service Documentation. Most of the settings are set when the OVF template, included in the installation media, will be deployed.

The OpenScape EcoServer hardware may come to limits in customer setups which exceed the limit of 100 OpenScape 4000 systems and 30000 ports.

NOTICE: The space capacity of the HDD must be 1 TB.

2.3 OpenScape 4000 Manager Software

The OpenScape 4000 Manager will be provided as SW appliance. This appliance includes the pre-hardened SLES (Suse Linux Enterprise System) based Operating System and all required Manager SW applications. The ISO Install image can be either copied to an USB stick for installation on OpenScape EcoServer HW Platform or mounted via VMware Management application.

The Appliance installation requires two IP addresses, one for the LINUX Platform and another one for the Manager application operating in the Container.

The SW Lifecycle is completed via Unify SWS, Manager HotFix, Platform HotFix and RLC (Release Level complete) for Fix/ Minor/ Major Release SW updates. The SWM application is the central point for the SW supply.

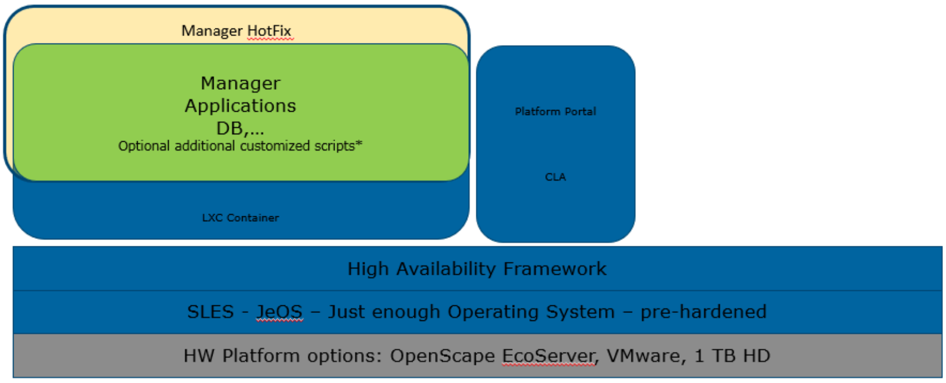

Manager HotFix
Manager
Applications
DB,...
Optional additional customized scripts*
LXC Container
Platform Portal
CLA
High Availability Framework
SLES - JeOS – Just enough Operating System – pre-hardened
HW Platform options: OpenScape EcoServer, VMware, 1 TB HD

Figure 2: OpenScape 4000 Manager Application HotFix

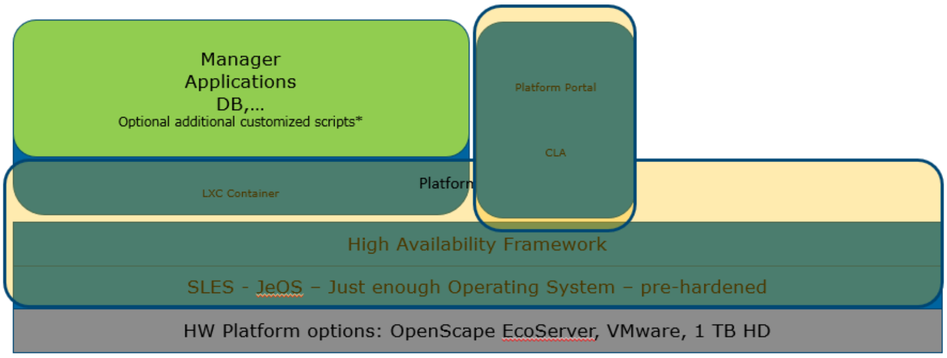

Manager
Applications
DB,...
Optional additional customized scripts*
Platform Portal
CLA
LXC Container
Platforn
High Availability Framework
SLES - JeOS – Just enough Operating System – pre-hardened
HW Platform options: OpenScape EcoServer, VMware, 1 TB HD

Figure 3: OpenScape 4000 Patform HotFix

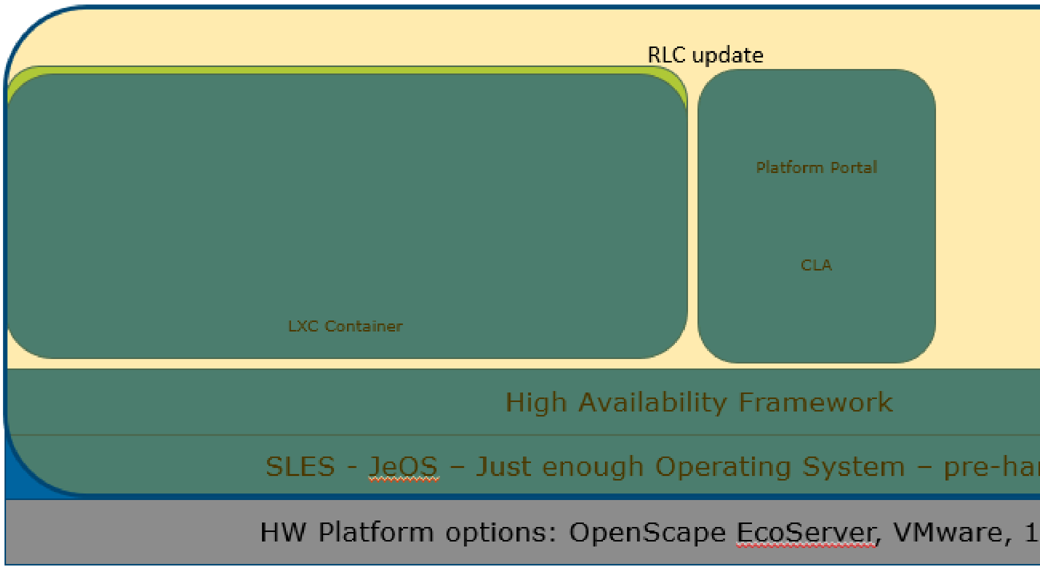

RLC update
Platform Portal
CLA
LXC Container
High Availability Framework
SLES - JeOS – Just enough Operating System – pre-ha
HW Platform options: OpenScape EcoServer, VMware, 1

Figure 4: OpenScape 4000 RLC update - including Major Release

2.3.1 Launchpad and Dashboard

When logged in to the Manager the first page being displayed is the Launchpad on the left and Dashboard on the right side. The Launchpad provides the user with an overview of all OpenScape 4000 Manager applications for which the current user is licensed and authorized. The starting of such applications does not require any further user authentication. The user can also use Launchpad to start the native management applications for network objects that are managed within the OpenScape 4000 Manager network (Direct Access).

The Launchpad consists of the application tree, which is used to organize and start the applications; the menu bar, which contains entries for customizing the application tree, sending client broadcast messages, invoking online help.

The Dashboard panel on the right provides a general overview of the system status.

The Launchpad dashboard --> Dashboard displays useful information about system statuses. This information is grouped based on the type of information into the following groups:

- User Info
- License Management
- Status Board
- Configuration Management
- System Management
- System Components
- Important Hints – Component, Version, System Start date/time

The content of the Launchpad tree depends on the registration data of each application, and can differ in each scenario. Applications that need interaction with a network object are only visible if at least one corresponding network object (type and version) is in the system.

Figure 3 shows the OpenScape 4000 Manager Launchpad with its default application groups.

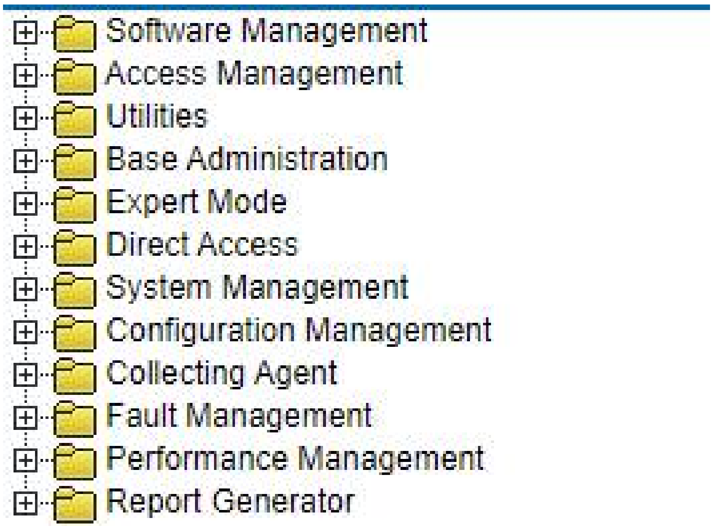
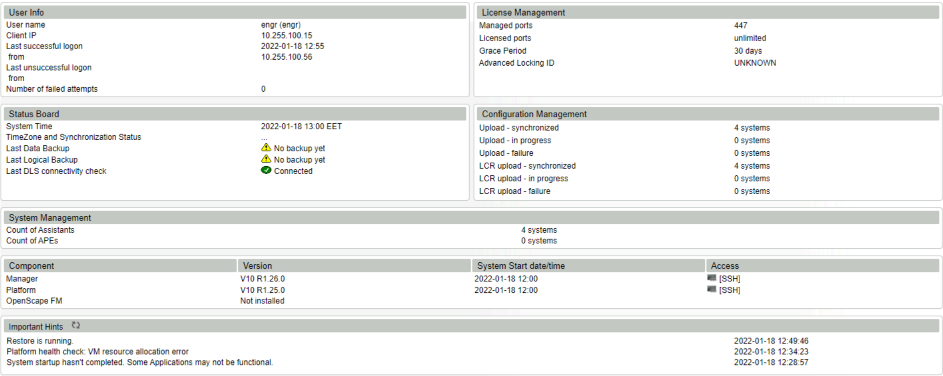


Figure 5: The OpenScape 4000 Manager Launchpad

Figure 4 shows the OpenScape 4000 Manager Dashboard with the status of the various components.



User Info	
User name	engr (engr)
Client IP	10.255.100.15
Last successful logon	2022-01-18 12:55
from	10.255.100.56
Last unsuccessful logon	
from	
Number of failed attempts	0

License Management	
Managed ports	447
Licensed ports	unlimited
Grace Period	30 days
Advanced Locking ID	UNKNOWN

Status Board	
System Time	2022-01-18 13:00 EET
TimeZone and Synchronization Status	...
Last Data Backup	⚠ No backup yet
Last Logical Backup	⚠ No backup yet
Last DLS connectivity check	✓ Connected

Configuration Management	
Upload - synchronized	4 systems
Upload - in progress	0 systems
Upload - failure	0 systems
LCR upload - synchronized	4 systems
LCR upload - in progress	0 systems
LCR upload - failure	0 systems

System Management	
Count of Assistants	4 systems
Count of APEs	0 systems

Component	Version	System Start date/time	Access
Manager	V10 R1.26.0	2022-01-18 12:00	[SSH]
Platform	V10 R1.25.0	2022-01-18 12:00	[SSH]
OpenScape FM	Not installed		

Important Hints	
Restore is running.	2022-01-18 12:49:46
Platform health check: VM resource allocation error	2022-01-18 12:34:23
System startup hasn't completed. Some Applications may not be functional.	2022-01-18 12:28:57

Figure 6: The OpenScape 4000 Manager Dashboard

2.3.2 Software Management

Software Management is the application group comprising functions for installing, activating, updating, transferring and backing up software applications and data. The applications that are available under Software Management in the OpenScape 4000 Manager include Appliance Management (RISO), Backup and Restore (HBR), Software Activation (SWA), Software Manager (SWM).

2.3.2.1 Software Manager (SWM)

Software Manager is a tool used to transfer software via LAN (TCP/IP) from the client PC. There the software must be downloaded from the Software Supply Server (SWS server) application to upload the corresponding software packages before activation.

It supports the Software Release Management version (SWRM) - Major, Minor, Fix, HotFix Release for Manager and Platform.

2.3.2.2 Software Activation (SWA)

After a Major, Minor, Fix, Manager or Platform HotFix Release has been transferred to the OpenScape 4000 Manager by means of SWM (Software Manager), it must be activated.

2.3.2.3 Backup and Restore

Backup and Restore is used to save configuration data or software from Manager applications to a backup copy, and to restore this data in the event of a system failure.

In addition to backup and restore functions, the user interface of Backup and Restore allows the user to display the contents of an archive or all archives, display the status of the last backup/restore procedure or the one currently in progress, administer external devices such as tape drives or backup servers, and display Backup and Restore log files.

NOTICE:

Backup / Restore refuses any custom files or subdirectories in the Backup directory. A check warns the user if other directories are created in the backup folder. The directory, which is specified on Backup Server for HBR backups and also /.AS/BACKUP/Backup directory on Assistant/Manager hard disk must be dedicated only for HBR backups.

The backup/restore is blocked when other folders are found under this dedicated directory.

At the beginning of backup/restore there is always the test of target archive (device). The test of given archive also checks whether there are no unexpected directory names in the archive. If the check fails (e.g. strange directories are found) then the backup/restore is not started (fails in early phase).The problem occurs when maximal count of backup sets is reached and older backup set (which was previously manually renamed) had to be updated.

2.3.3 Access Management

Access Management is the central access control point for OpenScape 4000 Manager servers. It controls which users are allowed to access the server and which applications and features these users may use.

Access Management is used to create user accounts, manage passwords and other account-related data, and control access via Web browser, windows client application (ComWin, for example), or linux remote shell.

2.3.3.1 License Management (LicM)

With the License Management (LicM) application, the administrator of the OpenScape 4000 Manager system can display information pertaining to installed license, and can also configure the location of the Customer License Agent (CLA). The license data has to be installed and activated on the configured Customer License Agent.

2.3.3.2 OpenScape 4000 License Management Tool (LMT)

The License Management Tool (LMT) handles the moving of software licenses across OpenScape/HiPath 4000 nodes in a network environment. This dynamic shifting of licenses, organized in LMT administration groups, relieves the customer of having to move licenses between switches when subscribers are moved/configured/removed. LMT functionality is not required for single switches.

2.3.3.3 Session Management

The Session Management function offers a user interface for changing the user password if necessary, and a Web Session Manager that lists all Web sessions belonging to the current user. Users can view login and connectivity information for their sessions, and can also close (kill) sessions manually.

2.3.3.4 Account Management

The Account Management part of Access Management provides user interfaces for performing tasks associated with user account administration, system account administration, access right configuration, and access right group configuration.

2.3.3.5 Manage Web Server Certificates

Manage Web Server Certificates provides tools to generate, import and activate SSL certificates on the current web server. A certificate can be generated as self-signed certificate or via Certificate Sign Request (CSR). The Individual Root Certificate Authority can be generated and used to sign CSR in Certificate Network Management.

2.3.3.6 Security Mode Configuration

The general security configuration can be maintained from Security Mode Configuration. This configuration covers restrictions of remote access over SSH, SecM, ODBC, JDBC interfaces. Further, the authentication mode (password and/or PKI), Gateway Security and TLS protocol selection can be switched.

2.3.3.7 Configuration of PKI Authentication

This tool is designed to maintain the Public Key Infrastructure (PKI) for authentication to the system via a PKI certificate. The tool covers the configuration of the PKI tree structure of certificates and the configuration of the revocation mode. The CRL and OCSP methods can be used to check the validity of the client certificate.

2.3.3.8 Configuration of Single Sign On Authentication

OpenScape 4000 Manager or Assistant supports a "Single Sign On" with Active Directory. This feature provides authenticated domain users with seamless sign on at OpenScape 4000 Manager or Assistant by just a single click. It is based on Kerberos credentials (authentication token) that are automatically provided by client web browser.

2.3.3.9 Customize Banner on Login Page

This application can be used to define a customer-defined text banner for the login page. This banner is visible during login to the system via SSH and web browser.

2.3.4 Utilities

The Utilities application group comprises following application: Import/Export API (XIE).

2.3.4.1 Import/Export API (XIE)

Through the use of an optional, open API feature, OpenScape 4000 Manager enables import/export data exchange with third party applications. Customers can quickly download or upload information, such as personal employee data, from/into the OpenScape 4000 Manager database. For example, they can also save time exporting fields from the subscriber database to their current or future directory services applications.

OpenScape 4000 Manager supports an enhanced Application Programming Interface (API), which makes it possible for customers to use their own database applications to read/write data from/to the OpenScape 4000 Manager database.

There are several ways to communicate with OpenScape 4000 Manager via the API:

1) API C++ Programming Interface using API class library The customer uses his own application program and programs the exchange of data.
2) API File Interface Uses Linux scripts at the Command Line Interface (CLI) to exchange data.
3) Import/Export Table from the Desktop. API Import/Export Client, which is a windows desktop application, available to be download from the LAP XIE.
4) Encrypted XIE Web server Interface. SOAP based interface to exchange data.
5) XIE Webservice: the HTTPS SOAP based interface for export/import data from/to OpenScape 4000 Manager database which can be used in customer applications.

2.3.5 Base Administration

Base Administration is the application group that comprises Webmin Base Administration and Logging Management.

2.3.5.1 Webmin Base Administration

Under Webmin Base Administration you can find information about:

- LAN Configuration (LAN Cards, DNS, Hosts, Routes, Service Access)
- WAN Configuration (Firewall)
- System Administration (Date/Time, Timezone, Reboot/Shutdown, Application Processes)

2.3.5.2 Logging Management

Logging Management is the base application that provides a central logging service to other applications running on the OpenScape 4000 Manager platform. These applications may still use their own facilities to record details, but all applications use Logging Management to maintain a summary of their activity and error events.

Logging Management can be used to view, for example, all activities on a specific switch, all activities on all switches on a specific day, or all errors from a specific application or process. Using a Web-based interface for access to all functions, the user can create, modify and save queries for specific activity and error log recording. Administration functions are provided for forwarding activity events to other platforms, such as remote service centers, for example.

2.3.6 Direct Access

The Direct Access feature of OpenScape 4000 Manager enables the user to start the native management application for a network object. Single login, where the user does not have to explicitly log in to the selected network object, is only possible if the login information is passed on to the relevant application. The user provides this required login information when the network object is created in System Management.

OpenScape 4000 Manager supports Web-based applications, Windows applications, and CLI-based applications for Direct Access.

2.3.6.1 OpenScape 4000

This function allows you to open Remote Access, File Transfer or application of the corresponding switch, which was defined in the System Management. It uses Single Sign On feature to bypass the authentication to the Assistant.

2.3.6.2 Batch Generator

The Batch Generator is an online/offline batch processing application that is used to send and execute AMO commands on OpenScape 4000 systems. The interface is based on a client/server architecture. AMO commands are saved as command files in a database. Command file templates containing user-defined parameters can be used to generate the command files.

Before command files can be sent to a OpenScape/HiPath switch, the user must edit a job file containing information about the switch and the command file that is to be sent to it. Each command file designated for a specific OpenScape/HiPath switch is called a batch job. A job file comprises one or more batch jobs.

2.3.6.3 Platform Portal

The Platform Portal is the web-based platform for performing administration, maintenance and service tasks for OpenScape 4000. The interface is referred to in the further course of this documentation as "portal" for short.

The following pages can be selected in the main menu:

- System (Shell to Host, LAN Configuration, Static Routes, UPS, SNMP Configuration)
- Status (Manager Installation-Status, Cluster-Recovery Status, LAN Overview, DISK Status, Software)
- Maintenance (Manager Reinstallation, Recovery HD, Logs, Shutdown/ Reboot)
- Manager

The footer area on every page contains the following:

- Control Panel
- sysinfo

When the portal is launched, an overview of the configuration options available with the portal is displayed automatically. The overview can be retrieved again at any time by selecting the **Start** menu option.

NOTICE: The Platform Portal requires its own IP address.

2.3.7 System Management

System Management is the application used to configure (add/delete) OpenScape 4000 systems into management of the OpenScape 4000 Manager.

2.3.8 Configuration Management (CM)

Configuration Management is the single entry point for managing subscriber data. An easy-to-use browser interface allows the administrator to perform moves, adds and changes for personal and station data for OpenScape 4000 networks. Moves across network nodes and the network dial plan handling are supported. While the network implementation of Configuration Management

(CM) does not support ACD, board, trunk, and maintenance objects, the local version of CM on the OpenScape 4000 Assistant must be used directly to provide these features.

2.3.9 Collecting Agent (COL)

The Collecting Agent (COL), the main component of Account Management (AM) integrated with the OpenScape 4000 Manager, is used to collect accounting data for AM as well as traffic measurement data for Performance Management (PM). The Web-based user interface of COL allows the user to perform various administrative tasks, such as defining input and output formats, defining output lines and filters, and monitoring COL status. A logging feature accessible from the COL home page makes it possible to specify a number of different log types, as well as date and time selectors for defining the reporting period of the logging events.

2.3.10 J-HPT Tool

Java Husim Phone Tester (J-HPT) for Web is a web tool to remotely control IP phones. It is used to simply reproduce the real phone behavior in a web interface and to generate events to be sent to the controlled phones.

2.3.11 Trace Download

The Trace Download is used to collect diagnostic data (trace logs) for specific use cases or components on the Manager to simplify the diagnostics. When a trouble ticket is to be reported to the GVS, the diagnostic data from the Trace Download should be always attached.

2.3.12 Alarm Configurator

The Alarm Configurator is used to manage switch alarms, assign alarms to subscribers or trunks, and generate alarms automatically for trunks to which alarms have not yet been assigned. Alarm Configurator, which can be started from the OpenScape 4000 Manager Launchpad, has a number of options available for updating alarm data for a specific switch, managing alarms in the service module and switching unit, and defining and checking alarm assignments for subscribers and trunks.

2.3.13 SNMP Configurator

The SNMP Configurator is used to display SNMP protocol settings on the host. The parameters displayed for the user sees are centrally set with OpenScape 4000 Assistant.

For more information, refer to OpenScape 4000 Assistant V10, Simple Network Management Protocol HiPath SNMP, Administrator Documentation.

2.3.14 Performance Management (PM)

Performance Management (PM) is an application primarily intended to handle traffic measurement data. Most of the data for PM comes from the CDR records, ZAUSL files and CMI files collected by COL (Collecting Agent). Through a web-based user interface, the PM user can select which telephony items (extensions, hunt groups, attendant consoles, attendant console groups, trunks, trunk groups and cordless concentrators) are to be metered. Facilities are provided for creating, modifying, deleting and running reports and report groups, as well as for creating filters to apply to these reports.

2.3.15 Report Generator

Report Generator is a OpenScape 4000 Manager platform application that facilitates the reporting needs of other OpenScape 4000 applications. This feature allows the user to generate customized flexible reports, using newly created templates or predefined templates that can be modified for specific applications and report objects. Various options are provided for displaying, printing and exporting reports.

An e-mail notification facility makes it possible to define e-mails to be sent automatically after a report has been rendered, with or without exported files as attachments in HTML, PDF, CSV or XML format.

3 Preparing and Installing the OpenScape 4000 Manager Server

This chapter contains procedures that must be performed before and during the installation of the OpenScape 4000 Manager server.

3.1 Preparation

Follow the steps below to prepare the Manager installation:

1) Collect a MAC address of any LAN interface from the hardware which is to be installed.

2) Fill in the XML configuration file.

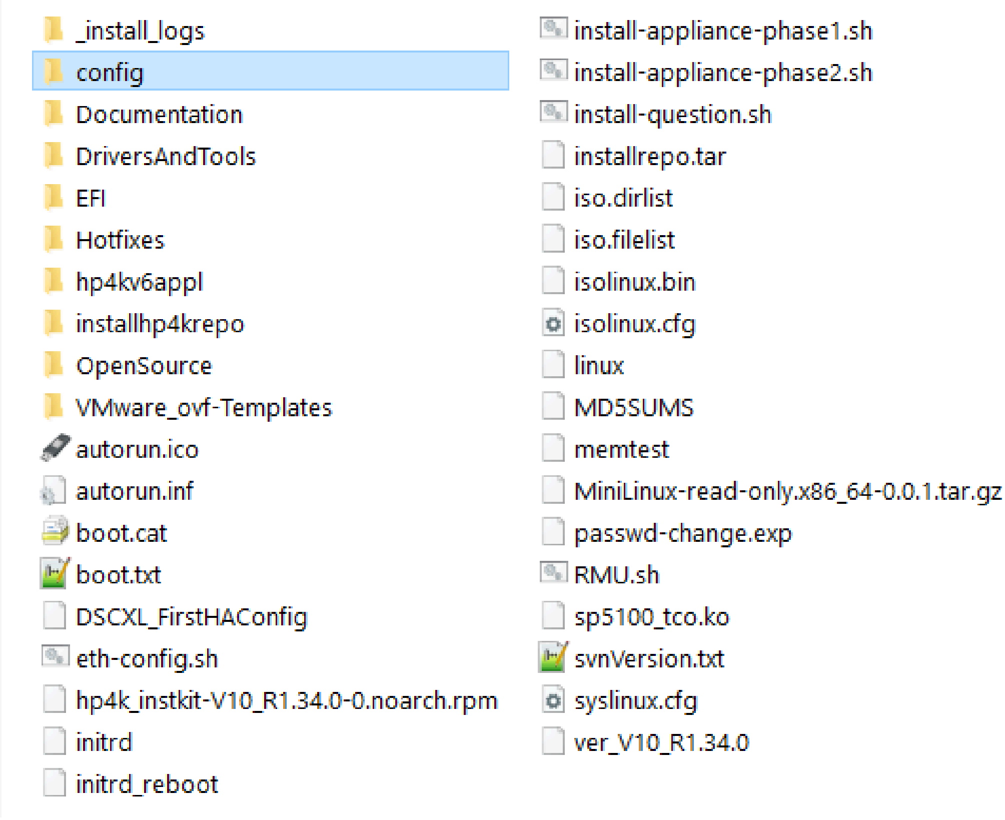
NOTICE: For more information about the XML file, please refer to the OpenScape 4000 Installation, Configuration and Migration document,chapter "XML Configuration File".

NOTICE:

Installation without XML is not possible.

Templates and examples of different XML configuration files for all deployment types are available on the ISO/installation stick in the \Documentation directory (e.g. firstinst-netw-xml_examples_v4.zip).

3) Copy the XML file(s) to the **config** folder on the installation media.



_install_logs
config
Documentation
DriversAndTools
EFI
Hotfixes
hp4kv6appl
installhp4krepo
OpenSource
VMware_ovf-Templates
autorun.ico
autorun.inf
boot.cat
boot.txt
DSCXL_FirstHAConfig
eth-config.sh
hp4k_instkit-V10_R1.34.0-0.noarch.rpm
initrd
initrd_reboot
install-appliance-phase1.sh
install-appliance-phase2.sh
install-question.sh
installrepo.tar
iso.dirlist
iso.filelist
isolinux.bin
isolinux.cfg
linux
MD5SUMS
memtest
MiniLinux-read-only.x86_64-0.0.1.tar.gz
passwd-change.exp
RMU.sh
sp5100_tco.ko
svnVersion.txt
syslinux.cfg
ver_V10_R1.34.0

Figure 7: XML file location on the installation media

NOTICE:

It is possible to copy multiple XML configuration files for multiple systems to the **config** folder if they have different MAC addresses allocated.

3.2 Installation procedure using monitor/keyboard

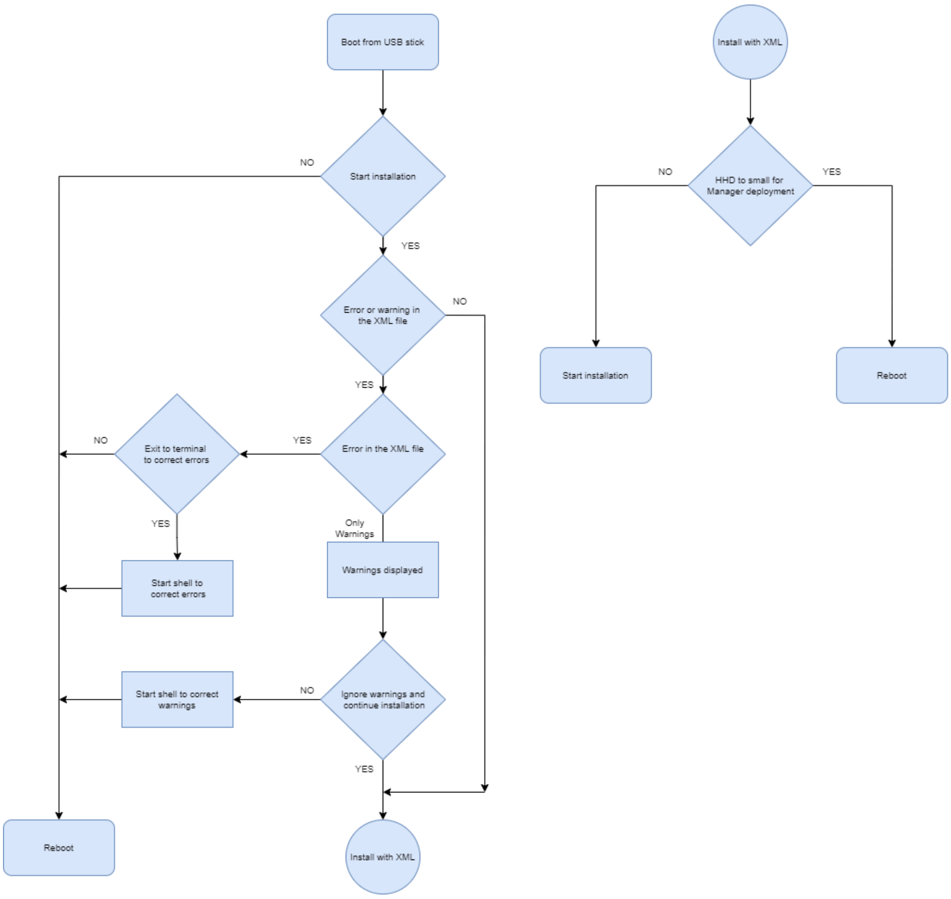

Boot from USB stick
Start installation
NO
YES
Error or warning in the XML file
NO
YES
Error in the XML file
YES
Exit to terminal to correct errors
NO
YES
Start shell to correct errors
Only Warnings
Warnings displayed
Ignore warnings and continue installation
NO
Start shell to correct warnings
YES
Reboot
Install with XML
Install with XML
HHD to small for Manager deployment
NO
YES
Start installation
Reboot

Figure 8: Installation procedure overview

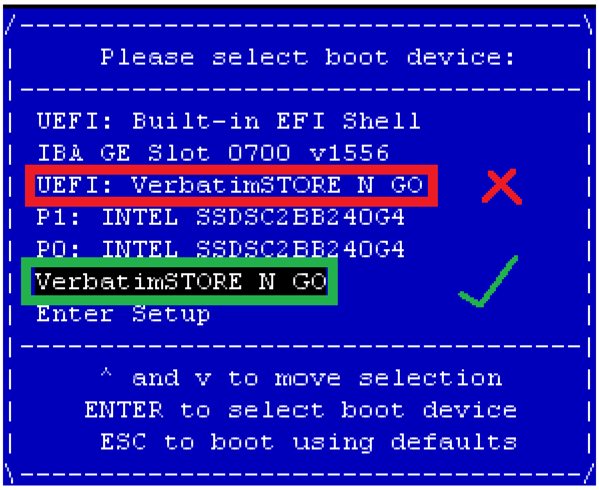
Follow the steps below to perform the Manager installation using monitor/ keyboard:

1) Enter the boot menu and select the boot device:

   EcoServer / Branch: F11 direct, F11 console

2) Please be aware that when using F11 to choose the boot device from BIOS, the USB device in use can be presented twice (i.e. once with the UEFI prefix

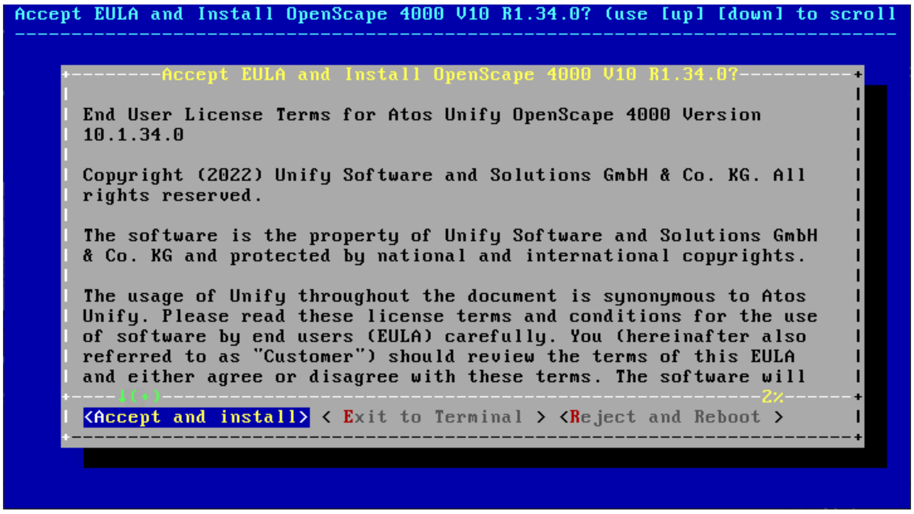
and once without it). The boot device without the UEFI prefix should be selected.



```
/-------------------------------------\
|      Please select boot device:     |
|-------------------------------------|
| UEFI: Built-in EFI Shell            |
| IBA GE Slot 0700 v1556              |
| UEFI: VerbatimSTORE N GO            |
| P1:  INTEL SSDSC2BB240G4            |
| P0:  INTEL SSDSC2BB240G4            |
| VerbatimSTORE N GO                  |
| Enter Setup                         |
|-------------------------------------|
|      ^ and v to move selection      |
|     ENTER to select boot device     |
|      ESC to boot using defaults     |
\-------------------------------------/
```

Figure 9: BIOS Boot device selection

3) Boot the machine from the installation media (USB stick). You will be asked to start the installation or to reboot.



```
Accept EULA and Install OpenScape 4000 V10 R1.34.0? (use [up] [down] to scroll
------------------------------------------------------------------------------

  +--------Accept EULA and Install OpenScape 4000 V10 R1.34.0?----------+
  |                                                                      |
  | End User License Terms for Atos Unify OpenScape 4000 Version         |
  | 10.1.34.0                                                            |
  |                                                                      |
  | Copyright (2022) Unify Software and Solutions GmbH & Co. KG. All     |
  | rights reserved.                                                     |
  |                                                                      |
  | The software is the property of Unify Software and Solutions GmbH    |
  | & Co. KG and protected by national and international copyrights.     |
  |                                                                      |
  | The usage of Unify throughout the document is synonymous to Atos     |
  | Unify. Please read these license terms and conditions for the use    |
  | of software by end users (EULA) carefully. You (hereinafter also     |
  | referred to as "Customer") should review the terms of this EULA      |
  | and either agree or disagree with these terms. The software will     |
  +-----↓(+)---------------------------------------------------2%-------+
  | <Accept and install> < Exit to Terminal > <Reject and Reboot >       |
  +----------------------------------------------------------------------+
```

Figure 10: Machine Boot from the installation media

4) Check if a compatible XML configuration file is available.

If you choose Yes (start the installation), a check on the installation media (in the config folder) will be executed to identify if there is a compatible XML configuration file for the hardware.

There are multiple possibilities for this step:

- **Case 1**: an XML configuration file is found.

  If an XML configuration file containing a MAC address from one of the system interfaces is found, the file will be checked for errors regarding Linux configuration data.

  a) **Case 1.1: The XML configuration file contains no errors/warnings**

  The installation procedure checks the available disk space on the hard disk and determines if the deployment matches the hard disk space.

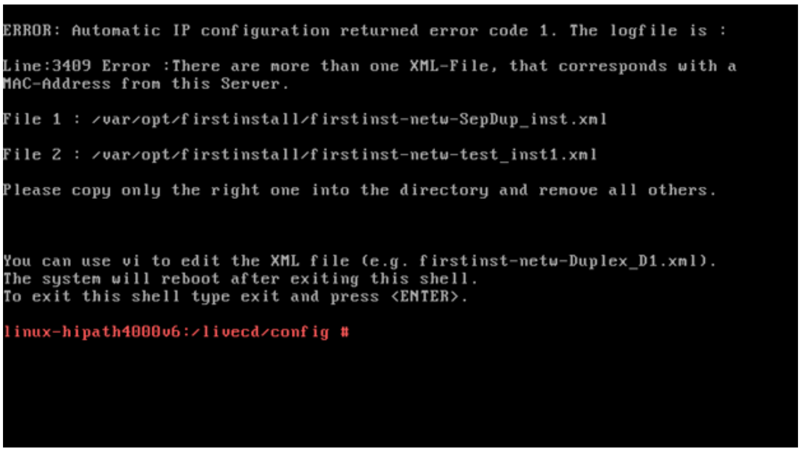
  For more information, please refer to step 5 .

  b) **Case 1.2: The XML configuration file contains errors**

  If the XML configuration file contains errors, the installation will stop with error messages. The error logs will be written on the installation media, in the **_install_logs** folder.

  Examples:

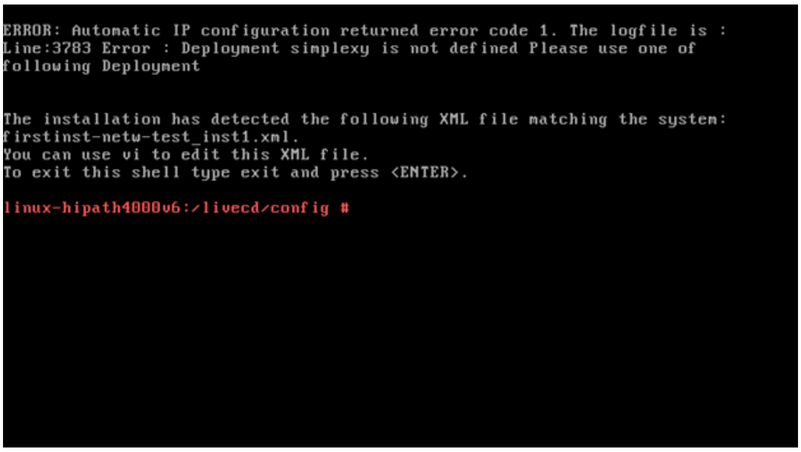
  – More than one XML configuration file corresponds to a MAC address from this server:



```
ERROR: Automatic IP configuration returned error code 1. The logfile is :

Line:3409 Error :There are more than one XML-File, that corresponds with a
MAC-Address from this Server.

File 1 : /var/opt/firstinstall/firstinst-netw-SepDup_inst.xml

File 2 : /var/opt/firstinstall/firstinst-netw-test_inst1.xml

Please copy only the right one into the directory and remove all others.


You can use vi to edit the XML file (e.g. firstinst-netw-Duplex_D1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

linux-hipath4000v6:/livecd/config #
```

Figure 11: First installation - log file for an XML configuration file with error messages

  – Wrong deployment in the XML configuration file

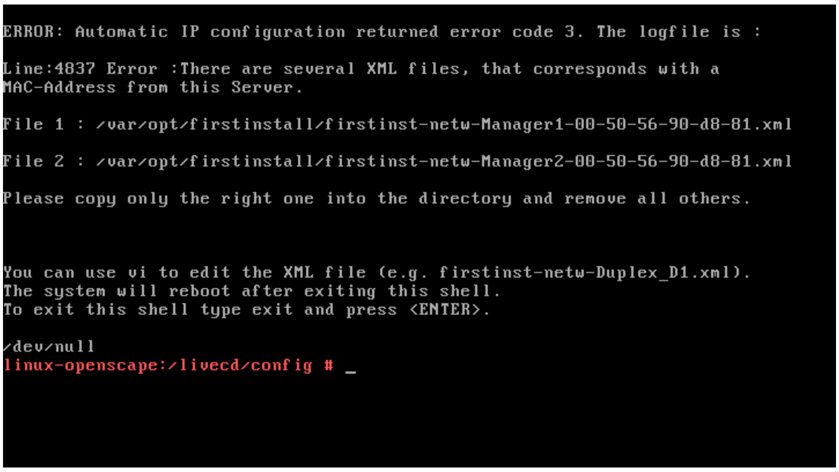


```
ERROR: Automatic IP configuration returned error code 1. The logfile is :
Line:3783 Error : Deployment simplexy is not defined Please use one of
following Deployment


The installation has detected the following XML file matching the system:
firstinst-netw-test_inst1.xml.
You can use vi to edit this XML file.
To exit this shell type exit and press <ENTER>.

linux-hipath4000v6:/livecd/config #
```

Figure 12: First installation - log file for an XML configuration file with error messages

c) **Case 1.3: The XML configuration file contains warnings**

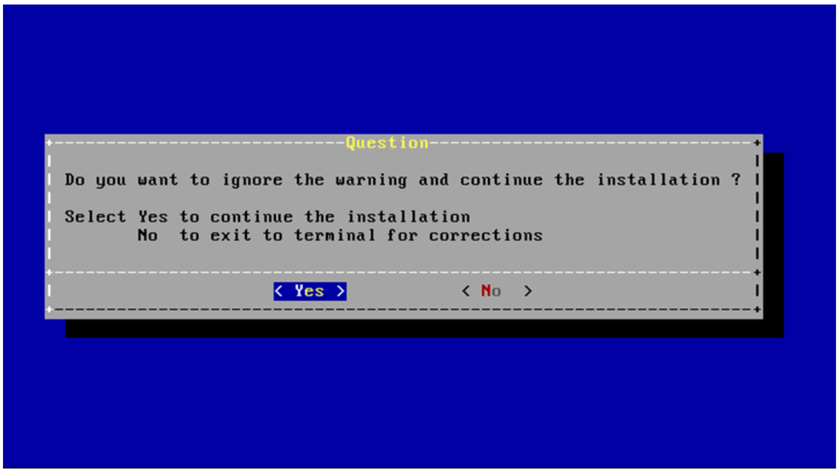
If there are only warnings found in the XML configuration file, these warnings are displayed.



```
ERROR: Automatic IP configuration returned error code 3. The logfile is :

Line:4837 Error :There are several XML files, that corresponds with a
MAC-Address from this Server.

File 1 : /var/opt/firstinstall/firstinst-netw-Manager1-00-50-56-90-d8-81.xml

File 2 : /var/opt/firstinstall/firstinst-netw-Manager2-00-50-56-90-d8-81.xml

Please copy only the right one into the directory and remove all others.


You can use vi to edit the XML file (e.g. firstinst-netw-Duplex_D1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

/dev/null
linux-openscape:/livecd/config # _
```

Figure 13: First installation - XML configuration file with warnings

Press **Continue**. The following screen will be displayed:



```
Question

Do you want to ignore the warning and continue the installation ?

Select Yes to continue the installation
       No  to exit to terminal for corrections
```

Figure 14: First installation - XML configuration file with warnings

Select:

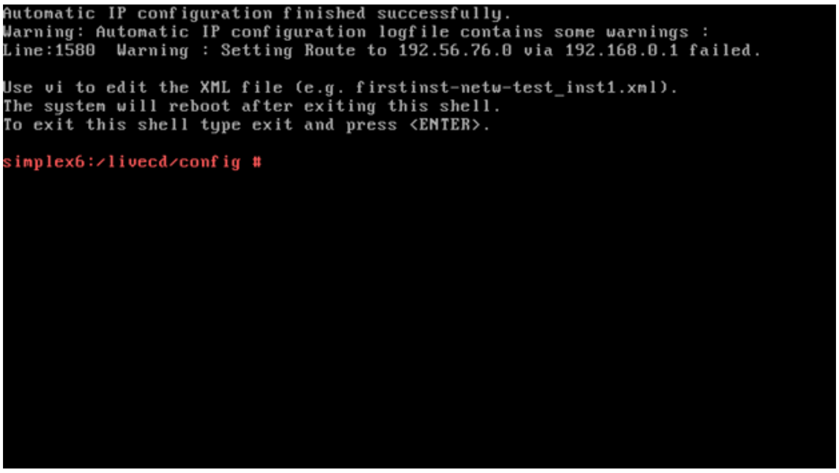
- **Yes** to ignore the warnings and continue the installation procedure.

or

- **No** to exit the installation and open a terminal session for performing the corresponding corrections.

If you select **Yes**, the installation procedure will check the available disk space on the hard disk to determine if the deployment matches the required hard disk space. For more information, please refer to step 5.

If you select **No**, the following screen will be displayed:



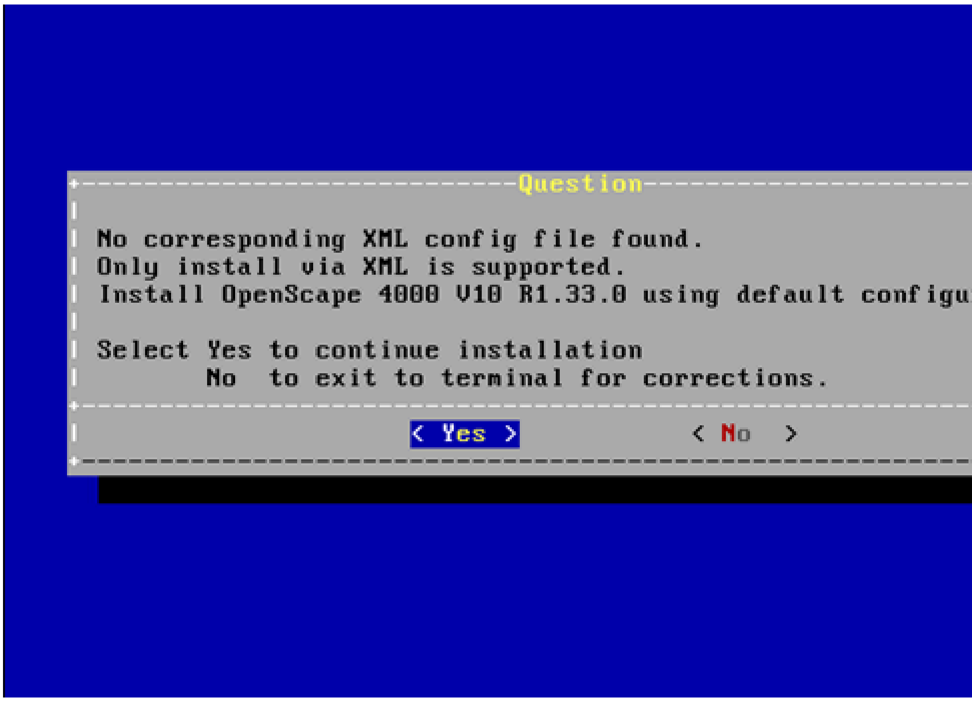
```
Automatic IP configuration finished successfully.
Warning: Automatic IP configuration logfile contains some warnings :
Line:1580  Warning : Setting Route to 192.56.76.0 via 192.168.0.1 failed.

Use vi to edit the XML file (e.g. firstinst-netw-test_inst1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

simplex6:/livecd/config #
```

Figure 15: First installation - Log file for an XML configuration file with warnings

- **Case 2: No XML configuration file found**

  If no XML configuration file is found containing the MAC address from the hardware that is currently running the installation, you can continue the installation using a default configuration or you can start a shell session for doing some corrections.

In case of an incorrect *.xml file name, a warning message will be displayed: "No corresponding XML file...". The file name must start with **firstinst-netw-*.xml**.



```
+---------------------------Question---------------------
|
| No corresponding XML config file found.
| Only install via XML is supported.
| Install OpenScape 4000 V10 R1.33.0 using default configu
|
| Select Yes to continue installation
|        No  to exit to terminal for corrections.
+--------------------------------------------------------
|                    < Yes >            < No  >
+--------------------------------------------------------
```

Figure 16: First installation - XML configuration file not found

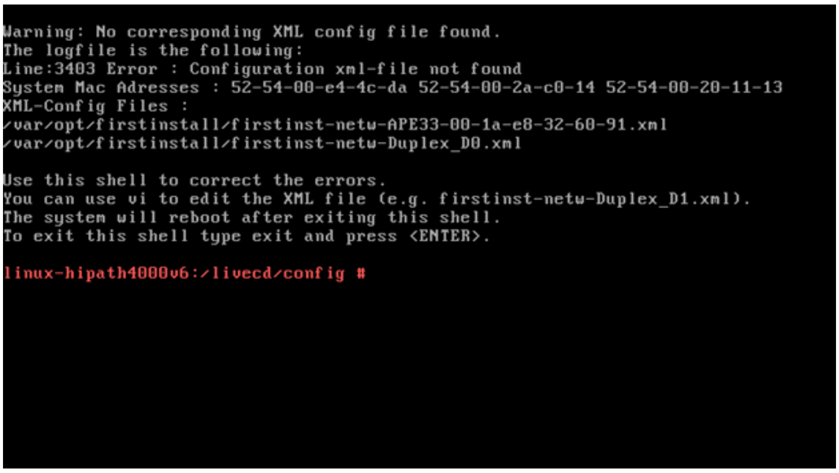
a) **Case 2.1: Installation with default configuration**

If you select **Yes**, the installation will start, but a default IP address will be configured for eth0 (IP address 192.168.0.2 /24). In this case, it is recommended to repeat the installation with a correctly configured XML file.

The installation procedure checks the available disk space on the hard disk and determines the possible deployments. For more information, please refer to step 5.

b) **Case 2.2: Start shell for corrections**

If you select **No**, the following warning will be displayed and you will have the possibility to correct the error.



```
Warning: No corresponding XML config file found.
The logfile is the following:
Line:3403 Error : Configuration xml-file not found
System Mac Adresses : 52-54-00-e4-4c-da 52-54-00-2a-c0-14 52-54-00-20-11-13
XML-Config Files :
/var/opt/firstinstall/firstinst-netw-APE33-00-1a-e8-32-60-91.xml
/var/opt/firstinstall/firstinst-netw-Duplex_D0.xml

Use this shell to correct the errors.
You can use vi to edit the XML file (e.g. firstinst-netw-Duplex_D1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

linux-hipath4000v6:/livecd/config #
```

Figure 17: First installation - Warning no corresponding XML configuration file found

NOTICE: Check if the .xml file is located in the right path and if yes, check also if it contains the correct MAC address of the node. To edit the .xml file you can use the vi editor.

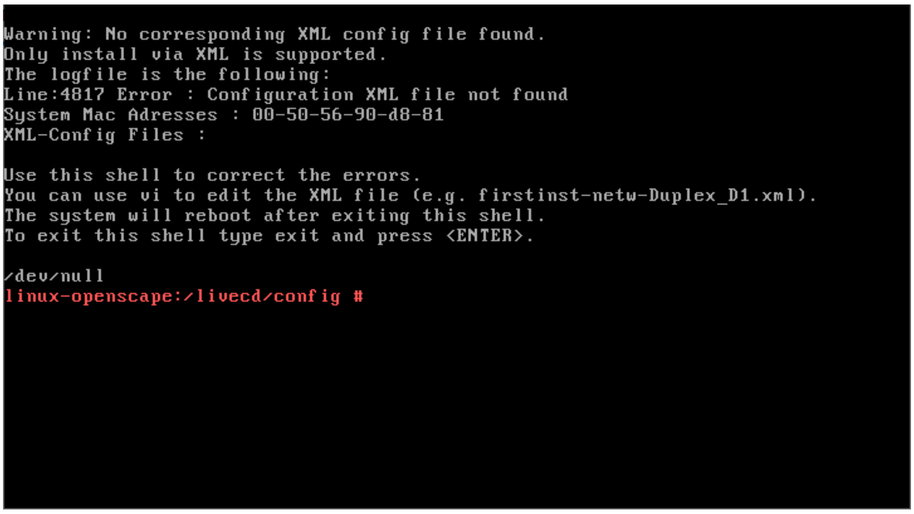
5) Check the available disk space.

There are two possibilities for this step:

- **Case 1: The deployment matches the hard disk size**

  If the hard disk is suitable for the deployment of the XML configuration file, then the procedure will check if the current deployment is a Duplex or a Separated Duplex deployment. For more information, refer to step 6.

6) When the installation finishes successfully, a message will be displayed and you will be asked to remove the installation media and press OK to restart the system.



```
Warning: No corresponding XML config file found.
Only install via XML is supported.
The logfile is the following:
Line:4817 Error : Configuration XML file not found
System Mac Adresses : 00-50-56-90-d8-81
XML-Config Files :

Use this shell to correct the errors.
You can use vi to edit the XML file (e.g. firstinst-netw-Duplex_D1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

/dev/null
linux-openscape:/livecd/config #
```

Figure 18: Installation completed successfully

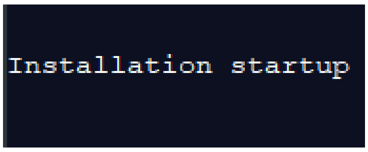
7) After rebooting, the system will start from the installed software on the hard disk, and it can be accessed over any configured IP address for the connected LAN interfaces.

3.3 Installation using only the OLED display and the "ON" button

Starting with V8 R1.19, the OpenScape 4000 Installation on EcoServer can be performed using only the OLED display and the "ON" button which is placed on its left. There is no need to connect either a monitor or a keyboard, as the necessary installation steps are confirmed using the button. This method can be used now for the Manager deployment as well.

Follow the steps below to perform the installation with the OLED display:

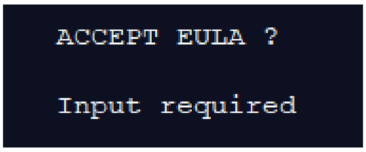
1) Plug in the USB stick, remove all HGs/SSDs and Power on the EcoServer. Wait for about 2-3 minutes for the installation setup. The system will display the "Installation Startup" message.



```
Installation startup
```

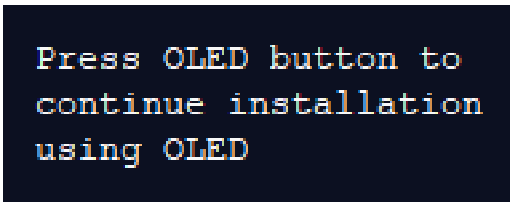
To power cycle the, use the **HW Reset** button.

2) Next, the OLED display will show the message "ACCEPT EULA?". Press the **ON** button.



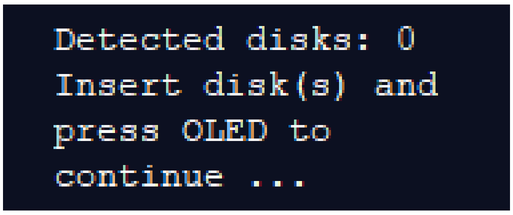
```
ACCEPT EULA ?

Input required
```

3) Wait for the next prompt to be displayed. It will ask to continue the installation using OLED.



```
Press OLED button to
continue installation
using OLED
```

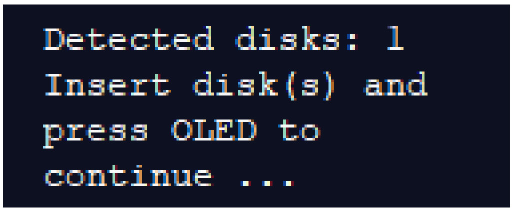
Press the **ON** button and wait until the following message is displayed on the OLED:



```
Detected disks: 0
Insert disk(s) and
press OLED to
continue ...
```

4) At this point, insert one or two HDs/SSDs depending on your deployment and wait for the correct number of disks to be displayed on the OLED.

Press the **ON** button to continue the installation.

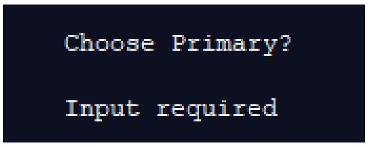


```
Detected disks: 1
Insert disk(s) and
press OLED to
continue ...
```

NOTICE: The display will automatically refresh every 30 seconds.

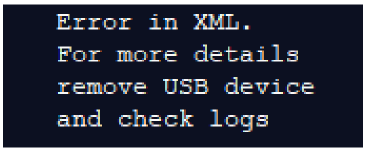
NOTICE: In case of Duplex or GSD systems, the node configured as primary in the XML must be confirmed.

Press the **ON** button to confirm.



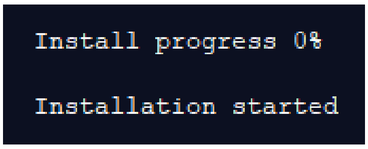
```
Choose Primary?

Input required
```

NOTICE: In case an error has been detected in the XML file (e. g. missing mandatory parameters), the following message will be displayed:



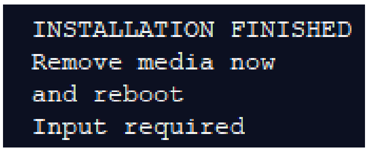
```
Error in XML.
For more details
remove USB device
and check logs
```

While the OpenScape 4000 installation is in progress, the OLED displays the following message:



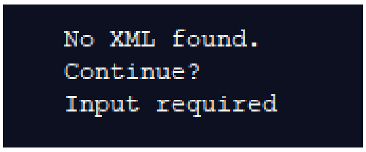
```
Install progress 0%

Installation started
```

5) After the installation finishes, remove the USB drive and press the **ON** button one more time to reboot and start the OpenScape4000 system for the first time.



```
INSTALLATION FINISHED
Remove media now
and reboot
Input required
```

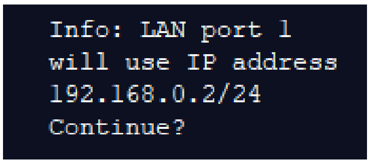
If an installation without XML is performed, the OLED will show the following message:



```
No XML found.
Continue?
Input required
```

Press the **ON** button to continue the installation without XML.

In case of an installation without XML, the OLED will show the IP Address which will be assigned to the first physical LAN interface of the Eco Server. You can connect the first physical LAN interface to a network that has DHCP Server running and then the Eco server will try to obtain an IP address. This will be shown on the OLED for verification purposes. Continue by pressing again the **ON** button. At the end of the installation, the OpenScape4000 Platform Portal will be accessible over that IP address. In case no DHCP answer is received, the default IP address/netmask will be set to 192.168.0.2/255.255.255.0.



```
Info: LAN port 1
will use IP address
192.168.0.2/24
Continue?
```

NOTICE: In case of any errors, remove the USB Stick, check the logs inside the "<usb_stick_root>/_install_logs" directory, then correct the issue(s) and start again from Step 1.

It is recommended to Power OFF the ECO Server/Branch before step 1. Additionally, for it is recommended to remove all HDs, connect the USB Stick and use the HW Reset button to return to step 1.

3.4 OpenScape 4000 installation on Hypervisor

Please check the OpenScape Virtual Machine Resourcing and Configuration Guide for dimensioning the resources required by each deployment.

Information Required from the Customer

- Network identification names e.g.: Management, Voice, Atlantic.
- First installation file firstinst-netw-XXXXX.xml (including the configuration data for OpenScape 4000 Softgate, if this is available).
- Free IP address from the customer address range for the Service PC.
- MAC address.

Service PC

The Service PC is used for the following tasks:

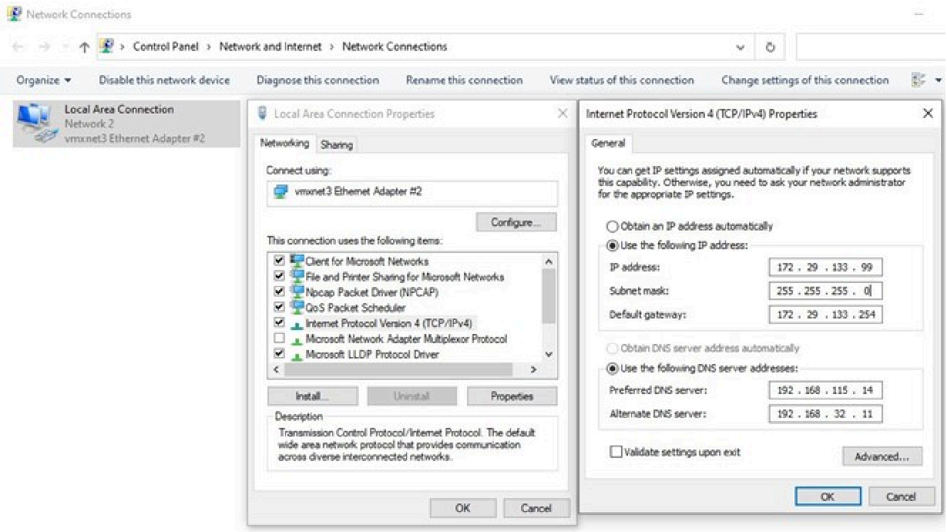
- Accessing the OpenScape 4000 Assistant following the first installation.
- Accessing the OpenScape 4000 with the assistance of OpenScape 4000 Expert Access (=Comwin) following the first installation.
- Using the VMware environment.
- Generating and adapting the configuration files.
- Modifying the OpenScape 4000 ISO file.

Preparations on the Service PC

- Enter a free customer IP address and netmask on the LAN card of the Service PC.

Console > **Start** > **Control Panel** > **Network and Internet** > **Network Connection** > **LanAdapter** > Right mouse-click **Properties** > **TCP / ipV4** > **Properties ...**

Select the **Use the following IP address** radio button and confirm by clicking **OK**.


Network Connections
Control Panel > Network and Internet > Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Local Area Connection
Network 2
vmxnet3 Ethernet Adapter #2
Local Area Connection Properties
Networking
Sharing
Configure...
Install...
Uninstall
Properties
OK
Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Advanced...
OK
Cancel

Connect using: vmxnet3 Ethernet Adapter #2

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 29 . 133 . 99
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 29 . 133 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 115 . 14
Alternate DNS server: 192 . 168 . 32 . 11

□ Validate settings upon exit

Figure 19: Ip address and netmask example for the Service PC

- Create a working path on the PC for:
  - XML file,
  - ISO editor software (e.g AnyBurn),
  - Hotfixes.
- Copy the installation ISO file to a location that can be accessed by the Hypervisor Client (e.g. datastore).

Preparing the OpenScape 4000 ISO file

For ISO handling, users can choose their preferred handling, whereby AnyBurn has been successfully verified.

Creating a custom ISO with mandatory configuration file and optional Hotfixes, allows the user to deploy OpenScape 4000 without the use of additional FLP and HF's image.

IMPORTANT:

- AnyBurn tool. Minimum lab verified version was V5.9.
- The XML configuration file generated from XML Config File Generator (delivered with HiPath 4000 Expert Access) should be copied to the ISO under /config.
- Hotfixes for installation with the ISO should be copied to /hotfixes and activation configured in the XML Config File Generator where necessary.

NOTICE: Former installation method using FLP and HF's image works in legacy mode. No support is offered using this method. The needed resources can be found on installation media under `\DriversAndTools\VMware_Installation_Resources_Legacy_V10`

Preparing the Hotfix Installation

Hotfixes can be activated during the first installation. For this purpose the needed HFs can be directly added to the ISO before installation, under the folder`\Hotfixes`.

3.4.1 OpenScape 4000 installation on VMware ESXi

Openscape 4000 Manager is one of the Openscape 4000 Deployments and the installation is similar to any of the Openscape 4000 deployment.

For details regarding ovf deployment and installation on VMWare, please consult Chapter 3.1 of the OpenScape 4000, Installation, Configuration and Migration, Installation Guide.

3.4.2 OpenScape 4000 installation on Microsoft Hyper-V

Openscape 4000 Manager is one of the Openscape 4000 Deployments and the installation is similar to any of the Openscape 4000 deployment.

For details regarding creation of a Virtual Machine and installation on Hyper-V, please consult Chapter 3.2 of the OpenScape 4000, Installation, Configuration and Migration, Installation Guide.

3.4.3 OpenScape 4000 installation on KVM

Openscape 4000 Manager is one of the Openscape 4000 Deployments and the installation is similar to any of the Openscape 4000 deployment.

For details regarding creation of a Virtual Machine and installation on KVM, please consult Chapter 3.3 of the OpenScape 4000, Installation, Configuration and Migration, Installation Guide.

3.4.3.1 OpenScape 4000 installation on Proxmox VE

Openscape 4000 Manager is one of the Openscape 4000 Deployments and the installation is similar to any of the Openscape 4000 deployment.

For details regarding creation of a Virtual Machine and installation on KVM, please consult Chapter 3.3 of the OpenScape 4000, Installation, Configuration and Migration, Installation Guide.

3.5 Compatibility of OpenScape/HiPath 4000 Systems

This section describes the OpenScape/HiPath 4000 systems supported by the OpenScape 4000 Manager V10.

3.5.1 Supported OpenScape/HiPath 4000 Systems

The OpenScape 4000 Manager V10R0 supports the following OpenScape/HiPath 4000 systems:

- OpenScape 4000 V10
- OpenScape 4000 V8
- OpenScape 4000 V7
- HiPath 4000 V6
- HiPath 4000 V5
- HiPath 4000 V4
- HiPath 4000 V3.0, V3.1
- HiPath 4000 V2.0
- HiPath 4300
- HiPath 4500

The OpenScape 4000 Manager V10R1 supports the following OpenScape/HiPath 4000 systems:

- OpenScape 4000 V10
- OpenScape 4000 V8
- OpenScape 4000 V7
- HiPath 4000 V6

NOTICE: For the administration of OpenScape/HiPath 4000 networks via the OpenScape 4000 Manager it is required to use at the OpenScape 4000 Manager a release equal to or higher than the highest release used on any of the Assistants at the customer's side.

NOTICE: ALL the upgrades of mixed deployments (OpenScape/HiPath 4000 and CMP/UC) have to be done in the specific order of first upgrading the UC and afterwards the OpenScape/HiPath 4000. If the upgrade is done in reverse order (first the OpenScape/HiPath 4000 and then the UC), there will be a phase between the OpenScape/HiPath 4000 upgrade and the UC upgrade where there is no communication between these two products!

3.5.2 Current UPLO2-Versions for Older HiPath 4000 Variants

Please, use the latest available releases of HiPath 4000 variants.

3.6 Connecting to OpenScape 4000

OpenScape/HiPath 4000 systems can be connected to the OpenScape 4000 Manager only via LAN.

3.6.1 LAN Connection for OpenScape 4000

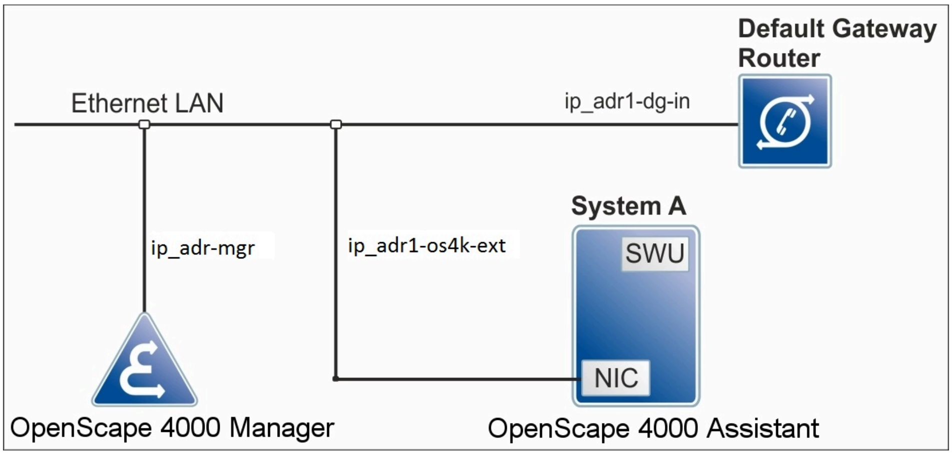


Figure 20: OpenScape 4000 Manager and OpenScape Assistant in the Same Network

In this example, the OpenScape 4000 Manager accesses the ADP of the OpenScape Assistant system directly via the NIC (`<ip_adr-os4k-ext>`). The assigned IP addresses must be unique within this network, i.e., they must not be used more than once. If this network is connected to other networks by means of a router (forming a LAN domain), the uniqueness of addresses must be guaranteed. This is generally handled by the system or network administrator. Since neither the OpenScape 4000 Manager LAN nor the OpenScape Assistant LAN is connected directly (i.e., without a router) to public networks, the assigned IP addresses can be taken from the address ranges assigned to the customer, they do not have to be requested publicly (e.g., from NIC service centers or other providers).

3.6.2 Port Lists

The current portlists for OpenScape 4000 Manager and Assistant can be found in Interface Management Database (IFMDB) at:

- Unify Partner Portal: https://unify.com/en/partners/partner-portal

- From the Intranet: https://apps.g-dms.com:9090/ifm/php/php_ifmdb/login.php

3.7 Configuring SIRA Access

In this scenario we need to configure the router with the Router Configuration Tool (made for Sesap) In that scenario we use NAT to get access from the SIRA Network to the customer devices.

The router is owned by the service organization. The main router type should be the Huawei AR 18-35. In addition we can use a Cisco 836.

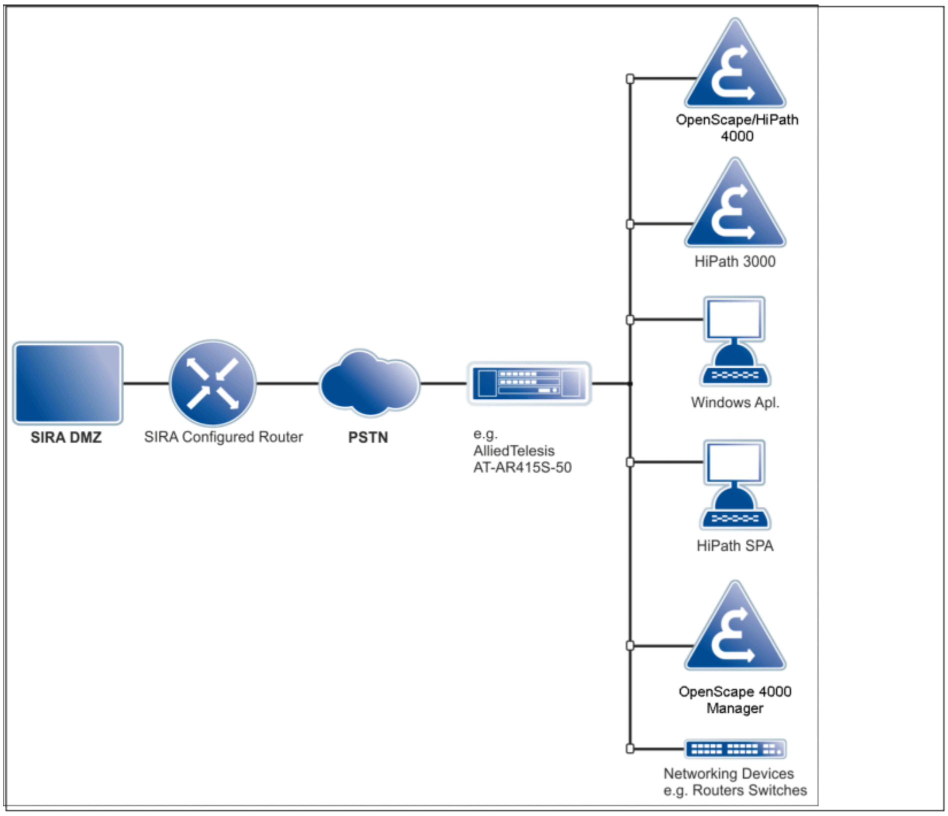
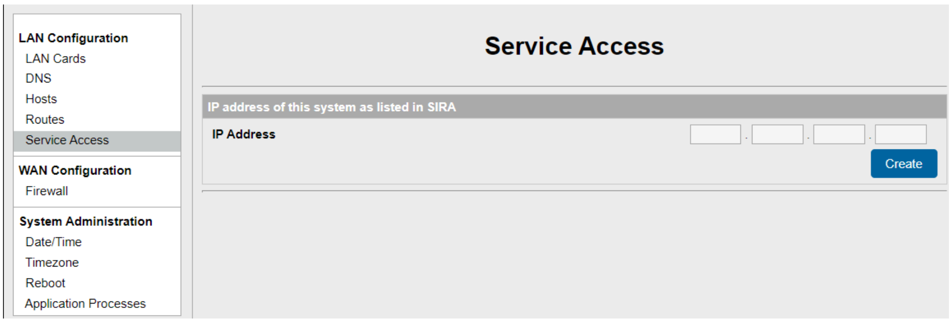


Figure 21: External SPoA (single point of access) provided by Service



Service Access

IP address of this system as listed in SIRA

IP Address . . .

Figure 22: Webmin tool for system base administration

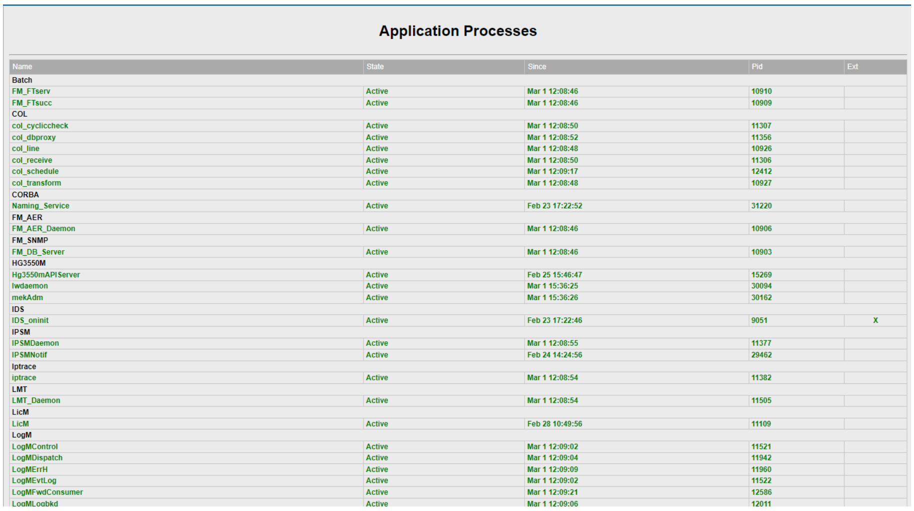
3.8 Verifying Successful Starting of Processes and Components

During the OpenScape 4000 Manager server boot sequence, many independent and dependent processes are started automatically. If any of these processes are not started, OpenScape 4000 Manager may not communicate properly with the managed systems. Following a boot of the OpenScape 4000 Manager server, you can verify that these processes started successfully:

1) Display **Application Processes** Webmin page.

   This page displays the current status of most application processes.

   See Figure 42.



Application Processes

Name	State	Since	Pid	Ext
Batch				
FM_FTserv	Active	Mar 1 12:08:46	10910	
FM_FTsucc	Active	Mar 1 12:08:46	10909	
COL				
col_cycliccheck	Active	Mar 1 12:08:50	11307	
col_dbproxy	Active	Mar 1 12:08:52	11356	
col_line	Active	Mar 1 12:08:48	10926	
col_receive	Active	Mar 1 12:08:50	11306	
col_schedule	Active	Mar 1 12:09:17	12412	
col_transform	Active	Mar 1 12:08:48	10927	
CORBA				
Naming_Service	Active	Feb 23 17:22:52	31220	
FM_AER				
FM_AER_Daemon	Active	Mar 1 12:08:46	10906	
FM_SNMP				
FM_DB_Server	Active	Mar 1 12:08:46	10903	
HG3550M				
Hg3550mAPIServer	Active	Feb 25 15:46:47	15269	
lwdaemon	Active	Mar 1 15:36:25	30094	
mekAdm	Active	Mar 1 15:36:26	30162	
IDS				
IDS_oninit	Active	Feb 23 17:22:46	9051	X
IPSM				
IPSMDaemon	Active	Mar 1 12:08:55	11377	
IPSMNotif	Active	Feb 24 14:24:56	29462	
Iptrace				
iptrace	Active	Mar 1 12:08:54	11382	
LMT				
LMT_Daemon	Active	Mar 1 12:08:54	11505	
LicM				
LicM	Active	Feb 28 10:49:56	11109	
LogM				
LogMControl	Active	Mar 1 12:09:02	11521	
LogMDispatch	Active	Mar 1 12:09:04	11942	
LogMErrH	Active	Mar 1 12:09:09	11960	
LogMEvtLog	Active	Mar 1 12:09:02	11522	
LogMFwdConsumer	Active	Mar 1 12:09:21	12586	
LogMLogbkd	Active	Mar 1 12:09:06	12011	

Figure 23: Webmin process list

2) If any of the processes are in Inactive status, contact the next level of support for assistance.

3.9 CHD links update for Manager V10R1

When upgrading from V6, V7, V8 to V10 there is NO need to follow the procedure in this chapter. With an upgrade to OpenScape 4000 Manager V10R1, all CPTP entries on already existing OpenScape 4000 systems have to be adapted. Otherwise, functions for file transfer, alarm messaging and error messaging on the OpenScape 4000 Manager V10R1 will not work.

With an upgrade to OpenScape 4000 Manager V10R1, the HLB mode has been retired and all switches must be migrated to HLO mode. This is done automatically in the CM database during the HBR restore of previous Manager data. The CPTP entries on already existing OpenScape 4000 systems have to be also adapted using the below instructions.

3.10 Preparing the OpenScape 4000 Manager Client

Before you can use the full scope of features of the OpenScape 4000 Manager, you must provide the necessary software environment for the client PC. This requires to perform the client preparation steps.

The client preparation can be done from the Public Page, while connected to the OpenScape 4000 Manager server.

For more information about client preparation, refer to Client Preparation from the Public Page of the OpenScape 4000 Manager Server .

The OpenScape 4000 Manager is delivered with a pre-installed SSL certificate. It is highly recommended to replace this certificate with an individual certificate for security reasons. Refer to Generating and Activating an Individual Certificate for details.

You can also generate the individual certificate just before the OpenScape 4000 Manager client preparation.

3.10.1 Client Preparation from the Public Page of the OpenScape 4000 Manager Server

To take a guided tour through the complete installation process, do the following:

1) Start the browser.

2) Enter the newly assigned LAN address:

https://<address>/public/cltprep/install/

3) Follow the listed instructions to take a guided tour (recommended for new users) or to begin the installation.

3.10.2 Connecting to OpenScape 4000 Manager

3.10.2.1 Connecting through SSH / SFTP

The SSH/SFTP service is provided by Linux OS and can be used for

- service access,
- access to the XIE file interface

NOTICE: Only the access to Manager Linux Container is allowed and not to the platform OS.

Only users with engr, rsta or rsca security profile or users who have assigned the Access right "Access management - Linux file system" can access Manager through SSH or SFTP.

For more information, please refer to Section 4.6, "User Management – Creating User Names and Assigning Applications".

3.10.3 Generating and Activating an Individual Certificate

Without an individual certificate your browser may display messages that the certificate is invalid and may issue a security warning. Therefore, the preinstalled SSL certificate should be replaced with an individual certificate.

To generate and activate an individual certificate, you need to evaluate one of the 3 options to use:

- a self signed certificate (go to Section 3.6.3.1, "Self signed certificate"), or
- an imported certificate signed by CA (go to Section 3.6.3.2, "Imported certificate signed by CA"), or
- a certificate signed by an official CA and generated via CSR (go to Section 3.6.3.3, "Certificate signed by an official CA and generated via CSR").

3.10.3.1 Self signed certificate

Step A: Generate a certificate

1) On the **Start Page** of **OpenScape 4000 Manager** navigate to **Access Management –> Manage Web Server Certificates –> Certificates for this Web Server**.
2) Click the **Generate** item.
3) Enter all required data in the **Generate Server Certificate (self signed)** dialog and click the **Continue** button.
4) Check the data in the **Display Certificate** dialog. Click the **Continue** button.
5) The program switches to the **Activate Server Certificate** dialog.

Step B: Activate the generated certificate

1) Select the generated certificate in the **Overview of all certificates that can be activated** list.
2) Click the **Activate selected certificate** button.
3) Enter a password for the private key, if required, and click the **Activate Certificate** button.
4) Click the **OK** button in the message box displayed and follow the instructions on the screen.

3.10.3.2 Imported certificate signed by CA

NOTICE: The certificate of the signing CA has to be imported to the trusted root CA store of the web browsers as this is not done by the OpenScape 4000 Manager client preparation.

Step A: Import a certificate

1) On the **Start Page** of **OpenScape 4000 Manager** navigate to **Access Management –> Manage Web Server Certificates –> Certificates for this Web Server**.
2) Click the **Import** item.
3) Enter the appropriate file name.
4) Enter a password for the private key.
5) Click the **Import Certificate** button.
6) The program switches to the **Activate Server Certificate** dialog.

Step B: Activate the imported certificate

1) Select the imported certificate in the **Overview of all certificates that can be activated** list.

2) Click the **Activate selected certificate** button.
3) Enter a password for the private key, if required, and click the **Activate Certificate** button.
4) Click the **OK** button in the message box displayed and follow the instructions on the screen.

3.10.3.3 Certificate signed by an official CA and generated via CSR

Step A: Generate a certificate

1) On the **Start Page** of **OpenScape 4000 Manager** navigate to **Access Management** –> **Manage Web Server Certificates** –> **Certificates for this Web Server**.
2) Click the **Generate via CSR** item.
3) Click the **Generate New Certificate Request** button.
4) Enter all required data in the **Generate Certificate via CSR** dialog and click the **Continue** button.
5) Check data in the **Display Certificate** dialog. Click the **Continue** button.

Step B: Test the generated self-signed certificate

1) Click the **Test** icon in the **Action** column of the table displayed in the **Generate Certificate via CSR** dialog.
2) Activate the generated certificate in the **Activate Server Certificate** dialog.

Step C: Export the certificate

Step D: Send the exported CSR to your Certificate Authority for signing purposes.

1) Open the **Generate Certificate via CSR** dialog.
2) Click the **Export** icon in the **Action** column.
3) Copy the CSR with Copy & Paste or export CSR to file.

Step E: Import the signed certificate

1) Open the **Generate Certificate via CSR** dialog.
2) Click the **Import** icon in the **Action** column.
3) Copy the content of the signed certificate with Copy & Paste or import the signed certificate from file.
4) Enter a password for the private key and click the **Continue** button.

Step F: Activate the signed certificate

1) Open the **Generate Certificate via CSR** dialog.
2) Click the **Activate** icon in the **Action** column.
3) Once you click the **Activate** icon, the web server is restarted automatically.

3.11 Verifying Licensing

The licensing is performed during staging. To verify that the licensing was done correctly, perform the following steps:

1) From the OpenScape 4000 Manager Launchpad, select Access Management and click the License Management application (see Figure 47).

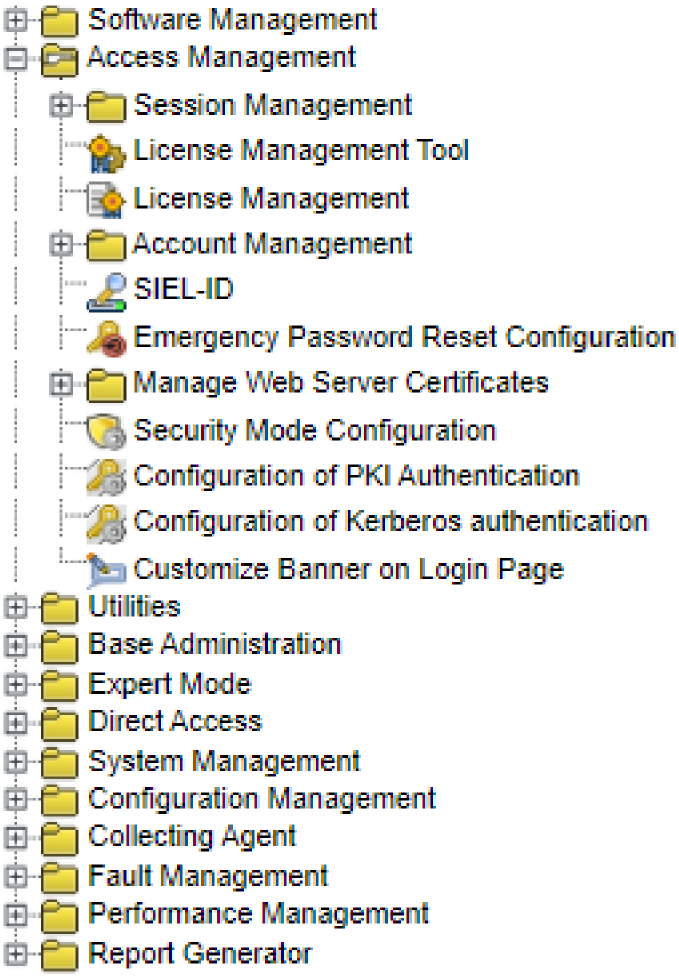


Figure 24: Starting License Management to Verify Server Licensing

2) On the License Management home page (see Figure 48)

=> click Display installed License data to view the licensing data that may have been installed during staging or

=> click **Display CLA IP-Address/DNS Name** to view the address of the configured Customer License Agent.

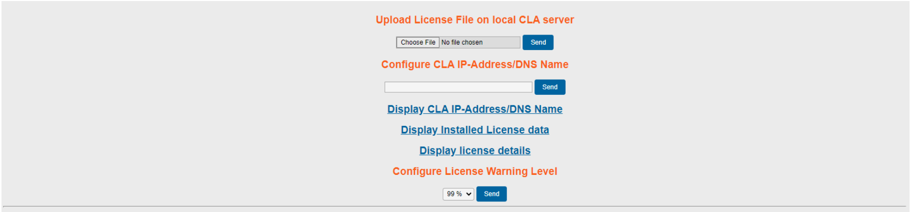

Upload License File on local CLA server
Choose File
No file chosen
Send
Configure CLA IP-Address/DNS Name
Send
Display CLA IP-Address/DNS Name
Display Installed License data
Display license details
Configure License Warning Level
99 %
Send

Figure 25: License Management Home Page

NOTICE: If no licensing data has been installed, refer to Section 5.8, "OpenScape 4000 Manager Server Licensing" for instructions on installing license information.

3.12 Configuring an External Backup Server

In order to save OpenScape 4000 Manager Backup Sets remotely, a compliant SFTP or NFS server has to be installed in the customer LAN. Backup/Restore in OpenScape Manager and Assistant does not support insecure FTP. Only SFTP is supported.

The specific configuration of the SFTP server is out of scope of this manual. Please follow the instructions in the manual provided by the SFTP server vendor.

OpenScape 4000 Manager and Assistant utilize the SFTP client module which has been tested and complies with the SSH File Transfer Protocol (SFTP) protocol version 3 defined by the IETF. Any SFTP server implementing this protocol version can be used as SFTP backup server. Please note that we can not provide support for problems caused by the SFTP server software itself or by its failure to comply with the SFTP protocol definition.

The following SFTP servers have been reported to work with Backup & Restore:

- Linux:
  - OpenSSH
- Windows:
  - OpenSSH based on cygwin
  - SilverSHielD SSH/SFTP Server
  - Free FTPd SFTP Server

NOTICE: Our company can not provide support for problems caused by the SFTP server software itself.

4 Setting Up Systems and Users with OpenScape 4000 Manager

This chapter provides instructions for setting up the OpenScape 4000 Manager System Management software.

4.1 System Management Overview

System Management is the application used to manage network objects in the OpenScape 4000 Manager. In other words, the OpenScape 4000 Manager can be seen as a network element manager for OpenScape/HiPath 4000 communication servers. Therefore, System Management focuses on the administration of OpenScape/HiPath 4000s. Although SNS (System and Network Solutions) products are no longer supported, System Management works for a predefined set of network object types, including OpenScape/HiPath 4000 and Network Management Servers.

System Management is the owner of general system data as well as communication parameters. Application-specific data (for example Performance Management, Collecting Agent or Access Management) are displayed within System Management, but managed by the application itself.

All network objects to be managed by OpenScape 4000 Manager must first be created in System Management. The functionality provided by the System Management GUI is the ability to add, modify, or delete network objects.

System Management may be started from the Launchpad (application tree or menu bar). Upon successful entry into System Management (see Figure 49), a record appears for each managed system.

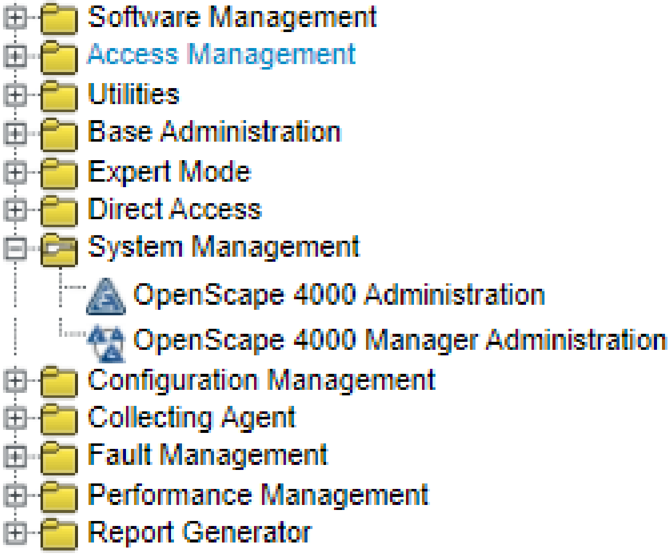


Figure 26: System Management Application Tree

4.2 System Management – Adding OpenScape/HiPath 4000 Systems

NOTICE: For additional information on the screens and fields used in System Management and further instructions on creating the object described in this section, please refer to the mouseover texts and to the online Help.

IMPORTANT: From V10 onwards, the HLB communications mode is no longer supported.

To add a new OpenScape/HiPath 4000 in the OpenScape 4000 Manager server, perform the following steps:

1) On the OpenScape 4000 Manager Launchpad, click System Management.

2) Click OpenScape 4000 Administration (see Figure 50).

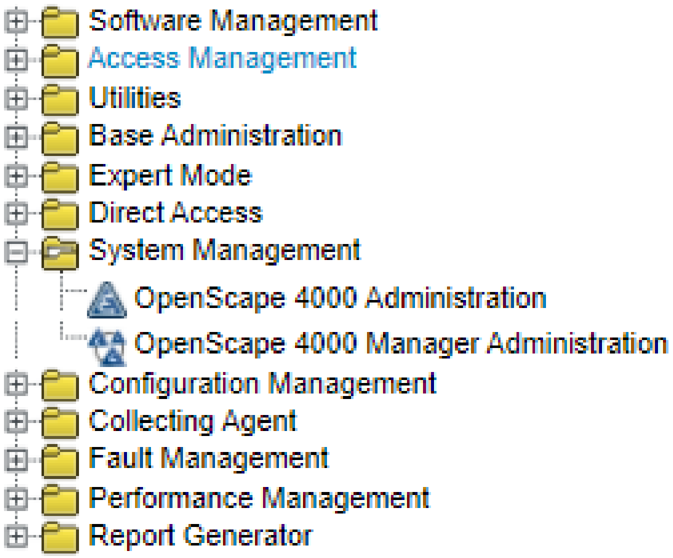


Figure 27: Creating an OpenScape/HiPath 4000 in System Management

3) In the OpenScape 4000 Administration screen, open the Object menu and select New (see Figure 51).

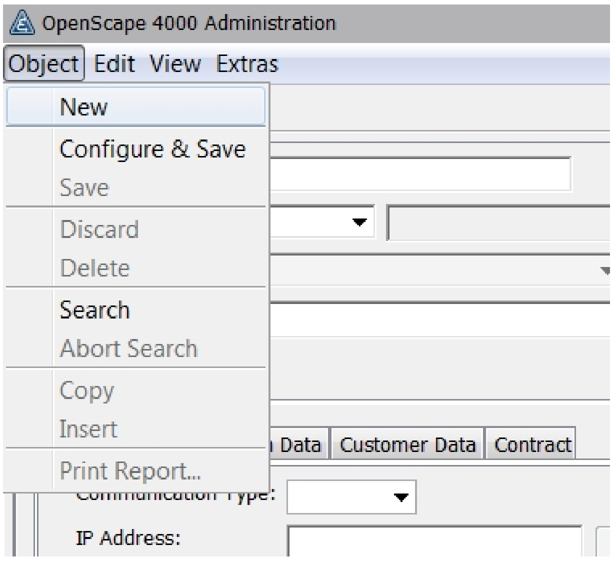


Figure 28: Object Menu in OpenScape 4000 Administration Screen

4) Clicking on the New button in the Object menu or in the lower right corner of the System Management dialog opens the New Object view. If the data of an existing network object has been displayed before opening the New Object view, the contents of certain fields are not deleted, but kept from the previously displayed object in order to ease the creation of the next/new one.

The following fields will not be cleared and will keep the existing data from a previously displayed object:

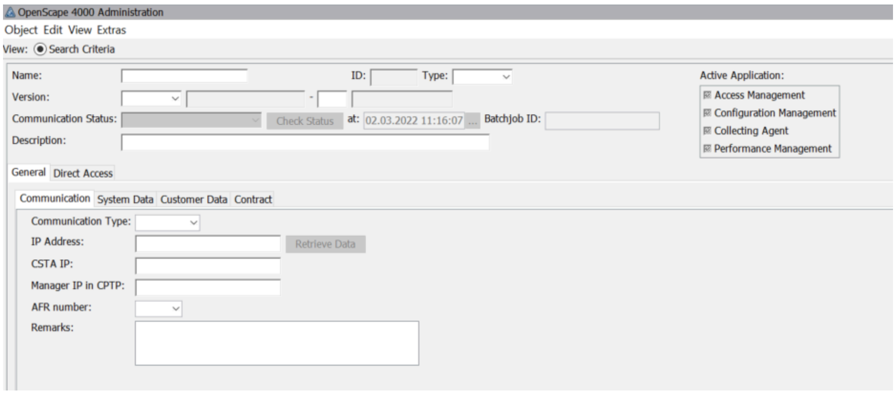
- Version
- Type (HLO)
- Customer Name (displayed on the Customer Data tab sheet)
- Communication Type (Communication tab sheet)
- Domain (System Data tab sheet)
- Node Number (System Data tab sheet)

There is a feature Retrieve Data under the button of the same name, which retrieves all possible OpenScape 4000 information (Assistant, ADP, ...) from the given Assistant's address.

5) Please enter the IP Address and click the Retrieve Data button. The automatic data retrieval via the Assistant uses the default nsl-engr Assistant's account; therefore it should be kept in synch between the Manager and the Assistant. However, you still have the option to enter the Assistant credentials manually if the automatic connection fails.

6) The following fields are retrieved if available: Manager IP in CPTP, AFR number, Version, System Number, Access Point System (also with the APE Number), AMO Language, Domain, Node Number, Time Zone (works

only from the Assistant V7R0 latest Hotfix and newer releases), Contract Number.

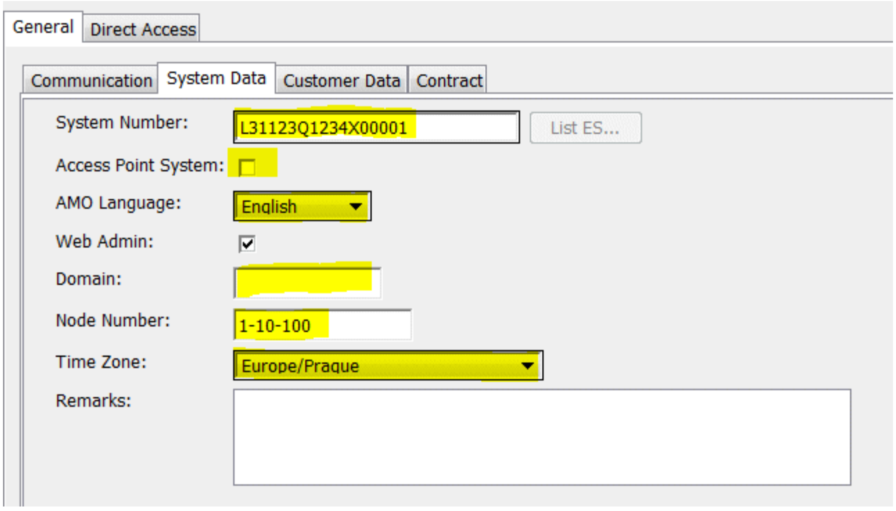


Name:
ID:
Type:
Version:
Communication Status:
at: 02.03.2022 11:16:07
Batchjob ID:
Description:

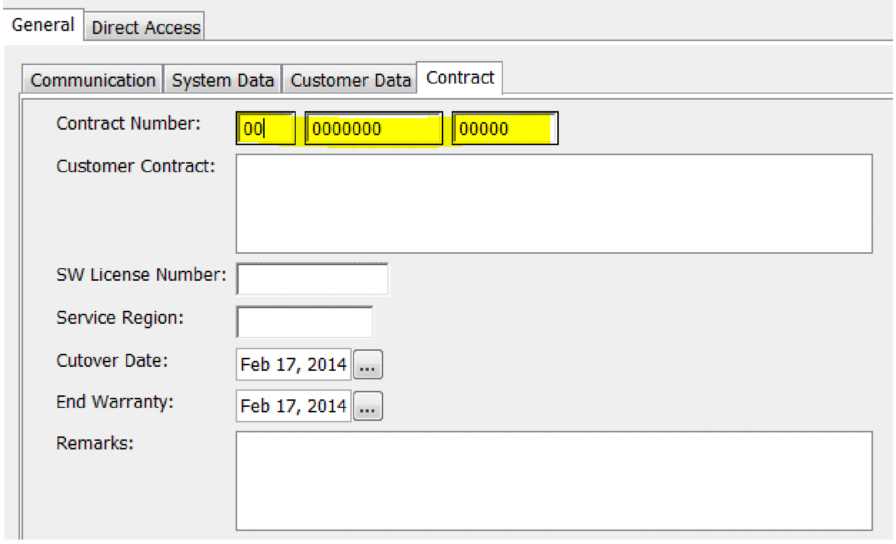
Active Application:
☒ Access Management
☒ Configuration Management
☒ Collecting Agent
☒ Performance Management

Communication Type:
IP Address:
CSTA IP:
Manager IP in CPTP:
AFR number:
Remarks:

Figure 29: New Object - Communication, System Data & Contract Tabs



System Number: L31123Q1234X00001
Access Point System: □
AMO Language: English
Web Admin: ☑
Domain:
Node Number: 1-10-100
Time Zone: Europe/Prague
Remarks:



Contract Number: 00 0000000 00000
Customer Contract:
SW License Number:
Service Region:
Cutover Date: Feb 17, 2014 ...
End Warranty: Feb 17, 2014 ...
Remarks:

7) Fill in the missing mandatory fields – usually Customer Name and Name. Decide which Communication Type you want to use – HLO (see also Table 3). The Manager IP in CPTP is read-only and the AFR number is

mandatory only in case you want to Configure & Save the switch. It is not mandatory for Save only option (see below for more information).

8) Select all other Active Applications that are relevant for this system.

Note that an additional tab appears on the display for each application selected.

Table 1: Hardware Types for OpenScape/HiPath 4000

Hardware Type	Description	Version
HLO	Online connection to OpenScape/HiPath 4000 (FAMOS connection in dialog mode, sending AMO, waiting for answer); default connection type	UV1.0, UV2.0, UV3.0, UV4, UV5, UV6, UV7, UV8, RGV5, RGV6, RGV7
HLB	OpenScape/HiPath 4000 w/ Atlantic LAN and Unix; but without Unix usage by DMS; fallback solution if no other connection works	UV1.0, UV2.0, UV3.0, UV4, UV5, UV6, UV7, UV8
VMSR	Voice Mail Server (without Unix); only for CM usage	
VMSU	Voice Mail Server (with Unix); only for CM usage	

9) Under the General tab, complete the System Data as follows:

a) Enter the System Number if not retrieved automatically

NOTICE: The system number is stored in the AMO ANSU in the OpenScape 4000 communication platform. Although a required field, the OpenScape 4000 Manager server does not validate the OpenScape/HiPath 4000 system number.

b) Make sure the AMO Language is set to the correct value (German or English).

c) Type in the Domain in which the new OpenScape/HiPath 4000 is being added. If this is the first OpenScape/HiPath 4000 to be configured in System Management, a domain may not have been created yet. To create a new domain, refer to Section 4.5.1.3, "Creating a New Domain in OpenScape 4000 Manager".

d) Select the Time Zone for this system from the drop-down list, based on where the system is located. This is required in order to account for time zone differences between the OpenScape 4000 Manager and the systems it manages.

NOTICE: For additional information on date/time administration using OpenScape 4000 Manager, refer to OpenScape 4000 Management, Webmin Base Administration Online Help.

10) Click the Customer Data subtab (see Figure 53).

Enter the Customer Name (mandatory) and other optional information as obtained from the customer.

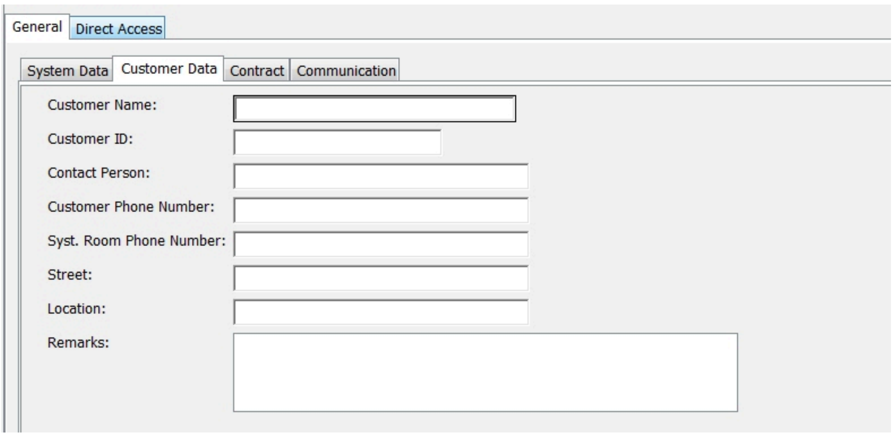
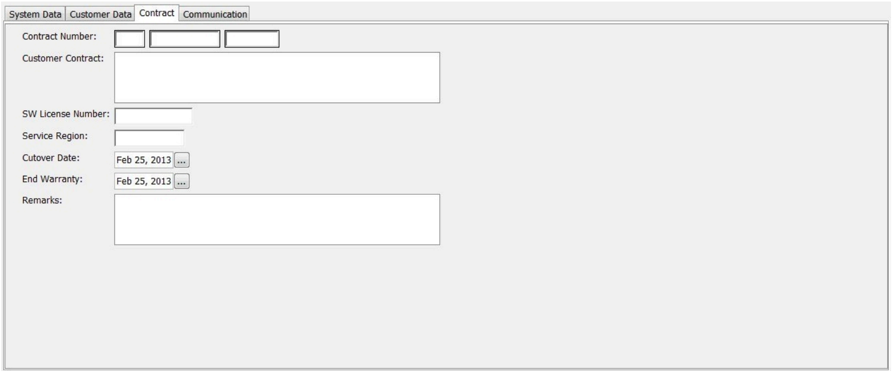


Figure 30: Customer Data Subtab

11) Click the Contract subtab (see Figure 54)

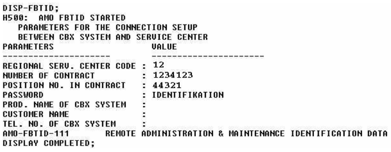
Enter the Contract Number if not retrieved automatically. This is a required field and should be obtained automatically from the AMO FBTID in the corresponding OpenScape/HiPath 4000 (see Figure 55). If the value in the Contract Number field does not correspond to the FBTID information, Fault Management may not work. The remaining data under the Contract subtab can be obtained from the customer.



Cutover Date: Feb 25, 2013

End Warranty: Feb 25, 2013

Figure 31: Contract Subtab



```
DISP-FBTID;
H500:  AMO FBTID STARTED
   PARAMETERS FOR THE CONNECTION SETUP
   BETWEEN CBX SYSTEM AND SERVICE CENTER
PARAMETERS                     VALUE
---------------------          ----------------------
REGIONAL SERV. CENTER CODE :  12
NUMBER OF CONTRACT         :  1234123
POSITION NO. IN CONTRACT   :  44321
PASSWORD                   : IDENTIFIKATION
PROD. NAME OF CBX SYSTEM   :
CUSTOMER NAME              :
TEL. NO. OF CBX SYSTEM     :
AMO-FBTID-111       REMOTE ADMINISTRATION & MAINTENANCE IDENTIFICATION DATA
DISPLAY COMPLETED;
```

Figure 32: AMO FBTID

12) Click the Communication subtab (see Figure 56).

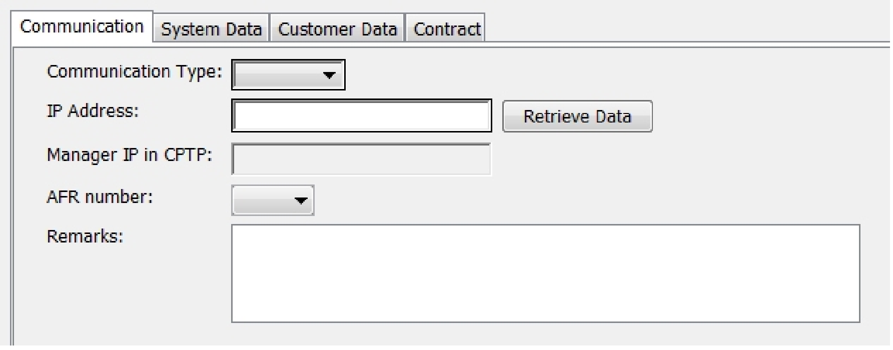


Figure 33: Communication Subtab

13) The only Communication Type supported by Manager is LAN.

14) Please decide whether you want to configure & test the communication to the switch. If yes, please use the button Configure & Save, otherwise use the Save only button.

15) If Configure & Save was clicked and the HLB type is selected, these steps are executed:

- **a)** the GUI data are saved to the DB (chdmain);
- **b)** the AFR number value is mandatory and must be selected;
- **c)** /opt/chd/chd_util.sh –m <mnemonic> is called to update the TNS entries database;
- **d)** /opt/chd/addcptp is called to configure the relevant CPTP, AFR and FTCSM entries on the switch;
- **e)** /opt/chd/hlbtest.sh is called to execute the testing batchjob and the connectivity status;
- **f)** the Communication Status field is changed according to the test result – new status value called "Batchjob failed" is introduced;
- **g)** the new Communication Status is updated in the DB table chdmain, field hicom_status.

16) If Configure & Save is clicked and the HLO type is selected, these steps are executed:

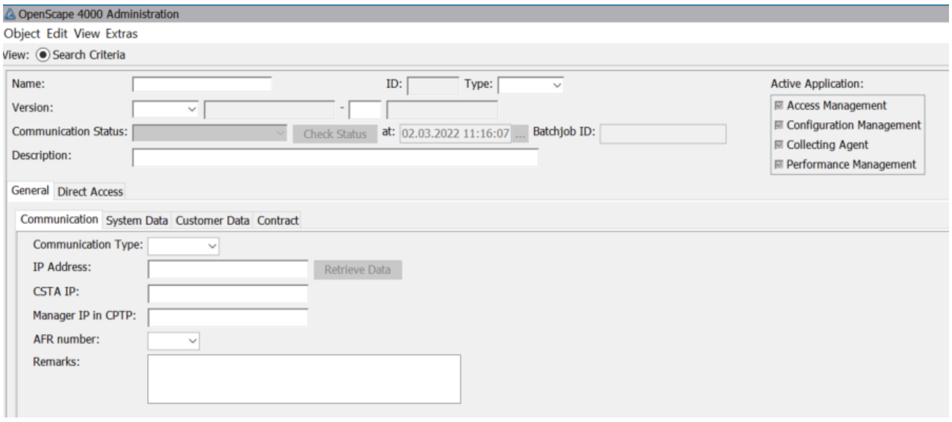
- **a)** the steps a) to d) above are executed;
- **b)** connection to RMX and Assistant is made to test the Communication Status;
- **c)** the Communication Status field is changed according to the test result – new state "IP connectivity failed" is set;
- **d)** the new Communication Status is updated in the chdmain, field hicom_status.

17) Repeat this procedure to create additional OpenScape 4000 IP communication platforms that are administered by the OpenScape 4000 Manager server.

4.3 System Management – OpenScape 4000 Manager Administration

OpenScape 4000 Manager Administration (see Figure 57) allows you to configure the default element that is automatically created when the server is installed. This default element represents the OpenScape 4000 Manager server itself. It is not possible to delete this element or to add more elements of this type.

The name configured for this OpenScape 4000 Manager is the name that appears in the HTML title bar of each Web application, i.e. the first word that is visible when you bookmark applications of the OpenScape 4000 Manager in your browser.



at: 02.03.2022 11:16:07

☒ Access Management
☒ Configuration Management
☒ Collecting Agent
☒ Performance Management

Figure 34: OpenScape 4000 Manager Administration

4.4 Configuration Management Tasks

After all systems have been built in System Management, the following specific tasks must be performed in Configuration Management.

- Perform an upload for each OpenScape/HiPath 4000 (refer to Section 4.5.3)

4.4.1 CM – Domain Management in OpenScape 4000 Manager

This section provides basic information about domains and how they are created and managed in the OpenScape 4000 Manager environment.

4.4.1.1 General Information on Domains

The term domain refers to a single OpenScape/HiPath 4000 or a group of networked OpenScape/HiPath 4000s with unique or closed dial plans.

- A unique or closed dial plan means that there is no duplication of station numbers.
- An open dial plan may contain duplicated station numbers.
- Domain Type 1 means that AMO WABE commands for updating route information will not be sent to all systems in the domain when a station is deleted. An AMO command for deletion of station is sent only to the system where the station exists.
- Domain Type 2 means that AMO WABE commands for updating route information will be sent to all systems in the domain when a station is deleted.

Single OpenScape/HiPath 4000

If an OpenScape/HiPath 4000 is not networked to another OpenScape/HiPath 4000 through CorNet, it belongs to a domain that includes only that OpenScape/HiPath 4000. There can be no repetition of station numbers within a single OpenScape/HiPath 4000; therefore, all station numbers are unique.

Networked OpenScape/HiPath 4000s

If OpenScape/HiPath 4000s are networked together through CorNet, all of the networked OpenScape/HiPath 4000s can belong to the same domain if all of the station numbers are unique. It is not always possible to maintain unique station numbers throughout a network. The Enhanced Private Network Plan (EPNP) provides the capability for location codes to be bonded to station numbers, forming up to twelve-digit complete numbers. Within a network of OpenScape/HiPath 4000s with an open dial plan, the dial plan can become closed if a unique EPNP location code is configured properly in each OpenScape/HiPath 4000. The unique EPNP location codes and the station numbers bond to form unique complete numbers. If all complete numbers are unique within the network of OpenScape/HiPath 4000s, the dial plan is closed. In this scenario, all of the networked OpenScape/HiPath 4000s can belong to a single domain.

OpenScape 4000 Manager provides the capability of managing domains. In OpenScape 4000 Manager, all managed systems in a network, e.g. OpenScape/HiPath 4000, must be assigned to a domain. If the dial plan of the network is closed, then all managed systems within that network can belong to the same domain. However, if the dial plan is open, these systems must be assigned to multiple domains.

4.4.1.2 WABE Configuration

If switches are configured into the same domain, the AMO WABE commands for updating the route information will be sent to all systems in the domain as soon as a station is deleted.

When working with with VNR sub-switches of several physical switches, it is necessary that the AMO WABE information is sent to all systems in a domain; these VNR sub-switches should be defined in one domain and they should have the same virtual node IDs.

The allocation of long WABE ranges causes inefficiencies, slows down the Assistant CM Application and increases the upload duration on the Manager. Please avoid using unnecessary AMO WABE configurations. Tests have shown that a WABE number higher than 50.000 may cause the mentioned inefficiencies.

4.4.1.3 Creating a New Domain in OpenScape 4000 Manager

To create a new domain in the OpenScape 4000 Manager server:

1) From the OpenScape 4000 Manager Launchpad, click the Configuration Management application bar.

2) In the Network folder, double-click Domain (see Figure 58).

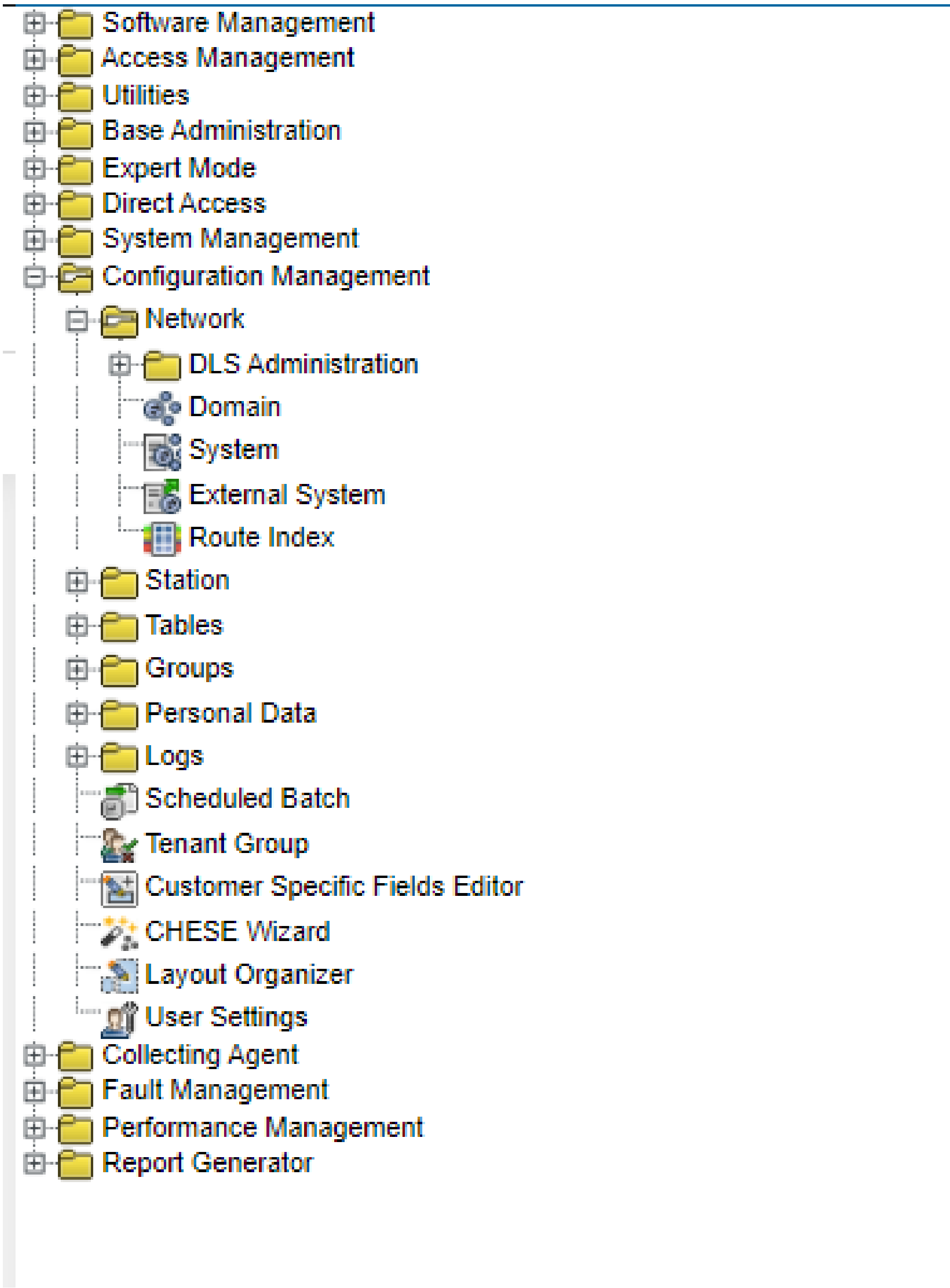


Figure 35: Creating a Domain in Configuration Management

3) In the Domain screen, open the Object menu and select New (see Figure 59).

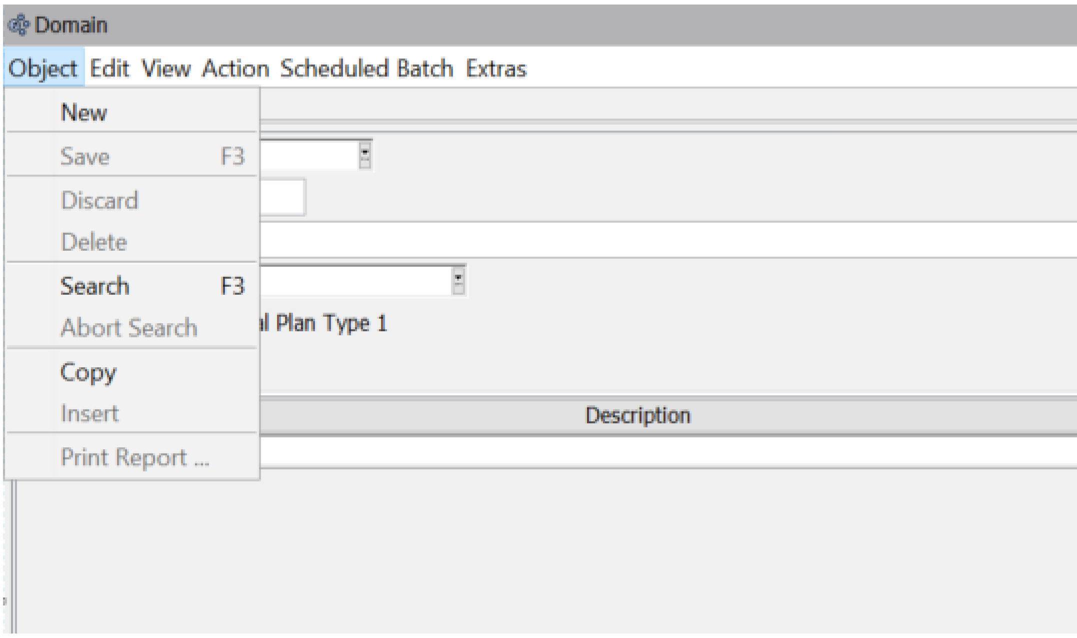


Figure 36: Object Menu in Domain Screen

4) In the Domain field (see Figure 60), enter a unique name for the new domain. This domain name is used to group together systems that are accessed by the same tie line code (closed numbering plan).

> **NOTICE:** The systems assigned to a particular domain are displayed under the Systems tab. The Sub-domain tab displays all systems assigned to a sub-network within this domain.

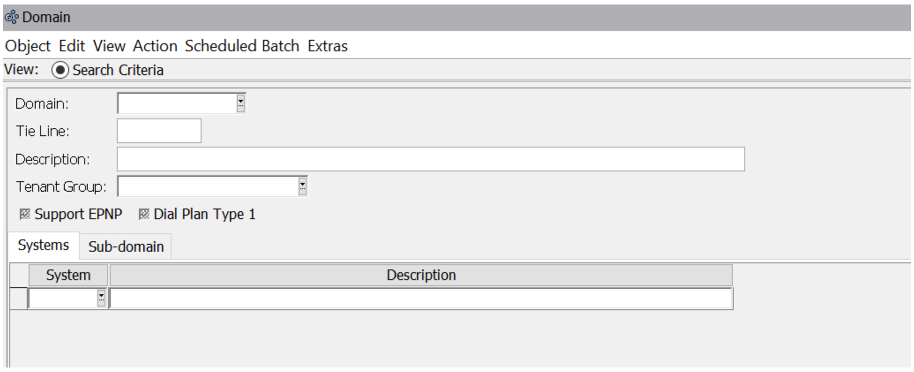


Figure 37: Creating a New Domain Object

5) Enter a brief description of the domain in the optional Description field.

6) Repeat this procedure to create additional domains if needed.

> **NOTICE:**
>
> If using an open numbering plan, multiple domains are required. When adding more than one domain, use the Tie Line field

to specify the tie line code that must be dialed to access this domain from systems in other domains.

The option Support EPNP (Enhanced Private Numbering Plan) must only be activated if the domain in question has U.S.-based systems assigned to it. EPNP is generally used there, rather than ISDN.

The option Dial Plan Type 1 must be activated if the numbering scheme does not apply to the entire domain, but rather is system-based. This means that the stations corresponding to a given block of numbers may be assigned only on one system. Therefore, station numbers in all dial plans must be allocated with their correct destination number, because changes in a dial plan are not broadcast to all systems within the network. The change is made only locally on the corresponding system.

The Tenant Group field can be used to restrict access for administration of the domain to specific users. Users belonging to this tenant group may administer this domain, but other users cannot. In fact, other users will not even be able to view this domain.

4.4.2 CM – Adding a New System in OpenScape 4000 Manager

The System window in Configuration Management can be used to initiate the following actions for the different system types:

- Search an existing system using various criteria
- Upload the system data for
  - Extension data (UPLO2)
  - VoiceMail data (UPLVM)
  - Least Cost Routing data (UPLOL)
- Add a new system
- Change an existing system
- Delete an existing system

To add a new system in Configuration Management:

1) From the OpenScape 4000 Manager Launchpad, click the Configuration Management application bar.

2) In the Network folder, click System (see Figure 61).

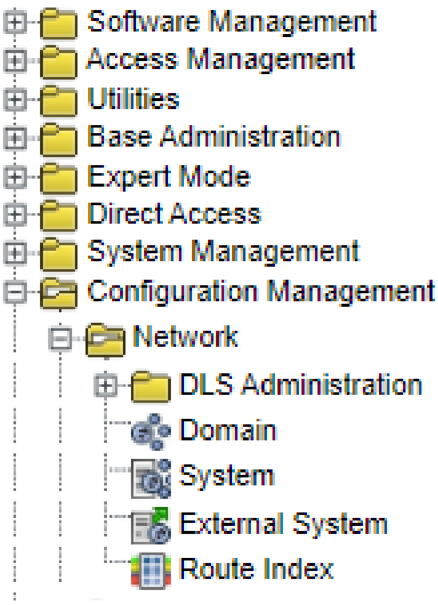
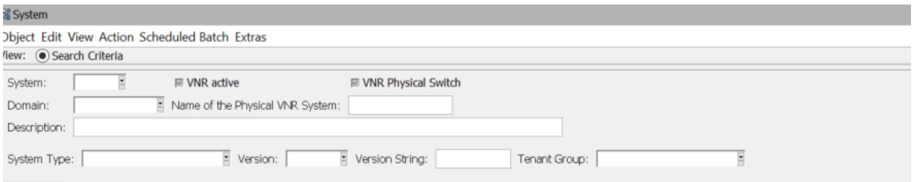


Figure 38: Adding a New System in Configuration Management

3) In the System screen, enter appropriate values in the generic data fields (see Figure 62):



System:
☒ VNR active
☒ VNR Physical Switch
Domain:
Name of the Physical VNR System:
Description:
System Type:
Version:
Version String:
Tenant Group:

Figure 39: Generic Data for a New System in Configuration Management

a) In the System field, enter the System ID (4-character alphanumeric value) as assigned in System Management for this system (refer to Section 4.3, "System Management – Adding OpenScape/HiPath 4000 Systems").

b) In the Domain list, select the domain that was assigned earlier in the Domain screen (refer to Section 4.5.1.3, "Creating a New Domain in OpenScape 4000 Manager").

   Note: The Domain screen may be opened by clicking on the underlined labe (see Figure 62), or by right-clicking inside the Domain field and then selecting 'Related Object' in the drop-down list.

c) The VNR Active check box indicates whether the length-enhancement feature of the extension field is enabled (check box selected) or disabled (check box cleared). With the feature enabled, long extension numbers can be used, i.e. extension numbers in the switch are combined in the following way:

Long Extension = Virtual Node Access Code + Short Extension

(see also Section 5.10, "Using VNR (Virtual Numbering Plan)")

NOTICE:

If the **VNR Active** checkbox is activated, the VNR feature (virtual numbering) has been switched on for this switch. All AMOs use the long number representation; also, AMO UPLO2 delivers all subscribers in long form. Regarding the AMO input, long numbers are accepted.

If the **VNR Active** checkbox is not activated, the user can not add non-unique numbers. All AMOs use short number as input, and UPLO2 also delivers short numbers.

Switching this feature on or off is not possible if there are any non-unique numbers configured on the switch. AMO ZANDE will return an error message in this case.

The Default value of this field is "off".

OpenScape 4000 Configuration Management follows the AMO representation of station numbers. This means, if the global flag is switched off, all station numbers will be represented in its short form and CM will not allow any kind of long number representation in any virtual node of that switch.

Since this feature is not administrated from within the CM but from AMO ZANDE, the user can not change this in the System window. The user can only see whether the VNR feature is switched on or off. The activiation of this feature has to be done via an AMO command.

After the VNR feature has been activated/deactivated by AMO ZANDE and the required subswitch definitions have been made, the user must execute an **Upload All** for that specific switch. The representation of station numbers must be the same on OpenScape 4000 Manager/ Assistant and on the OpenScape/HiPath 4000.

d) The VNR Physical Switch check box indicates whether this switch is VNRAD (VNR Across Domains) or Not as defined in the **Configuration Management** tab sheet for OpenScape/HiPath 4000 network objects in the **System Management** application. If it is activated, the user is able to define subswitches from the subswitch data tab of this screen.

e) The Name of the Physical VNR System text field displays the name of the Physical System that this switch (subswitch) is defined on. For subswitches this value is different from the name of the switch ('system' field). If this is not a subswitch, this value is identical with the 'system' field which represents the switch ID.

f) In the Description field, you may enter your own information for this system.

g) In the System Type list, select the correct type of system. It is very important to select the correct type otherwise there will be a problem with the synchronization of the data from the switch (UPLOADS).

The following options are available:

OpenScape4000 -> for OpenScape 4000 switches

VMSR -> VoiceMail switch without SCO-Unix

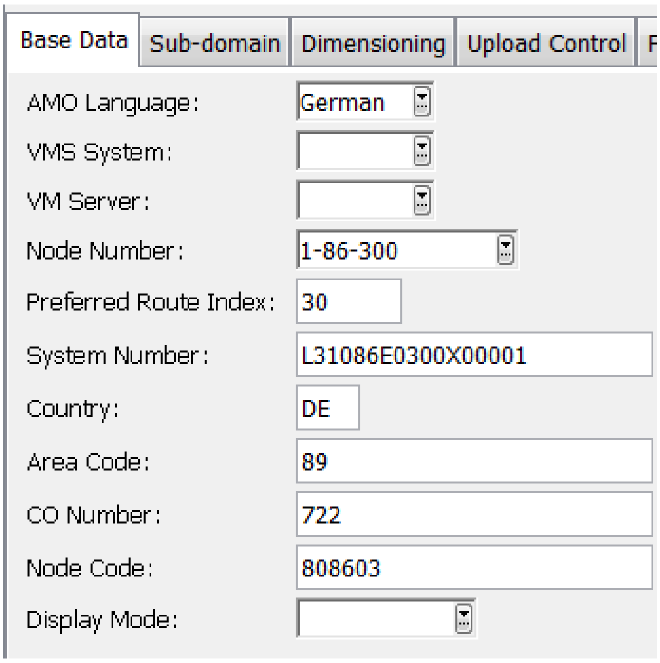
VMSU -> VoiceMail switch with SCO-Unix

h) In the Version list, choose the correct system version. The following values are supported:

- UV1.0, UV2.0, UV3.0, V4, V5, V6, V7, V8, V10(OpenScape 4000)

i) The Tenant Group field can be used to set up access restrictions for the administration of this system. Only users belonging to this tenant group may administer this switch. All other users will have no administration rights; in fact, they will not even be able to view this system.

4) Click the Base Data tab, and enter appropriate values in the following fields (see Figure 63).



AMO Language: German

VMS System:

VM Server:

Node Number: 1-86-300

Preferred Route Index: 30

System Number: L31086E0300X00001

Country: DE

Area Code: 89

CO Number: 722

Node Code: 808603

Display Mode:

Figure 40: Base Data for a New System in Configuration Management (Part 1)

a) In the AMO Language box, select 'German' or 'English' to specify AMO execution language of CM jobs. Generally, the AMO language is not defined in Configuration Management, but rather in System Management (refer to Section 4.3, "System Management – Adding OpenScape/HiPath 4000 Systems").

b) If there is still a Voice Mail Server in operation in your network, use the VMS System field to enter or select the system where the VM is installed.

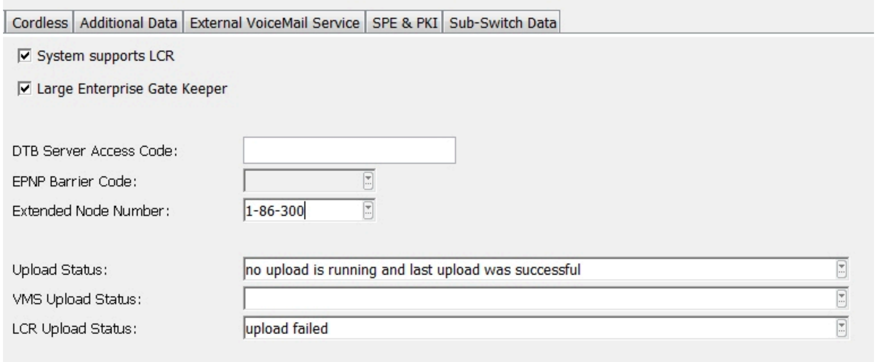
Then, in the VM Server box, select one of the values (V1 - V3, T1 - T3 or A1), depending on the Voice Mail installation.

c) In the Node Number field, enter the node number of the system as defined in the AMO ZAND. In the Preferred Route Index field, enter the destination number of the system. This destination number can be determined on another system in the network using the AMO WABE, namely by executing a REGEN command on an existing extension number for the system being created.

d) In the System Number field, enter the system number as assigned in AMO ANSU for this system.

e) In the Country field, enter the two-character code corresponding to the country in which the system is located, for example DE for Germany. In the Area Code field, enter the code for the city, for example 89 for Munich. In the CO Number field, enter the Central Office Code that is used to access this system, for example 7007 for our company in Munich at Hofmannstrasse.

f) The Node Code will be entered automatically by the Upload. This is the own code of the system assigned in the AMO ZAND.



☑ System supports LCR

☑ Large Enterprise Gate Keeper

DTB Server Access Code:

EPNP Barrier Code:

Extended Node Number: 1-86-300

Upload Status: no upload is running and last upload was successful

VMS Upload Status:

LCR Upload Status: upload failed

Figure 41: Base Data for a New System in Configuration Management (Part 2)

NOTICE: For Steps g) through the end, refer to Figure 64 above.

g) Select the System supports LCR check box, if you also want to capture the LCR-relevant data in the UPLOAD. The option Large Enterprise Gate Keeper will be detected by the upload and automatically activated.

h) The field DTB Server Access Code is important for mobile subscribers. The name keys of a device may be programmed to access the electronic telephone book (DTB-Key, Journal). The default value is 900 and will not be uploaded from the system.

i) The field EPNP Barrier Code is important for the US-specific dialing plan of the type EPNP using open numbering (PNP), to prevent conflicts between the location codes and extension numbers.

j) In the field Extended Node Number, the node number will be entered automatically for those systems which conform to the three-part node numbering scheme. In the case of older systems which do not conform to this numbering system, the node number can be adapted to the three-part numbering scheme here. For example, the node number 301of an older V3.4 system was adapted by entering 1-85-301 in the Extended Node Number field.

k) The fields Upload Status, VMS Upload Status and LCR Upload Status are strictly informational fields, displaying the current status of each type of upload.

l) Review all parameter values on the Base Data tab page, then click Save to save these settings.

m) Next, upload all relevant system data, as follows: (If the system is VNR, follow the instructions in step 5 below before continuing with the Upload):

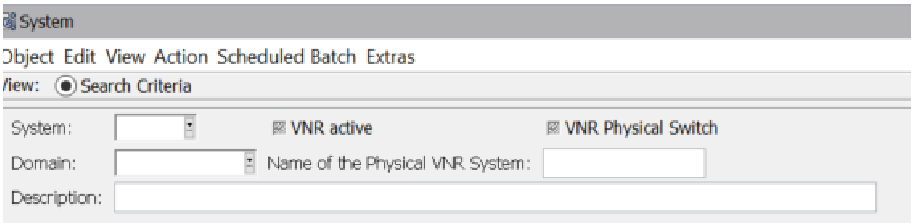
- Open the Action menu and select the menu item Upload. This initiates the retrieval of extension data for this system by Configuration Management.
- If applicable, initiate the retrieval of LCR data by selecting LCR Upload in the **Action** menu.
- If there is a Voice Mail Server associated with this system, upload the VMS data by selecting VMS Upload in the **Action** menu.

Upon completion of these uploads, the system-related data will also be displayed on the other tab pages.

5) To add a new subswitch in Configuration Management:

If the system is VNR, it is required to define the subswitches properly before startingthe Upload; otherwise the Upload will fail because of misconfiguration.

Click the **Sub-Switch Data** Tab and enter the appropriate subswitch information for that switch.



System

Dbject Edit View Action Scheduled Batch Extras

/iew: ● Search Criteria

System: ☒ VNR active ☒ VNR Physical Switch

Domain: Name of the Physical VNR System:

Description:

Figure 42: Generic Data and Sub-Switch tab for a New System in Configuration Management

a) This tab is used to define subswitches for the VNR systems. The **VNR Physical Swtich** field above should be checked for this VNR switch in order to define subswitches for it. The Administrator is expected to know the Virtual Node configuration of the switch before adding the subswitches.

b) The **Sub-switch ID** is the 4 character name of the switch which will be displayed in the **System** field. In this table, exactly the same number of subswitches should be defined as there are Virtual Nodes in the physical system.

c) The **Virtual Node ID** is the ID of the Virtual Node that this subswitch corresponds to on the switch. If there will be other subswitches from other VNR Physical Nodes in the Domain of this subswitch, the administrator needs to verify that they all have the same Virtual Node ID.

d) The **Virtual Node Access Code** is the Access Code of the Virtual Node that this subswitch corresponds to on the switch. If there will be other subswitches from other VNR Physical Nodes in the Domain of this subswitch, the administrator needs to verify that they all have same Virtual Node Access Code.

e) The domain of the subswitch is defined in the **Domain** field. It is important that all subswitches of the same physical node are in different domains.

Either an existing Domain can be selected from the choicelist or a new Domain name is entered (in this case, this domain will be created automatically).

f) The tie line of the domain of the subswitch is entered into the **Tie Line** field. Please note that the tie line of each domain in the network must be unique.

g) The **Route Index** represents the Preferred Destination Number that other switches can use while routing to this switch.

h) In the **Description** field, you may enter additional information about this system.

i) As soon as you click on Save, the new subswitches are created; they can then be searched and displayed from the System Dialog. They will have their own values for the parameters entered into this tab (name, Virtual Node ID, Virtual Node Access Code, Domain, Tie Line, Route Index and Description), but the other Virtual Node independent values will be copied from the physical system since they are common for every switch of the physical node.

j) The upload is done as described above; however, it can only be started for physical switches for VNR systems. It is not possible to start an Upload for a subswitch; this makes sure all subswitches of a system are uploaded together.

k) For the rest of the screens only subswitches will be displayed in the system field. Physical switches are displayed only in the System Dialog.

4.4.3 Uploading Systems

After all systems have been built in System Management and in Configuration Management, the OpenScape 4000 Manager server must be synchronized with the managed OpenScape/ HiPath 4000 systems. This database synchronization ensures that the OpenScape 4000 Manager server reflects the current system status.

Synchronization is achieved by performing an Upload from Configuration Management on each OpenScape/HiPath 4000. OpenScape 4000 Manager Configuration Management provides a graphical user interface for system administration of these systems.

4.4.3.1 Uploading an OpenScape/HiPath 4000

To upload an OpenScape/HiPath 4000:

1) From the OpenScape 4000 Manager Launchpad, click Configuration Management, then Network, then System (see Figure 66).

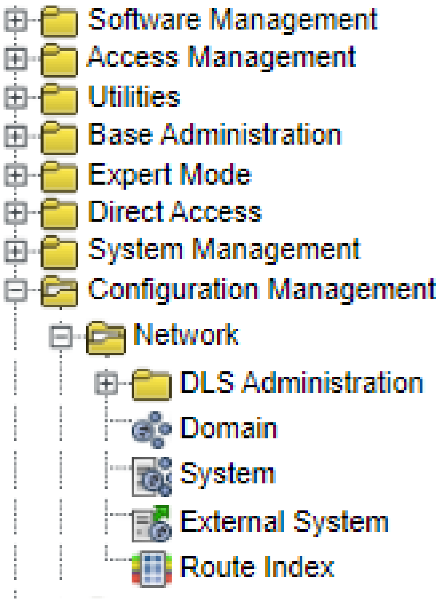


Figure 43: Initiating Uploads of OpenScape/HiPath 4000 from Configuration Management

2) In the System dialog box, click the Search button to search for all OpenScape/HiPath 4000s configured in System Management.

3) Use the ◀ and ▶ keys to select the OpenScape/HiPath 4000 system to be uploaded.

4) In the Configuration Management - System dialog box, open the Action menu again, then click Upload.

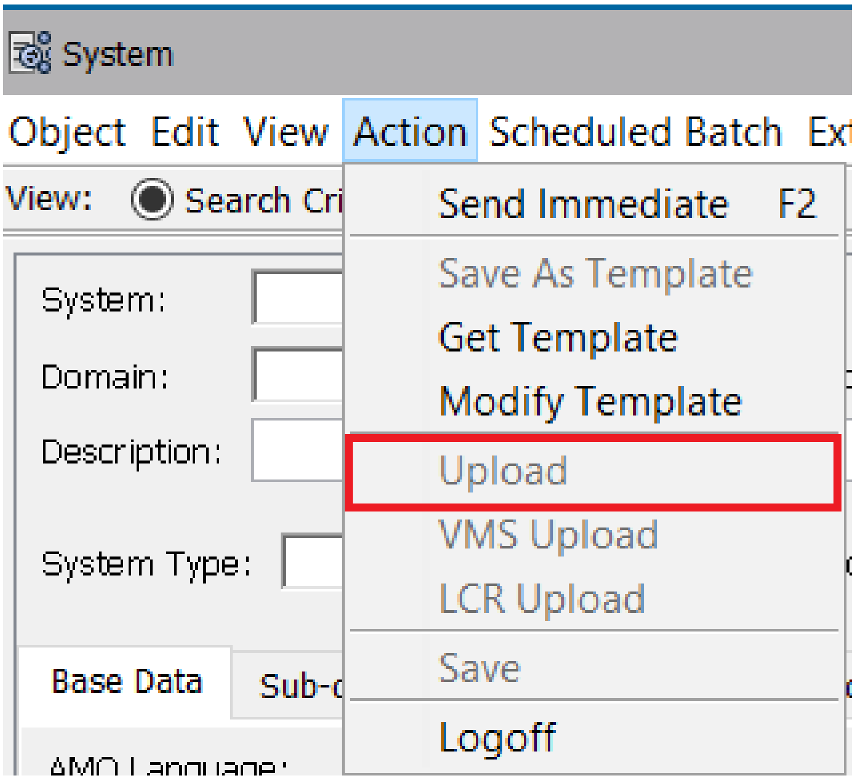


Figure 44: System Dialog Box, Action Menu

- Case 1: No Previous Uploads Performed

  If no previous uploads have been performed (new system), Configuration Management allows only an Upload All. Upload All is a total synchronization of the OpenScape 4000 customer database. As a result of an Upload All, all OpenScape 4000 Manager-related customer data is duplicated in the OpenScape 4000 Manager server.
- Case 2: Previous Uploads Performed If previous uploads have been performed, Configuration Management provides a choice of upload types:
  - Upload All
  - Upload Delta

NOTICE: The first time that an OpenScape/HiPath 4000 performs an Upload All to the OpenScape 4000 Manager server, a "snapshot file" is created in the OpenScape/HiPath 4000, which lists all of the customer database information that was duplicated in the OpenScape 4000 Manager server. When a subsequent Upload Delta is requested from the OpenScape 4000 Manager server, the OpenScape/HiPath 4000 compares the current customer database to the existing "snapshot file". Only the variances in the current configuration are sent to the OpenScape 4000 Manager server. Therefore, an Upload Delta typically runs much faster than an Upload All.

5) Click either Start Upload All or Start Upload Delta.

6) Click OK to start the selected Upload.

7) To perform Uploads on other OpenScape/HiPath 4000s, select the next record and repeat the Upload procedure.

4.4.3.2 Scheduling Periodic Uploads for OpenScape/HiPath 4000

After a system's initial Upload-All, periodic synchronizations must be scheduled. These synchronizations can be scheduled to occur daily or weekly. All scheduled uploads are delta uploads, which occur on the pre-selected day or days at 10:00 p.m.(default).

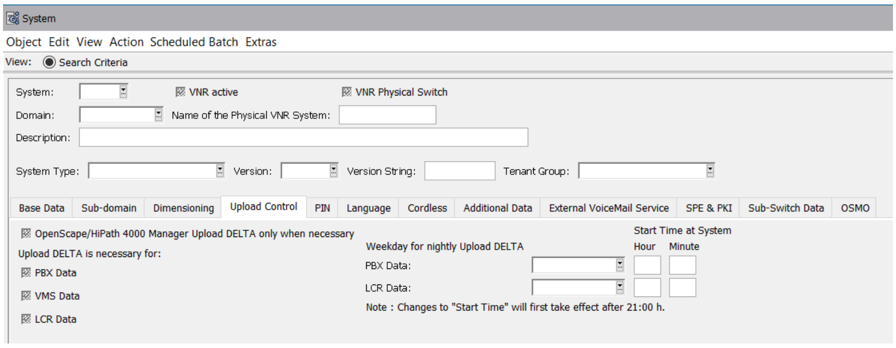
To schedule synchronization, perform the following steps:

1) From the OpenScape 4000 Manager Launchpad, click Configuration Management and double-click System.

2) In the System dialog box, click the Search button to search for all OpenScape/HiPath 4000s configured in System Management.

3) Use the ◀ and ▶ keys to select the OpenScape/HiPath 4000 system to be uploaded.

4) In the Configuration Management - System dialog box, click the Upload Control tab.



View: ● Search Criteria

System: ☒ VNR active ☒ VNR Physical Switch

Domain: Name of the Physical VNR System:

Description:

System Type: Version: Version String: Tenant Group:

☒ OpenScape/HiPath 4000 Manager Upload DELTA only when necessary

Upload DELTA is necessary for:

☒ PBX Data

☒ VMS Data

☒ LCR Data

Start Time at System

Weekday for nightly Upload DELTA Hour Minute

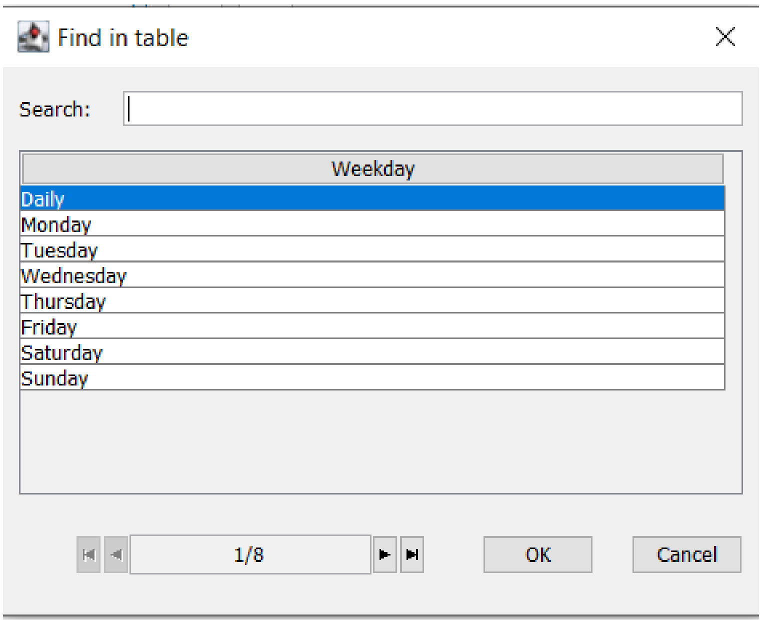
PBX Data:

LCR Data:

Note : Changes to "Start Time" will first take effect after 21:00 h.

Figure 45: System Dialog Box, Upload Control Tab

5) Under Weekday for Nightly Upload-DELTA, open the list box (PBX Data or LCR Data) to display the selection list labeled Find in table.



Find in table

Search:

Weekday
Daily
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday

1/8

6) Click the day of the week (or Daily option) on which the Upload-Delta is to be performed.

7) Click OK to return to the System dialog box.

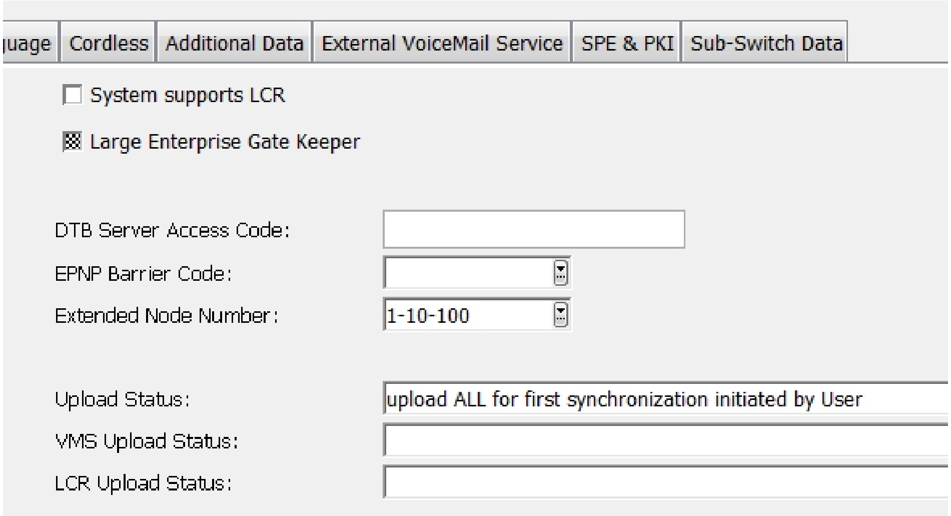
8) Click Save to save the changes.

9) In response to the confirmation question from Configuration Management, click OK to execute the change, or Cancel to ignore the change.

10) To schedule uploads on other OpenScape/HiPath 4000s, select the corresponding system record and repeat the procedure.

4.4.3.3 Viewing the Upload Status for OpenScape/HiPath 4000

In Configuration Management, the current upload status for OpenScape/HiPath 4000 can be viewed from the Base Data tab of the System dialog box.



☐ System supports LCR

▨ Large Enterprise Gate Keeper

DTB Server Access Code:

EPNP Barrier Code:

Extended Node Number: 1-10-100

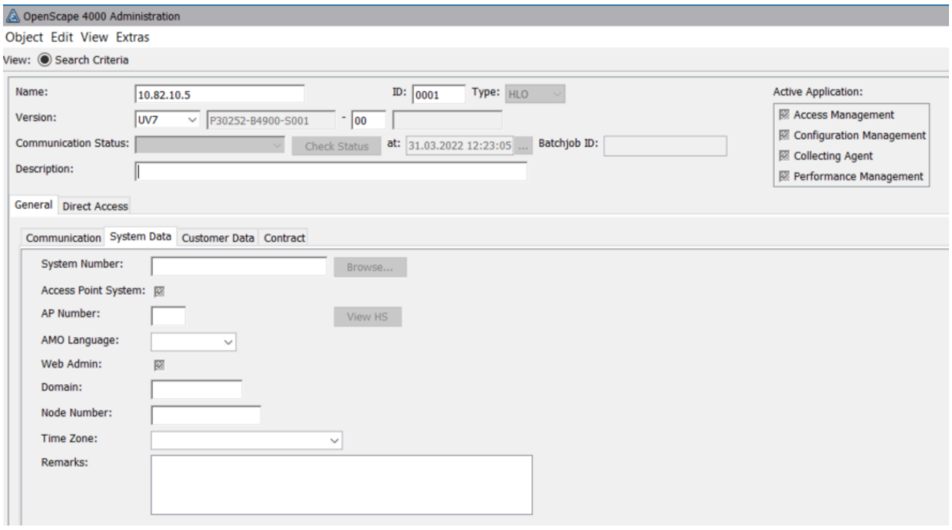
Upload Status: upload ALL for first synchronization initiated by User

VMS Upload Status:

LCR Upload Status:

Figure 46: Viewing the Upload Status in Configuration Management

The upload status can also be viewed from the Configuration Management tab for this OpenScape/HiPath 4000 in System Management.



Name: 10.82.10.5
ID: 0001
Type: HLO
Version: UV7 P30252-B4900-S001 - 00
Communication Status:
at: 31.03.2022 12:23:05
Batchjob ID:
Description:

Active Application:
☒ Access Management
☒ Configuration Management
☒ Collecting Agent
☒ Performance Management

System Number:
Access Point System: ☒
AP Number:
AMO Language:
Web Admin: ☒
Domain:
Node Number:
Time Zone:
Remarks:

Figure 47: Viewing the Upload Status in System Management

4.5 User Management – Creating User Names and Assigning Applications

The Access management defines five different security levels or user roles inside of the Manager Linux Container.

NOTICE: The root access to the platform is only intended for trouble shooting and for placing any customized data or scripts.

The predefined security levels are shown in Table 4 below.

Table 2: Security Levels in Access Management

Security Level	Predefined User Account	Linux Container Shell Access	Owner	Remarks
engr	engr	yes	Service	Engineer; To be used in emergency cases only. Includes all other security levels. Access to Linux Shell with superuser rights (uid 0).
rsta	rsta	yes	Service	Remote Service Technical Assistance; Used by upper level service technicians. Includes security level rsca.
rsca	rsca	yes	Service	Remote Service Customer Assistance; Used by lower level service technicians.
cusa	cusa	no	Customer	Customer Security Administrator; Used by the customerâs "master" admin- istrator(s). Includes security level cust.

Security Level	Predefined User Account	Linux Container Shell Access	Owner	Remarks
cust	----	no	Customer	Customer level; Individual accounts can be created at runtime to fit into the customer-specific environment.

All predefined accounts have a preset default password which is to be changed upon first logon. Individual accounts can be created according to the individual customer's needs. This ability requires logging on with a security level of cusa, rsca, rsta, or engr.

Each OpenScape 4000 Manager Client must use a unique user name. These additional user names are created in OpenScape 4000 Manager Access Management. Each user name is customized by assigning applications to meet the requirements of the user. When OpenScape 4000 Manager Clients use unique, customized user names, the user can only perform the tasks assigned to the user name.

To create a new user name and assign applications, perform the following steps:

1) On the OpenScape 4000 Manager Launchpad, click the Access Management application bar.

2) Under Account Management, click User Account Administration.

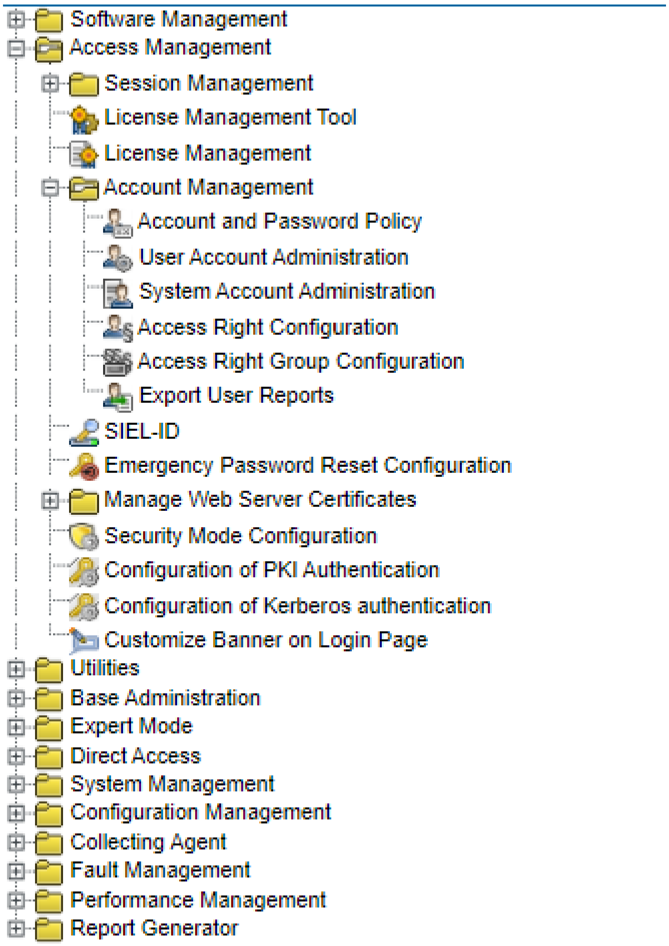

Software Management
Access Management
Session Management
License Management Tool
License Management
Account Management
Account and Password Policy
User Account Administration
System Account Administration
Access Right Configuration
Access Right Group Configuration
Export User Reports
SIEL-ID
Emergency Password Reset Configuration
Manage Web Server Certificates
Security Mode Configuration
Configuration of PKI Authentication
Configuration of Kerberos authentication
Customize Banner on Login Page
Utilities
Base Administration
Expert Mode
Direct Access
System Management
Configuration Management
Collecting Agent
Fault Management
Performance Management
Report Generator

Figure 48: Starting User Account Administration to Add a New User

3) In the User Account Administration dialog box, open the User menu and click Add.

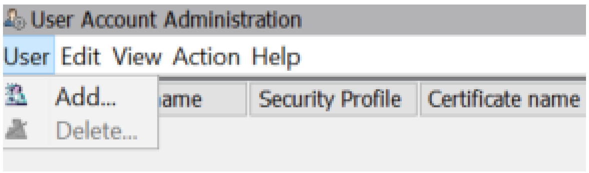


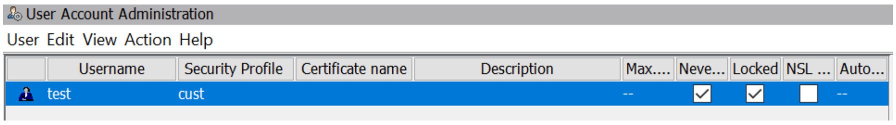
Figure 49: User Administration Dialog Box

4) In the Add New User dialog box, enter a unique user name in the New username field, and a brief description in the Description field. The **Certificate Name** should be filled only if the PKI infrastructure is used for login to the system. Select a Security Level for the user. The Default user is "cust". For a list of security levels, see Table 4.

5) Click OK.

NOTICE: Note that the new user name is added to the list in the User Account Administration dialog box.

6) Enter the following information on the right-hand side of the User Account Administration dialog box:



User Account Administration

User Edit View Action Help

	Username	Security Profile	Certificate name	Description	Max....	Neve...	Locked	NSL ...	Auto...
	test	cust			--	☑	☑	□	--

Figure 50: Completing the Information for a New User

a) Enter a New Password, then Retype Password. This password is used by the new user during the initial login attempt.

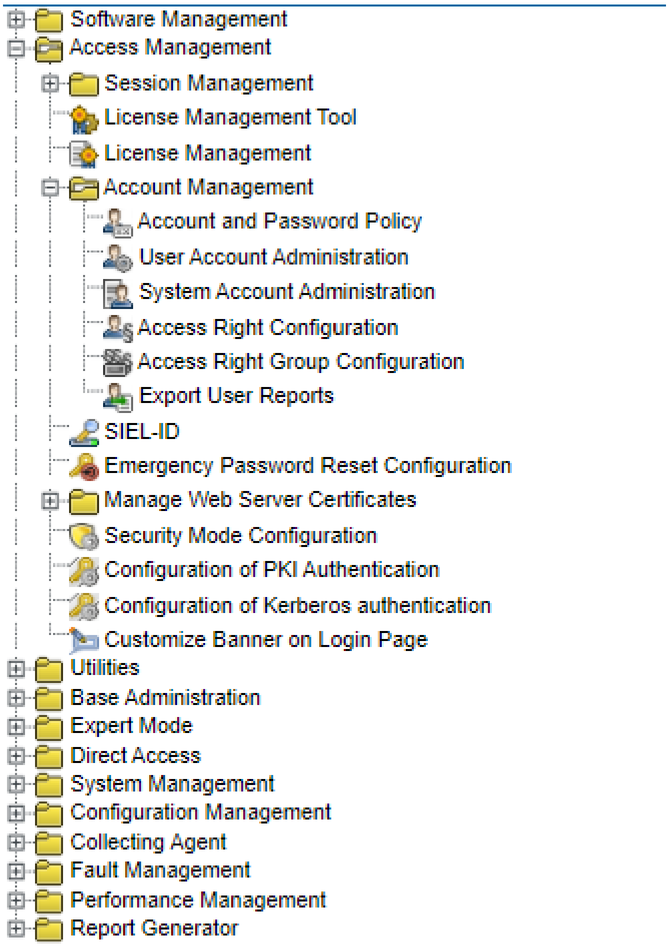
b) Click Force Password Change to prompt the new user to change the password after successfully logging on for the first time.

c) Set the Properties according to the customer-specific requirements.

7) Click Apply to save the new user's attributes.

8) Close the User Account Administration application.

9) Access rights can be defined for users with the security role 'cust'. Under Access Management on the Launchpad, click Access Right Configuration.

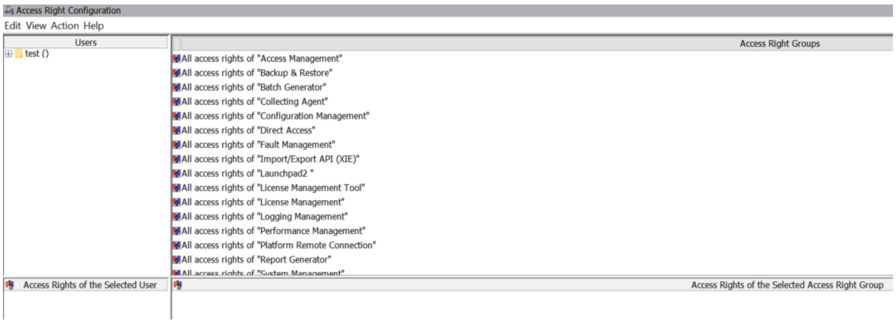


- Software Management
- Access Management
  - Session Management
  - License Management Tool
  - License Management
  - Account Management
    - Account and Password Policy
    - User Account Administration
    - System Account Administration
    - Access Right Configuration
    - Access Right Group Configuration
    - Export User Reports
  - SIEL-ID
  - Emergency Password Reset Configuration
  - Manage Web Server Certificates
  - Security Mode Configuration
  - Configuration of PKI Authentication
  - Configuration of Kerberos authentication
  - Customize Banner on Login Page
- Utilities
- Base Administration
- Expert Mode
- Direct Access
- System Management
- Configuration Management
- Collecting Agent
- Fault Management
- Performance Management
- Report Generator

Figure 51: Starting Access Right Configuration

10) In the Access Right Configuration window, select the new user name on the left, then select the access rights being assigned to the user from the column on the right.

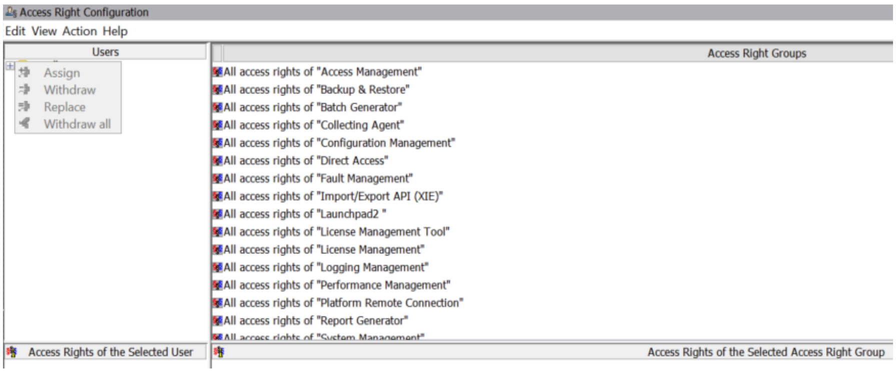
> **NOTICE:** In the example shown here, all available access rights are being assigned to the user. Use the Shift key or Ctrl key accordingly to select specific combinations or ranges of features. Refer to the online Help for more detailed instructions.


Access Right Configuration
Edit View Action Help
Users
test ()
Access Right Groups
Access Rights of the Selected User
Access Rights of the Selected Access Right Group

All access rights of "Access Management"
All access rights of "Backup & Restore"
All access rights of "Batch Generator"
All access rights of "Collecting Agent"
All access rights of "Configuration Management"
All access rights of "Direct Access"
All access rights of "Fault Management"
All access rights of "Import/Export API (XIE)"
All access rights of "Launchpad2 "
All access rights of "License Management Tool"
All access rights of "License Management"
All access rights of "Logging Management"
All access rights of "Performance Management"
All access rights of "Platform Remote Connection"
All access rights of "Report Generator"
All access rights of "System Management"

Figure 52: Selecting Access Rights to be Assigned to New User

11) To activate the assignment, open the Edit menu and select Assign.


Access Right Configuration
Edit View Action Help
Users
Assign
Withdraw
Replace
Withdraw all
Access Right Groups
Access Rights of the Selected User
Access Rights of the Selected Access Right Group

All access rights of "Access Management"
All access rights of "Backup & Restore"
All access rights of "Batch Generator"
All access rights of "Collecting Agent"
All access rights of "Configuration Management"
All access rights of "Direct Access"
All access rights of "Fault Management"
All access rights of "Import/Export API (XIE)"
All access rights of "Launchpad2 "
All access rights of "License Management Tool"
All access rights of "License Management"
All access rights of "Logging Management"
All access rights of "Performance Management"
All access rights of "Platform Remote Connection"
All access rights of "Report Generator"
All access rights of "System Management"

Figure 53: Assigning Access Rights in Access Management

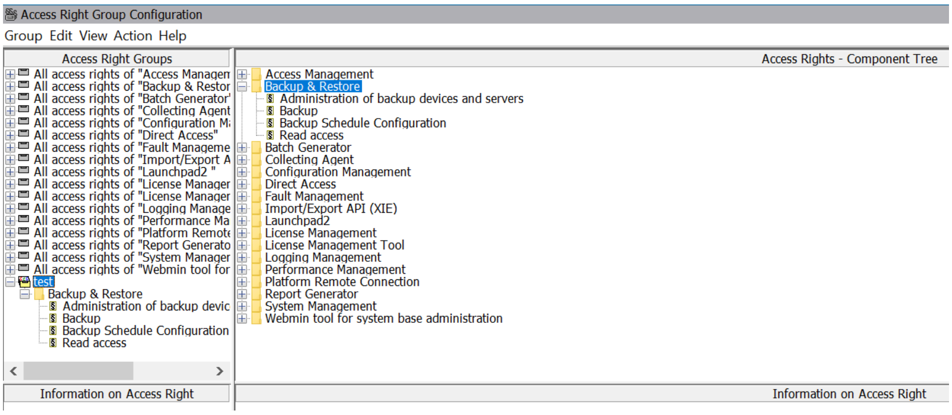
> **NOTICE:** Alternatively, you can click the Assign button in the upper right of the screen

12) To add another user name, repeat this procedure.

4.6 User Management – Configuring Access Right Groups

In the Access Right Group Configuration dialog box, you can create your own access right groups as needed for the users you created. Access Right Groups are used to administer the user rights for executing and using the applications available in the OpenScape 4000 Manager.

Immediately following initial installation, there are already some predefined access right groups available. The Access Right Group Configuration dialog box can be used to modify the existing groups or to create additional groups. Any changes made in an access right group will affect all users assigned to this access right group. Newly created access right groups are assigned to users in the 'Access Right Configuration' dialog box.


Access Right Group Configuration
Group Edit View Action Help
Access Right Groups
Access Rights - Component Tree
Information on Access Right
Information on Access Right

All access rights of "Access Managem
All access rights of "Backup & Restor
All access rights of "Batch Generator'
All access rights of "Collecting Agent
All access rights of "Configuration Ma
All access rights of "Direct Access"
All access rights of "Fault Manageme
All access rights of "Import/Export A
All access rights of "Launchpad2 "
All access rights of "License Manager
All access rights of "License Manager
All access rights of "Logging Manage
All access rights of "Performance Ma
All access rights of "Platform Remote
All access rights of "Report Generato
All access rights of "System Manager
All access rights of "Webmin tool for
test
- Backup & Restore
  - Administration of backup devic
  - Backup
  - Backup Schedule Configuration
  - Read access

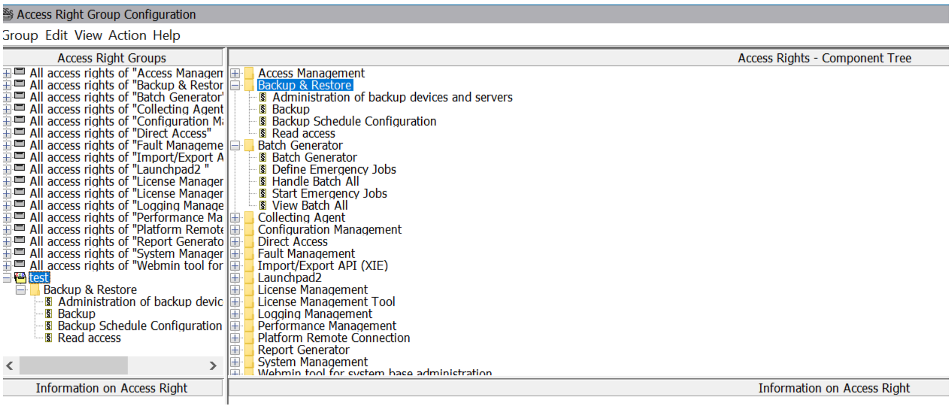
Access Management
Backup & Restore
- Administration of backup devices and servers
- Backup
- Backup Schedule Configuration
- Read access

Batch Generator
Collecting Agent
Configuration Management
Direct Access
Fault Management
Import/Export API (XIE)
Launchpad2
License Management
License Management Tool
Logging Management
Performance Management
Platform Remote Connection
Report Generator
System Management
Webmin tool for system base administration

Figure 54: Created Access Right Group 'Administrator'

Components of the User Interface

The dialog box is divided into two parts. The left side shows all the access right groups (predefined, self-defined and dynamic) with their tree structure. The right side shows the access right groups and their available elements, which can be assigned to the self-defined access right groups. Each side has its own preview panel, which displays the elements of the access right group in detail. These preview panels may be activated or deactivated. The predefined access right groups on the left side may be used to create a new derived access right group by copying the default group, thereby allowing it to inherit all the rights from the predefined group. The group created in this way can then be modified as needed. The different access right groups on the left side may be hidden for a better overview.


Access Right Group Configuration
Group Edit View Action Help
Access Right Groups
Access Rights - Component Tree
Information on Access Right
Information on Access Right

All access rights of "Access Managem
All access rights of "Backup & Restor
All access rights of "Batch Generator'
All access rights of "Collecting Agent
All access rights of "Configuration Ma
All access rights of "Direct Access"
All access rights of "Fault Manageme
All access rights of "Import/Export A
All access rights of "Launchpad2 "
All access rights of "License Manager
All access rights of "License Manager
All access rights of "Logging Manage
All access rights of "Performance Ma
All access rights of "Platform Remote
All access rights of "Report Generato
All access rights of "System Manager
All access rights of "Webmin tool for
test
- Backup & Restore
  - Administration of backup devic
  - Backup
  - Backup Schedule Configuration
  - Read access

Access Management
Backup & Restore
- Administration of backup devices and servers
- Backup
- Backup Schedule Configuration
- Read access

Batch Generator
- Batch Generator
- Define Emergency Jobs
- Handle Batch All
- Start Emergency Jobs
- View Batch All

Collecting Agent
Configuration Management
Direct Access
Fault Management
Import/Export API (XIE)
Launchpad2
License Management
License Management Tool
Logging Management
Performance Management
Platform Remote Connection
Report Generator
System Management
Webmin tool for system base administration

Figure 55: Tree Structure for the Access Right Group "Administrator"

4.7 User Management – Creating and Changing Passwords

4.7.1 Administrator changes the password for the user

Use the User Account Administration application in Access Management to create passwords for new users (refer to Section 4.6, "User Management – Creating User Names and Assigning Applications").

If the OpenScape 4000 Manager system administrator enters a password for a user, the password is subject to the following conditions:

- It must contain one or more alphanumeric characters.
- Alphabetical characters are case-sensitive.
- Special characters can be included.

If a user changes the password, the new password must (by default):

- Contain between six and sixteen total characters, including special characters.
- Contain at least one special character.
- The new password must differ from the previous password in at least 3 characters.

4.7.2 Account and Password Policy

The Account and Password Policy application is used to activate and configure advanced rules for password policies and rules for time-controlled account use.

Start the application

The Configuration page for configuring account and password policy is accessible from the start page: Under Account Management, select Account and Password Policy.

Configuration and activation of password rules

All future account passwords, both administrative and non-administrative, must comply with the configurable rules (xx values are configurable in application):

- Passwords must be at least xx characters long.
- Passwords must contain a specified mix of upper case letters, lower case letters, numbers, and special characters.
- The re-use of any of the previous xx passwords must not be possible.
- A change of passwords must not be allowed more than once in xx days, except for administrators or privileged users. Privileged users may be required to reset a user's forgotten passwords and the ability to change passwords more than once per day.
- If a password is changed, the new password must differ from the previous password by at least xx characters.
- If a password is changed, users must not be able to use dictionary words.

NOTICE: The password rules and account rules only become enabled if the corresponding checkboxes are checked. The 'passwd' command line tool is disabled!

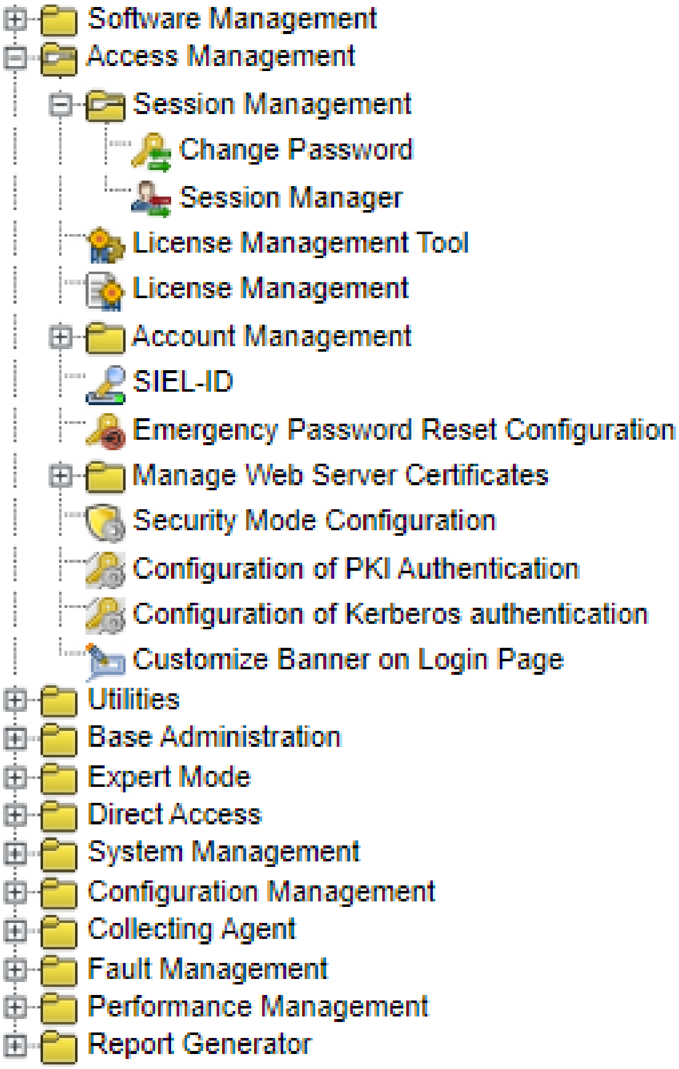
Configuration and activation of account rules

This configuration covers the general settings for all accounts.

- Enable duty hours
- Lock of account after certain period of inactivity
  - Password expiration. Password expiration is related only to new accounts.

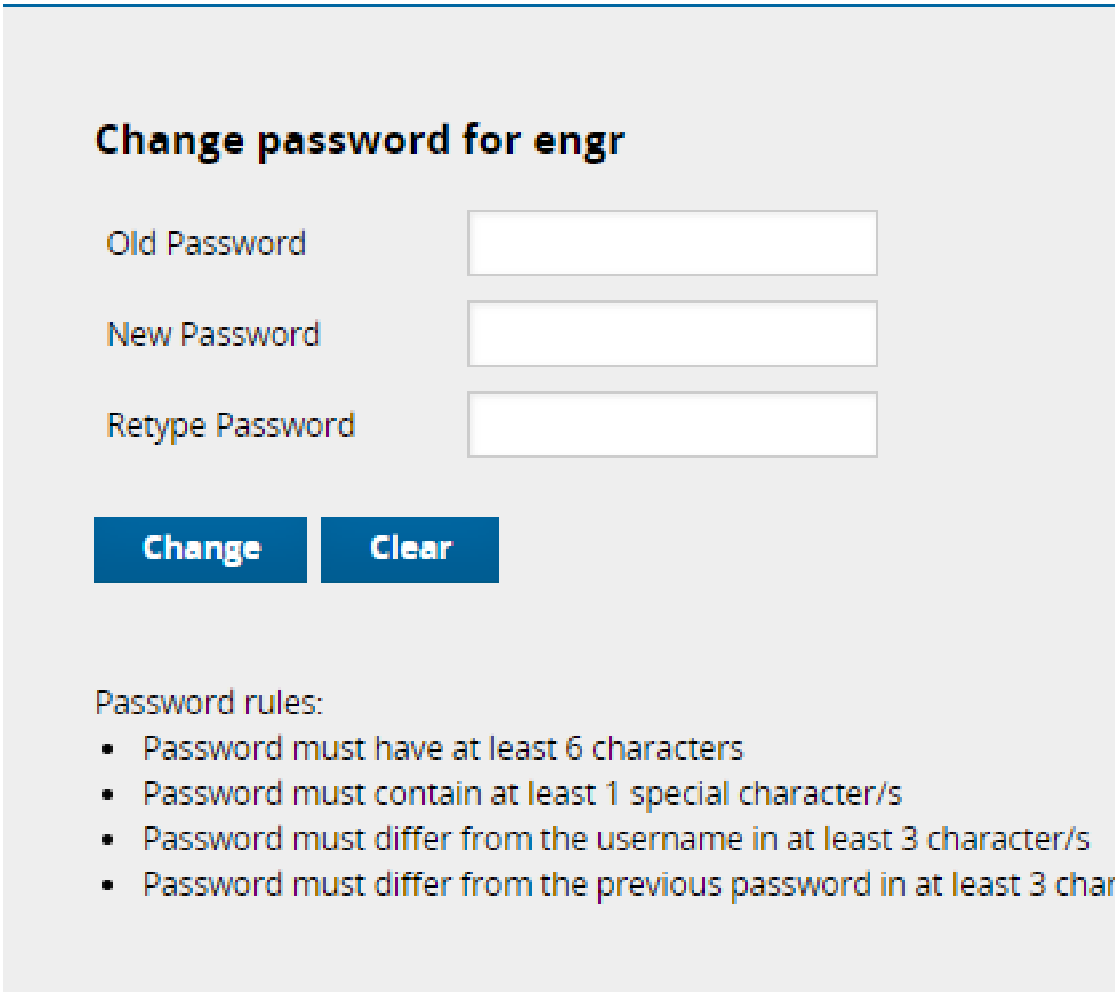
4.7.3 The user changes password himself

The interface for changing passwords is provided by the Session Management application of Access Management..



```
Software Management
Access Management
    Session Management
        Change Password
        Session Manager
    License Management Tool
    License Management
    Account Management
    SIEL-ID
    Emergency Password Reset Configuration
    Manage Web Server Certificates
    Security Mode Configuration
    Configuration of PKI Authentication
    Configuration of Kerberos authentication
    Customize Banner on Login Page
Utilities
Base Administration
Expert Mode
Direct Access
System Management
Configuration Management
Collecting Agent
Fault Management
Performance Management
Report Generator
```

Figure 56: Starting the Change Password Application in Session Management



Change password for engr

Password rules:

- Password must have at least 6 characters
- Password must contain at least 1 special character/s
- Password must differ from the username in at least 3 character/s
- Password must differ from the previous password in at least 3 char

Figure 57: The Change Password Application

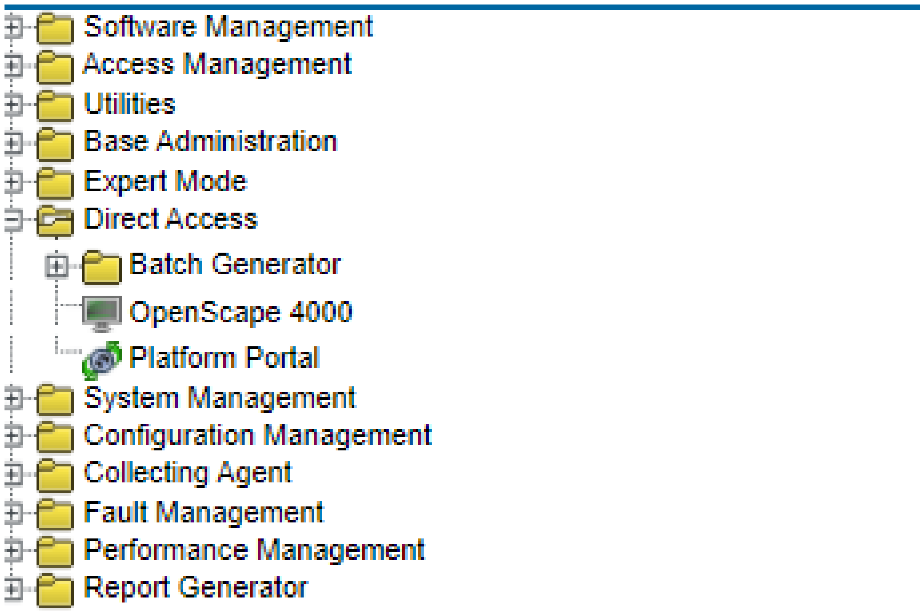
4.8 Connectivity test to OpenScape/HiPath 4000 switches

When all connections have been installed and the managed systems have been created in System Management, the physical connections to all systems should be tested.

4.8.1 Assistant and Single Sign On connectivity

To test the Assistant availability through Single Sign ON feature, perform the following steps:

1) Under Direct Access on the OpenScape 4000 Manager Launchpad, click OpenScape 4000.



- Software Management
- Access Management
- Utilities
- Base Administration
- Expert Mode
- Direct Access
  - Batch Generator
  - OpenScape 4000
  - Platform Portal
- System Management
- Configuration Management
- Collecting Agent
- Fault Management
- Performance Management
- Report Generator

Figure 58: Testing Access to an OpenScape 4000 Assistant

2) If applicable, select the system being tested from the list displayed in the Direct Access GUI (see Figure 86).

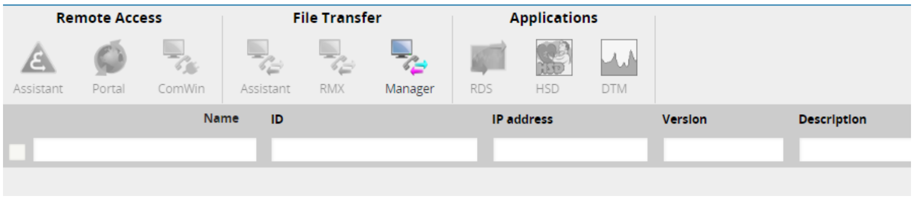


Figure 59: Direct Access GUI

3) Click the Assistant Icon in Remote Access box.

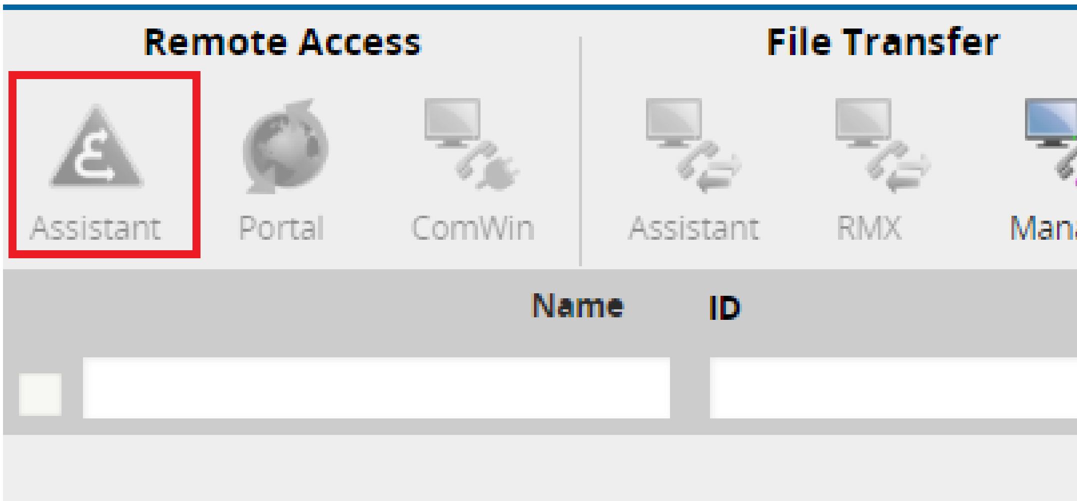


Figure 60: Direct Access: Assistant icon

4) If the OpenScape 4000 Assistant Launchpad of the selected OpenScape/ HiPath 4000 comes up (see Figure 88), the Assistant is up and Single Sign On feature works.

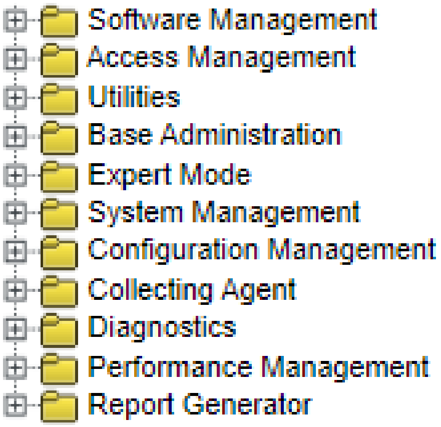


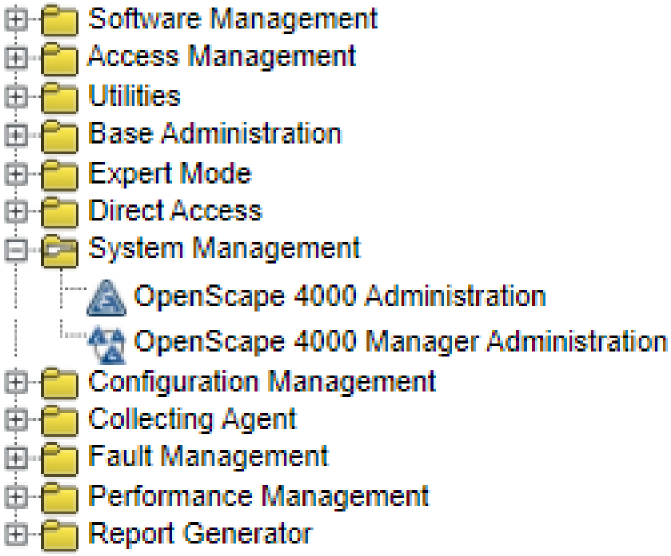
Figure 61: Launchpad of Selected OpenScape/HiPath 4000

5) Repeat this procedure for all OpenScape/HiPath 4000s managed by OpenScape 4000 Manager.

4.8.2 Testing AMO connectivity to OpenScape/HiPath 4000 switches

To test if AMO batchjobs can be executed on the connected OpenScape/HiPath 4000, perform the following steps:

1) Open System Management --> OpenScape 4000 Administration.



2) Click Search button to search for all the connected systems.
3) Switch the view to Object using the radio button at the screen top.
4) Now you can list through the configured systems using the arrows at the screen button.
5) The message box "Communication is OK" should be shown when AMO interface is accessible.
6) Each system's Communication Status field is Unknown and you can check the communication using the Check Status button.
7) Otherwise relevant eror message with a hint is shown:
8) The Communication Status "Communication Incomplete" is shown.

NOTICE: The field "Communication Status" is no more saved into the database and thus cleared by each system object redisplay.

4.9 OpenScape 4000 Manager and Assistant Usage Scenarios

This section is intended to provide clarification of functionality and interaction when AMOs and OpenScape 4000 Manager and/or OpenScape 4000 Assistant are used at the same time for switch configuration. Information is provided in the form of answers to frequently asked questions (FAQ).

Section 4.10.1, "Networks with OpenScape 4000 Manager" addresses networks involving AMOs, OpenScape 4000 Assistant and OpenScape 4000 Manager.

Section 4.10.2, "Networks without OpenScape 4000 Manager" addresses networks involving AMOs and OpenScape 4000 Assistant, but without OpenScape 4000 Manager.

4.9.1 Networks with OpenScape 4000 Manager

Basic Usage Rule: If a customer has a network with OpenScape 4000 Manager, then the Manager should be the only tool used to configure the switches. Using direct AMO commands may cause problems of database inconsistency within a network that includes both OpenScape 4000 Assistant **and** Manager.

4.9.1.1 What happens if I use AMO commands to change the switch configuration, bypassing the OpenScape 4000 Manager?

There is no mechanism to tell the Manager that the switch database was modified with the AMO command. In other words, as soon as the AMO command is executed, the Manager and the switch database are not synchronized with each other.

4.9.1.2 How can I determine whether the Manager database is synchronized with the switch?

There is no indication on the Manager that its database is synchronized. If someone executes an AMO command on a switch, the Manager will still say that its database is synchronized with the switch.

4.9.1.3 How can I synchronize the Manager and the switch database after executing an AMO command?

You can start a manual delta upload from the system (switch) screen (refer to Section 4.5.3.1, "Uploading an OpenScape/HiPath 4000"). If you don't do that, the nightly delta upload -- by default executed automatically every night at 10 p.m. -- will synchronize the databases (refer to Section 4.5.3.2, "Scheduling Periodic Uploads for OpenScape/HiPath 4000").

4.9.1.4 What happens if I use the Manager after executing an AMO command and before running a delta upload to synchronize the databases?

If you use the Manager to modify one of the objects affected by the AMO command you ran before, you may get incorrect error messages or get error messages when you shouldn't. This happens because the Manager validates any command you are attempting to execute. If the Manager database is not synchronized with the switch database, the validation process may not give reliable results.

Example:

If you delete a station with DEL-SBCSU, then immediately go to the Manager to create a station with the same number, the Manager will tell you that the station number is already in use (because the station still exists in the Manager database).

4.9.1.5 Is there any effect on the performance of the Manager when AMO commands are executed on the switch?

Yes, but the user may not notice it. The Manager uses AMO commands to change the switch configuration but, unlike the Assistant, it sends those AMO commands to the switch in the background. In other words, the Manager user is not blocked while the Manager is sending the AMO commands to the switch. It may take longer than usual for the switch to reply (because it is busy executing other AMO commands), but the Manager user can proceed with other tasks.

4.9.1.6 What if I use the Assistant to make configuration changes?

The Assistant also uses AMO commands to change the switch configuration. All the cases above apply: the Manager database will not be synchronized with the switch (Sections 4.10.1.1 through 4.10.1.4), and the Manager may experience performance degradation (Section 4.10.1.5).

4.9.1.7 I have to execute a large AMO batch file to update a customer configuration. This customer has a OpenScape Manager. How should I proceed?

Do not use the Manager while the AMO batch file is running. As soon as the AMO batch file finishes, run a delta upload from the Manager (for the affected switch[es] only, not for the entire network). If you also have to use the Assistant, wait until the Manager finishes the delta upload, then run an upload from the Assistant. (The Assistant upload may take some time to finish. It is recommended to wait for the nightly upload.)

4.9.1.8 If the Manager database is not synchronized with the switch and I try to use the Manager to change the switch configuration anyway, is there any chance I may corrupt the switch database (because the Manager may try to execute an invalid command)?

No. The switch always validates all configuration changes (from any source: AMO, Manager, Assistant) and rejects any invalid request. Even if the Manager allows you to execute a command that is not valid (because the Manager database does not have valid data to check the command; refer to Section 4.10.1.4), the switch catches it and returns an error message.

4.9.1.9 What happens to the Assistant database if someone makes a configuration change using the Manager?

The Assistant is notified that AMO commands were executed (the Manager sends AMO commands to the switches) and updates its database accordingly. For details on how this notification mechanism works, please refer to the chapter "Notification Mechanism and Usage Scenarios" in the OpenScape 4000 Service Manual.

4.9.1.10 Does the notification process affect the Manager performance?

Yes, but the Manager user may not notice it. The Manager generates AMO commands to change the switch configuration. The Assistant also uses AMO commands to synchronize its database. Since the switch can run only one AMO command at a time, if the Assistant is synchronizing its database, the AMO commands coming from the Manager will have to wait. However, the Manager user is not blocked while the Manager is sending AMO commands to the switch. It may take longer for the Manager to get a reply from the switch, but the user can proceed with other tasks. See also Section 4.10.1.5.

4.9.1.11 Is there any mechanism to synchronize the Manager database in case someone changes the switch database (since the Manager is not immediately informed)?

Yes. Every night (at 10 p.m., in the default configuration) the Manager synchronizes its database with the database of the switches connected to it. It uses a mechanism called "delta upload" that retrieves from the switch the database changes since the last upload was executed. On a quiet system (with no activity between 10 p.m. and the next morning), the Manager database should always be in sync with the switch database in the morning.

4.9.2 Networks without OpenScape 4000 Manager

Basic Usage Rule:

- If the customer does not have OpenScape 4000 Manager, use the Assistant to make configuration changes, not direct AMO commands.
- For answers to the following frequently asked questions (FAQ), and for details regarding the notification mechanism (how the Assistant database is synchronized with the switch database), please refer to the chapter "Notification Mechanism and Usage Scenarios" in the OpenScape 4000 Service Manual.
- What happens if I use AMO commands to change the switch configuration, bypassing the OpenScape 4000 Assistant?
- How long does it take to update the Assistant database when an AMO command is executed?
- What will the user see on the Assistant until the (Informix) database is updated?
- Does the Assistant notify the users after updating its database?
- Does the notification process affect the Assistant performance?
- Does the notification process slow down the execution of direct AMO commands?
- What happens if I execute a lot of AMO commands in a short period of time, e.g., run an AMO batch file?
- I have to execute a large AMO batch file to update a customer configuration. How should I proceed?
- Is there any automatic mechanism to synchronize the Assistant database when it goes out of sync?

5 Servicing and Maintaining the OpenScape 4000 Manager Server

This chapter provides instructions for servicing and maintaining the OpenScape 4000 Manager server.

5.1 Manager clock

The Manager clock is driven by the Platform Linux host. There is no option to configure an external NTP server or to configure the Manager as a clock source for another system in Webmin. The NTP server for Platform is configured the same way as for the Assistant during the system installation (i.e. firstinstall XML config file).

5.2 Restarting the Server

NOTICE: The procedure described in this section requires rsca or higher logon. Before proceeding with the steps below, broadcast a message to all logged on users, indicating that the server is about to be restarted.

To restart the server from the OpenScape 4000 Manager:

1) On the OpenScape 4000 Manager Launchpad, click **Direct Access**.
2) Click **Platform Portal**.

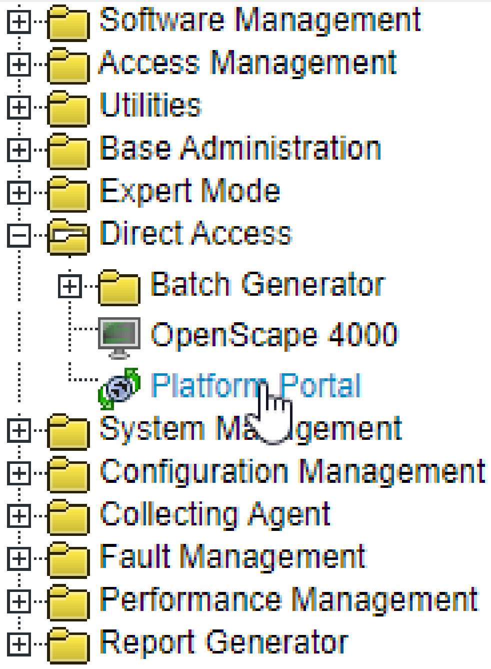
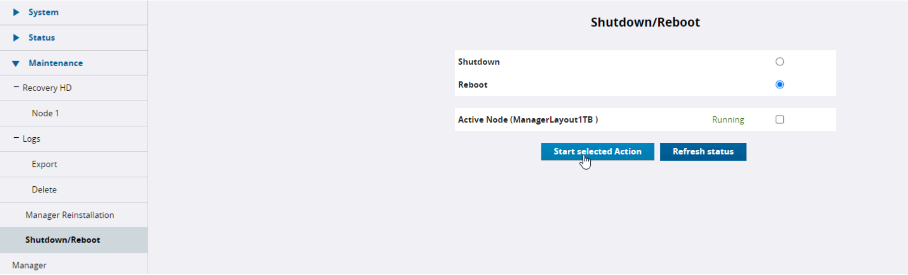


Figure 62: Accessing Webmin Base Administration

3) On the Platform Portal screen, click **Shutdown/Reboot** under Maintenance to display the Reboot and Shutdown screen.



Shutdown/Reboot

Shutdown ○
Reboot ●

Active Node (ManagerLayout1TB) Running □

Figure 63: Reboot and Shutdown Screen

4) Select the required option and click **Start Selected Action**.

Shutting Down the Operating System

The Manager Linux container can be shutdown/rebooted from **Webmin System Administration > Reboot/Shutdown**.

The Linux host can be rebooted/shutdown from **Platform Portal > Maintenance > Shutdown/Reboot**.

WARNING: Do not turn off or shut down the server while other users are logged in to OpenScape 4000 Manager and perform changes and system administration operations. This can corrupt the OpenScape 4000 Manager database. To see the list of the logged users, go to Session Manager in Session Manager section of the Launchpad tree.

5.3 Shutting Down the Operating System

To properly shut down the server, follow the procedures in this section.

NOTICE:

The procedures in this section are required when shutting down the server, and especially when hardware is to be added, removed or replaced in the server. Performing these procedures minimizes product failure.

Do not turn off the system without following these procedures. The file system can be damaged which requires reinstalling the operating system and applications.

Do not turn off or shut down the server while other users are logged on to OpenScape 4000 Manager (to see the list of the logged users, go to Session Manager in Session Manager section of Launchpad tree), performing moves and changes, or performing system administration. This can corrupt the OpenScape 4000 Manager database.

To shut down the operating system from the OpenScape 4000 Manager:

1) On the OpenScape 4000 Manager Launchpad, click **Direct Access**.
2) Click **Platform Portal**.

3) On the Platform Portal screen, click **Shutdown/Reboot** under Maintenance to display the Reboot and Shutdown screen.

4) Select the required option and click **Start Selected Action**.

5) In response to the displayed warning message, confirm the shutdown once more.

5.4 Software Updates using SWM/SWA

Software updates, in the form of Minor, Fix or HotFix Release for the OpenScape 4000 Manager can be handled using the Software Management applications Software Manager (SWM) and Software Activation (SWA).

Software Manager is used to transfer the software updates, and Software Activation is used to activate the transferred software. Both applications are accessible from the Launchpad.

If a HotFix causes problems, it can be deactivated by using the SWA Hotfix Deactivation feature.

NOTICE: For additional information and instructions on the use of SWM and SWA, please refer to the online Help of these applications.

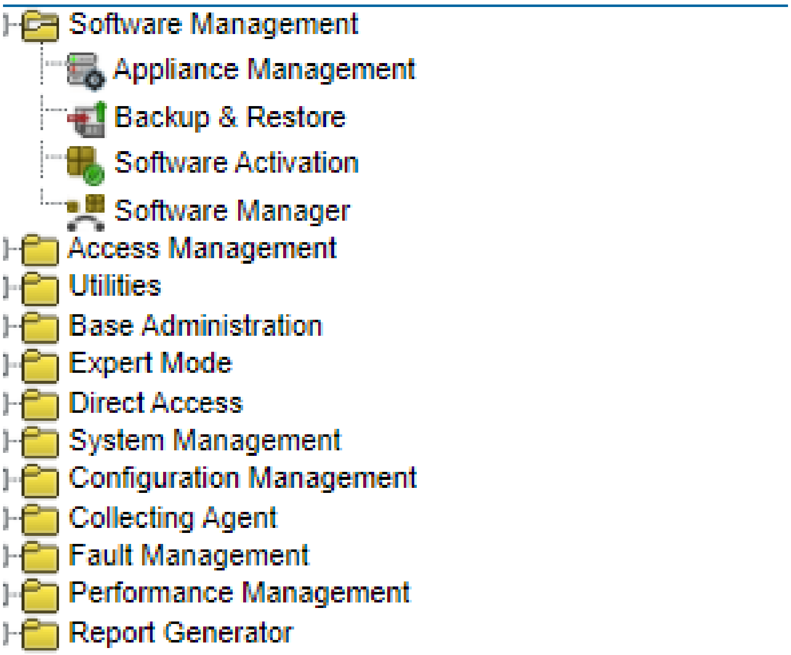


Figure 64: Accessing Software Manager / Software Activation in Software Management

5.5 Backing Up/Restoring Data with OpenScape 4000 Manager

This section briefly describes the Backup & Restore functionality in OpenScape 4000 Manager, including a fallback procedure to use if problems are encountered when upgrading to OpenScape 4000 Manager.

5.5.1 Performing a Database Backup

To back up the application database on the OpenScape 4000 Manager server:

1) On the OpenScape 4000 Manager Launchpad, click Software Management.

2) Click Backup & Restore to call up the Backup & Restore home page.

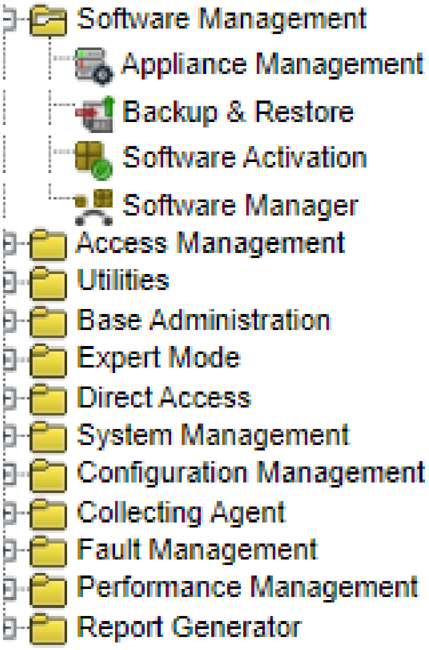
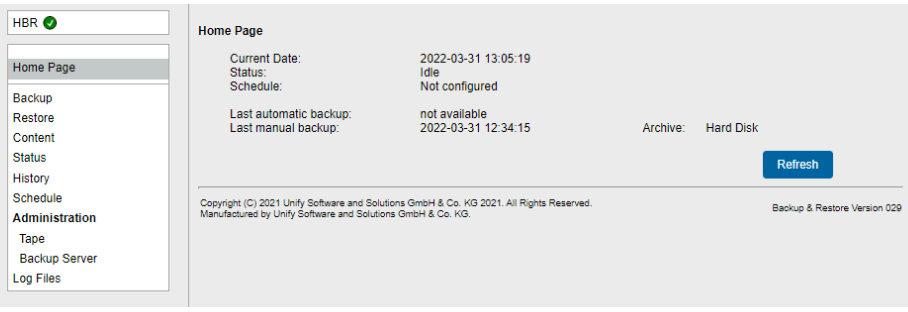


Figure 65: Accessing Backup & Restore in Software Management



Home Page

Current Date: 2022-03-31 13:05:19
Status: Idle
Schedule: Not configured

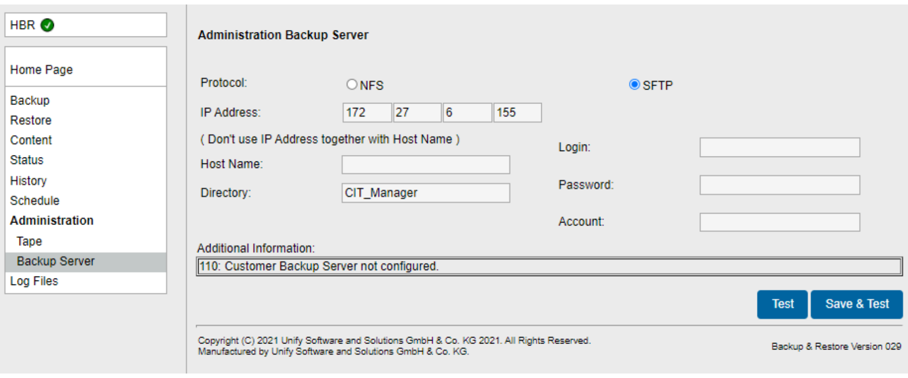
Last automatic backup: not available
Last manual backup: 2022-03-31 12:34:15   Archive: Hard Disk

Copyright (C) 2021 Unify Software and Solutions GmbH & Co. KG 2021. All Rights Reserved.
Manufactured by Unify Software and Solutions GmbH & Co. KG.

Backup & Restore Version 029

Figure 66: Backup & Restore Home Page

3) If you are archiving the data to a server elsewhere in the network, you must first define the destination server. Click Backup Server to display the Administration Backup Server screen. Refer to the online Help for instructions on configuring and testing the backup server.



Administration Backup Server

Protocol: ○ NFS ● SFTP

IP Address: 172 27 6 155

(Don't use IP Address together with Host Name)

Host Name:

Directory: CIT_Manager

Login:

Password:

Account:

Additional Information:

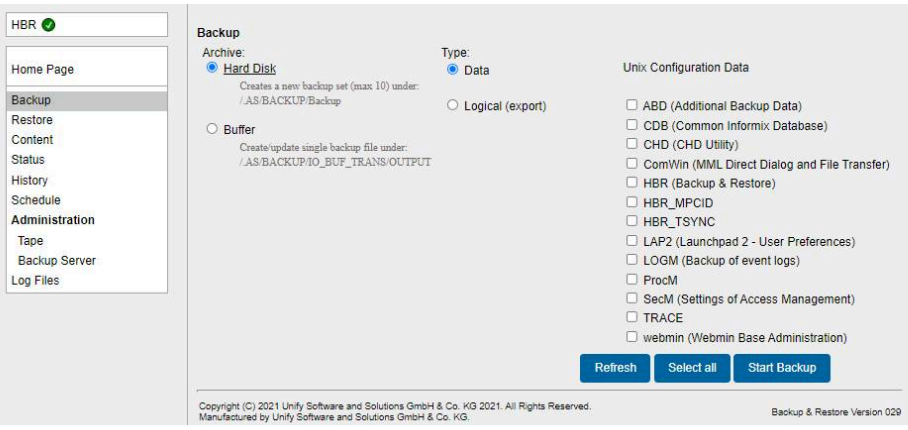
110: Customer Backup Server not configured.

Copyright (C) 2021 Unify Software and Solutions GmbH & Co. KG 2021. All Rights Reserved.
Manufactured by Unify Software and Solutions GmbH & Co. KG.

Backup & Restore Version 029

Figure 67: Specifying a Backup Server

4) Click Backup to select the parameters to be used for this backup procedure. Refer to the online Help for additional information and instructions.



Backup

Archive:

● Hard Disk
Creates a new backup set (max 10) under: /.AS/BACKUP/Backup

○ Buffer
Create/update single backup file under: /.AS/BACKUP/IO_BUF_TRANS/OUTPUT

Type:

● Data

○ Logical (export)

Unix Configuration Data

□ ABD (Additional Backup Data)
□ CDB (Common Informix Database)
□ CHD (CHD Utility)
□ ComWin (MML Direct Dialog and File Transfer)
□ HBR (Backup & Restore)
□ HBR_MPCID
□ HBR_TSYNC
□ LAP2 (Launchpad 2 - User Preferences)
□ LOGM (Backup of event logs)
□ ProcM
□ SecM (Settings of Access Management)
□ TRACE
□ webmin (Webmin Base Administration)

Copyright (C) 2021 Unify Software and Solutions GmbH & Co. KG 2021. All Rights Reserved.
Manufactured by Unify Software and Solutions GmbH & Co. KG.

Backup & Restore Version 029

Figure 68: Selecting the Backup Parameters

5) Click Start Backup to initiate the backup.

> **NOTICE:** To check the status of this procedure, click Status in the Backup & Restore menu.

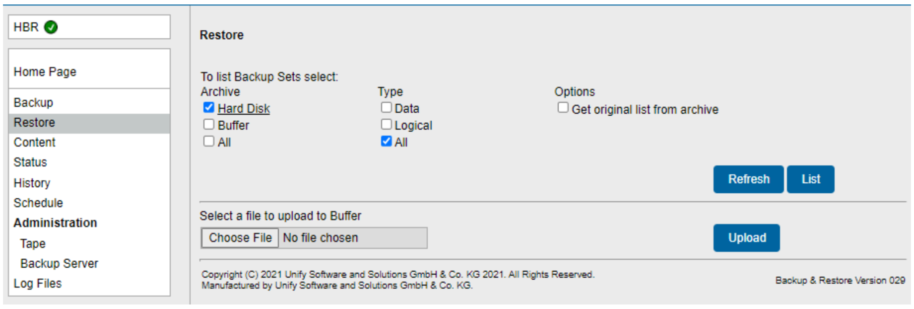
5.5.2 Restoring Archived Data

To restore data from a backup archive:

1) On the OpenScape 4000 Manager Launchpad, click Software Management.

2) Click Backup & Restore to call up the Backup & Restore home page.

3) Click Restore in the Backup & Restore menu on the left.



Restore

To list Backup Sets select:

Archive	Type	Options
☑ Hard Disk	□ Data	□ Get original list from archive
□ Buffer	□ Logical	
□ All	☑ All	

Select a file to upload to Buffer

No file chosen

Backup & Restore Version 029

Figure 69: Listing the Backup Sets for Restore

4) In the Restore screen, select the parameters to be used for this restore procedure. Refer to the online Help for additional information and instructions.

5) Click List to display the backup sets from which to select.

6) Select the relevant backup sets.

7) Confirm your selection to start the Restore.

NOTICE: To check the status of this procedure, click Status in the Backup & Restore menu.

CAUTION: Data Restore was certified as a recovery tool for OpenScape 4000 Manager/Assistant and works only on identical hardware with the same software version. If used any other way, the restore operation might be terminated with an error. In other cases, use the Logical Backup/Restore certified to be used for recovering data between different hardware and versions.

5.6 OpenScape 4000 Manager Server Licensing

5.6.1 License Management at the OpenScape 4000 Manager

The License Management application enables you to display information related to the installed licenses and to the Customer License Agent (CLA). Via this application you are also able to configure the location of the Customer License Agent (IP-Address or DNS Name).

To invoke the License Management application perform the following steps:

1) On your OpenScape 4000 Manager, log on as rsca or higher (for information on security levels in Access Management, refer to Table 4 on page 148).

2) On the Launchpad, click Access Management, then click **License Management**. As a result, the License Management Homepage opens .

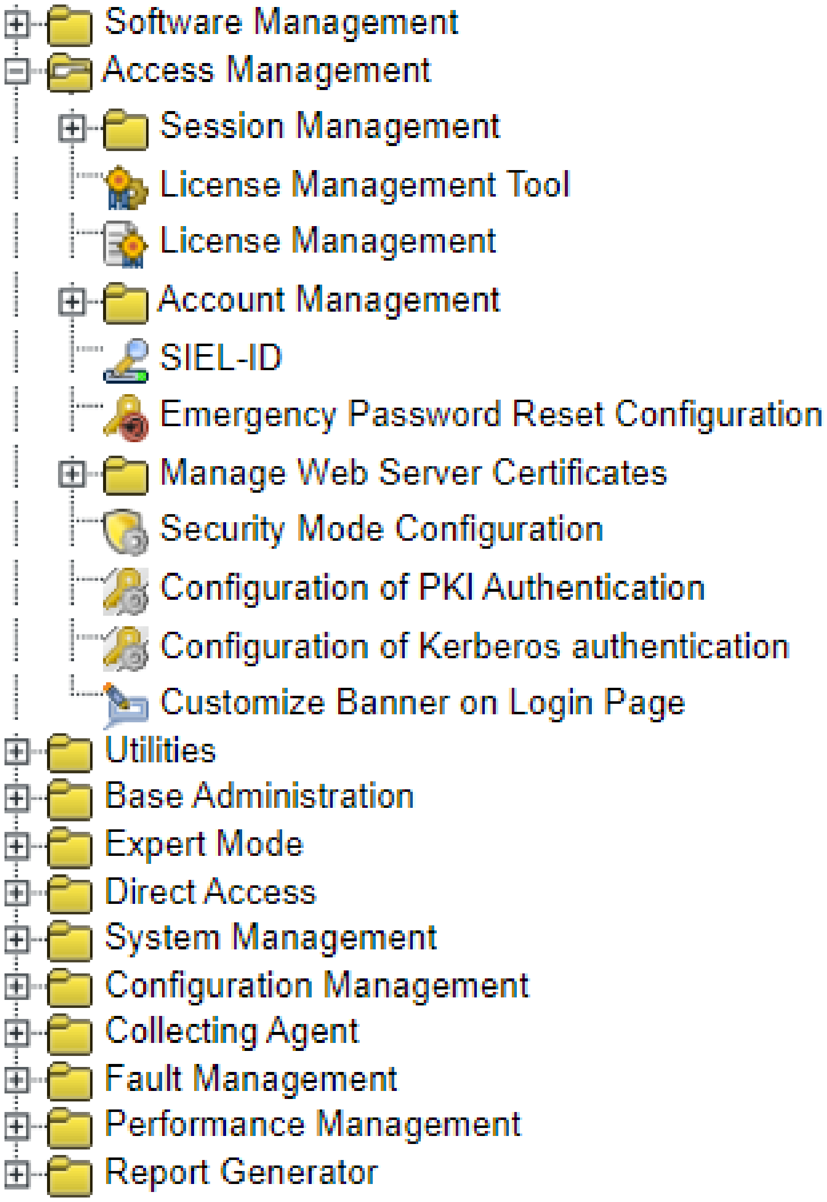


Figure 70: Initiating License Management

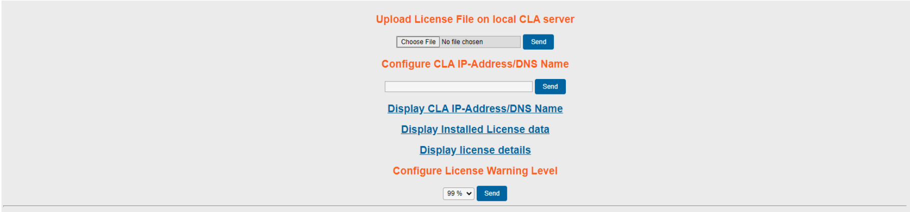

Upload License File on local CLA server
Choose File
No file chosen
Send
Configure CLA IP-Address/DNS Name
Send
Display CLA IP-Address/DNS Name
Display Installed License data
Display license details
Configure License Warning Level
99 %
Send

Figure 71: License Management Home Page

5.6.2 Obtaining the License Key for the OpenScape 4000 Manager Server

A license key is required in order to place the OpenScape 4000 Manager into service. The license key contains encrypted information relating to the port configuration and other data which is necessary to enable the purchased applications. The license key is obtained using a Web-based interface, by setting up an Internet connection to the license server.

NOTICE: It is possible that the procedure described here will undergo changes resulting from adaptation to SAP (Service Agreement Policy) requirements, or from harmonization with licensing procedures used for other products. In such cases, the relevant instructions will be made available in the form of online help on the license server. Refer also to the CLS (Central Licence Server) online help for details of the license generation procedure.

NOTICE: Since OpenScape 4000 Manager V10, the licenses are locked to Advanced Locking ID (ALI) instead of MAC address of the Manager server. The ALI is a key required for purchasing license. The ALI key is displayed on Manager dashboard.

5.7 Installing the Expert Access Client

The Expert Access Client can be downloaded and installed from the OpenScape 4000 Manager server itself.

Downloading the Expert Access Client from the OpenScape 4000 Manager Server

To download and install the Expert Access Client from the OpenScape 4000 Manager server:

1) On the OpenScape 4000 Manager Launchpad, click Direct Access, then click OpenScape 4000.

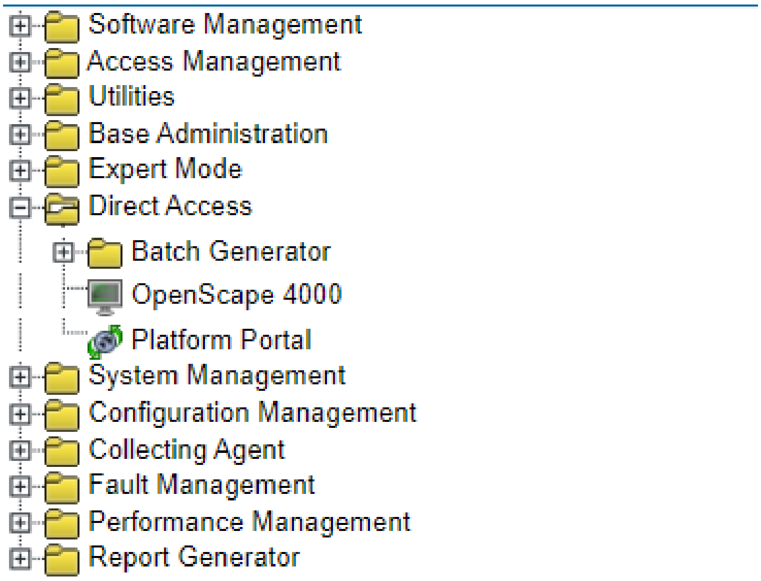
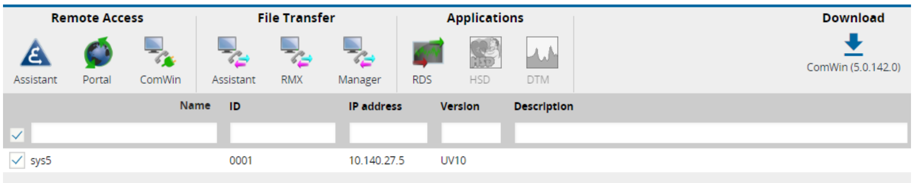


Figure 72: Installing the Expert Access Client from OpenScape 4000 Manager Server (Direct Access)

2) In the menu on the right side of the Expert Access page, you can download installation file from ComWin Expert Access.



Name	ID	IP address	Version	Description
☑				
☑ sys5	0001	10.140.27.5	UV10	

Figure 73: Starting Expert Access Client Installation

3) Download the installation file and follow the on-screen instructions to complete the installation of the Expert Access Client.

5.8 Using VNR (Virtual Numbering Plan)

With the VNR feature it is possible to define the same and similar numbers in one physical node.

5.8.1 General Concept

In this section, some general concepts of Configuration Management are presented to make clear why and how things have been changed in order to match the requirements of a Virtual Numbering Plan.

Domain, Switch and Routing Concept Used up so far

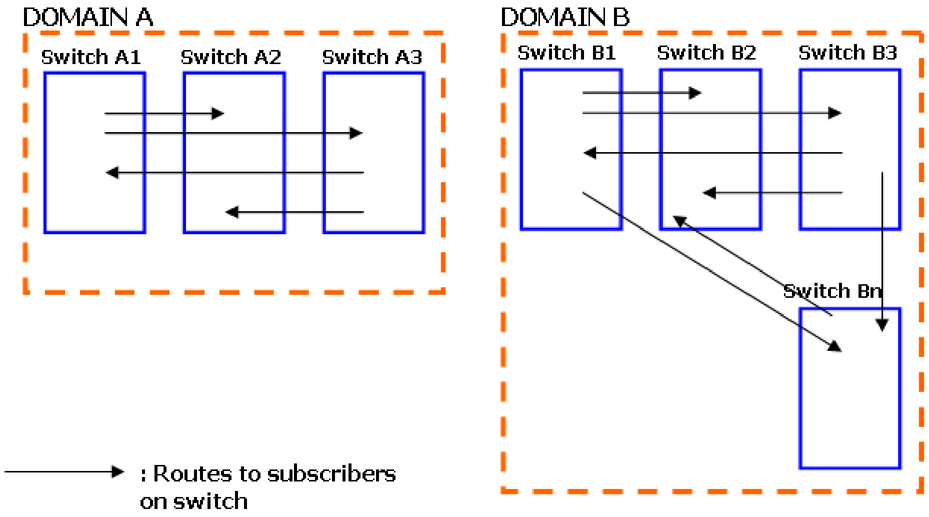


Figure 74: Domain, Switch and Routing Concept

With the current domain concept, one switch can exist only in one domain and domains consist of Physical Nodes (switches). Routing operations are only handled within one domain. For example if a station is deleted from (or added to) Switch A1 in Figure 2, only the switches in the Domain A (A2, A3) are affected by this operation and their routes are updated. The route handling in Domain B is not affected.

The VNR Concept

Using the VNR feature it is possible to define the same and similar numbers in one physical node in different Virtual Nodes. With this feature, extensions are used in the long representation which can be up to 12 digits maximum (6 Digit Virtual Node Access Code + 6 digit short extension).

For this purpose it is not enough to define the routing to a particular station only by means of the Route Index (ZLNR) and of the extension number.

As shown in the figure below, if a station from PN A3 VN2 wants to call a station on PN A1, three different parameters are required.

(Note: Physical Node = Physical Switch)

1) Route Index (ZLNR) to find the correct Physical Node (**PN**) in the domain

2) • Virtual Node Access Code (VNAC) to find the correct Virtual Node (**VN**) on the Physical Node.

- Station Number

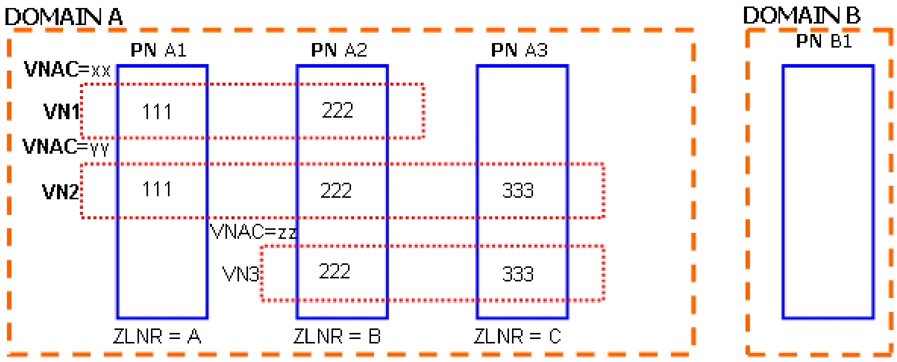


Figure 75: VNR Network

Routing Problems in Mixed Networks (with VNR and non-VNR)

While VNR switches hold the routing information with all three parameters (PN = (DestNo), VNAC and station number (= long extension)), the same is not valid for non-VNR switches.

In non-VNR switches the Virtual Node information is not available for routing since they use short extensions. This results in the problem described below where three different stations with number 222 exist on the VNR-switch PN A2. If a user from the non-VNR switch **PN A3** calls 222 it is not clear which 222 on the **PN A2** is addressed, since the Virtual Node information is missing. Therefore it is not possible to obtain proper routing in this scenario, since Station Number (short) and Route Index are not enough. This is the reason why Mixed Networks need a special routing configuration.

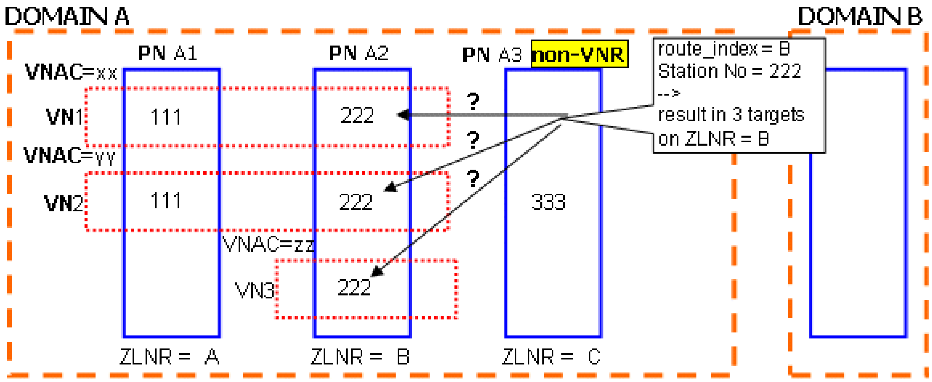


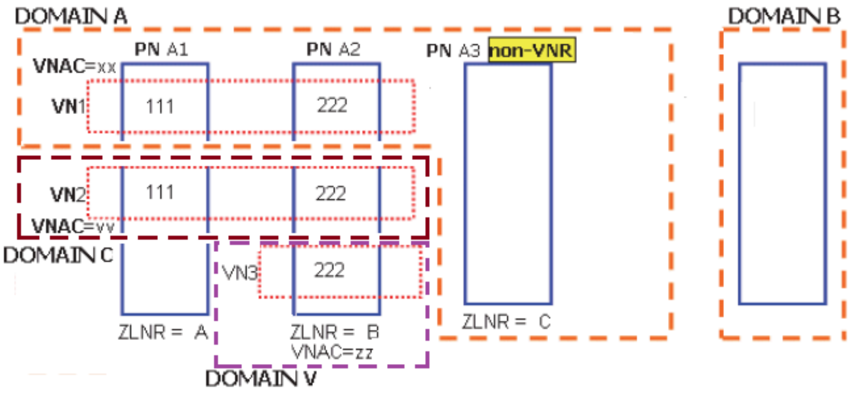
Figure 76: Routing Problem With Mixed Networks

Operating one VNR Switch in Several Domains

The restrictions with mixed VNR and non-VNR switches mentioned above resulted with the design shown in the next figure. In this figure it can be observed that several non-VNR switches and **one single VNR-switch** are used in the same domain. The small boxes with ZLNRs represent the non-VNR switches. According to this scenario, one switch can have different Virtual Nodes in different domains. Within one domain, one virtual node (sub-switch) is defined. Sub-switches of different VNR Physical Nodes can exist in the same domain; however, they must have the same Virtual Node ID and Virtual Node Access Code. This requirement (having same Virtual Node ID and Virtual node

Access Node) is not needed for non-VNR systems. Another requirement is that every virtual node on a physical switch should have different ZLNR/DestNo's.

This configuration can be realized now (starting with V4) with the new possibility to divide one Physical Node into different **Subswitches** using the Virtual Node and configuring these sub-switches in different domains.



Up to Release V4, a switch could not exist in more than one domain and it was also not possible to define virtual nodes as members of a domain (only switches, i.e. Physical Nodes could be defined in a domain).

5.8.2 Introduction of the Sub-switch Concept

Before of the realization of the VNR-feature, the switch and domain concepts in CM allowed to define a switch (as one physical node) in one domain only. It was not possible to define a switch in more than one domain. Previously, it was also not possible to define a node other than a physical switch within a domain.

In order to be able to define a switch that can exist in more than one domain at the same time, the new "**Sub-switch**" concept for VNR switches has been introduced.

Sub-switches are actually virtual switches created within one VNR switch and separated from each other with virtual nodes. Since for the CM logic they are not different from physical switches, they are treated by CM as usual. However, only CM handles sub-switches as a switch and from the outer world the VNR switch will be treated as an ordinary switch with virtual nodes as before and sub-switches will be masked.

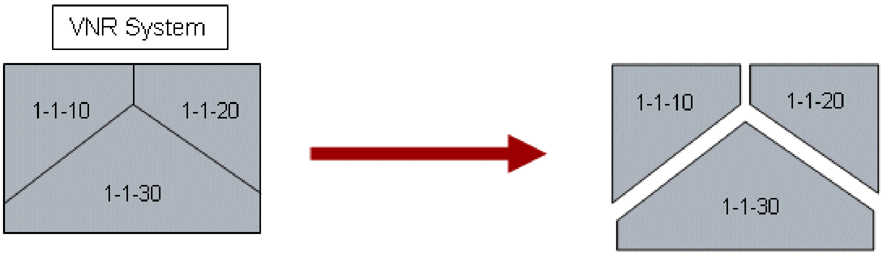


Figure 77: Defining one VNR Switch as several sub-switches

Enabling the "VNR Physical Switch" attribute

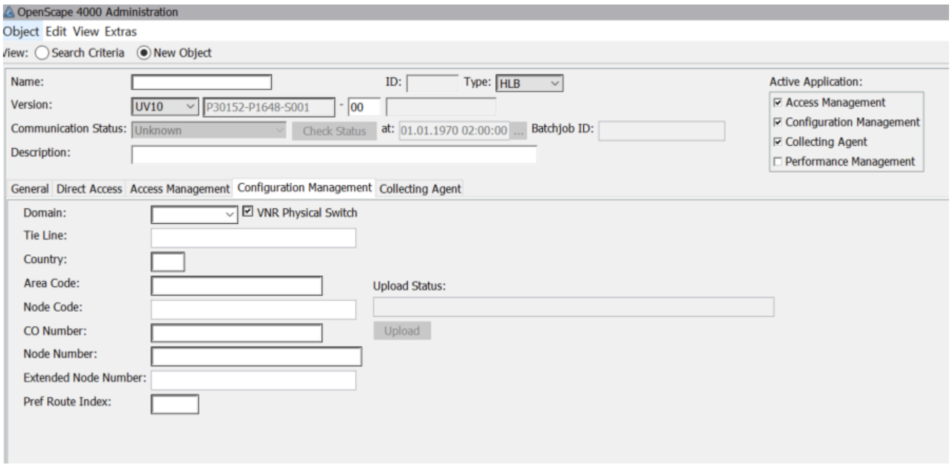
There is a new checkbox in Configuration Management hooking into the System Management Dialog called "VNR Physical Switch" to distinguish if a VNR will or will not be used on this physical switch. This checkbox should only be checked if the switch to be added is a VNR switch.

If the VNR Physical Switch checkbox is checked on the Configuration Management tab of the System Management dialog of the OpenScape 4000 Administration, it is possible to define multiple domains on this switch from the Sub-Switch Data tab of the System window in Configuration Management; this tab is used to define the sub-switch – Domain-Virtual Node relationship to the system.

You can enable the "VNR Physical Switch" attribute in the System Management screen only during the introduction of new switch. This flag cannot be updated for an already existing switch. After the switch was added, this flag can only be changed if no sub-switch has been added. But as soon as at least one sub-switch was added, it is no longer possible to modify it.

Sub-switches can be created only on **VNR switches**, and there can be only one sub-switch on one Virtual Node of a VNR Switch. And on one sub-switch there will be only one Virtual Node.

With the introduction of sub-switches it is still possible to continue with the current domain and switch implementation.



View: ○ Search Criteria ● New Object

Name:
ID:
Type: HLB
Version: UV10 P30152-P1648-S001 - 00
Communication Status: Unknown
at: 01.01.1970 02:00:00
Batchjob ID:
Description:

Active Application:
☑ Access Management
☑ Configuration Management
☑ Collecting Agent
☐ Performance Management

Domain:
☑ VNR Physical Switch
Tie Line:
Country:
Area Code:
Node Code:
CO Number:
Node Number:
Extended Node Number:
Pref Route Index:
Upload Status:

Figure 78: VNR Physical Switch checkbox in SysM / OpenScape 4000 Administration Dialog

Once the sub-switches are created, they are treated as physical switches. All the necessary conversions are done by the components that communicate with the switch and the CDB database. Inside CM there are *n* sub-switches, and outside CM there is one physical switch; all necessary conversions are made automatically when the data is received or sent.

Starting an upload just after adding this switch will fail until the correct sub-switch information is entered into the **Configuration Management -> System Dialog -> Sub-Switch Data** tab.

If the **VNR Physical Switch** checkbox is not checked, this VNR switch will not appear on the **Sub-Switch Data** tab of the **System** window in **Configuration Management**, and the user will not be able to define different nodes on this switch.

The **VNR Physical Switch** checkbox is also visible (read-only) on the **System** window in **Configuration Management**.

5.8.3 CM System Window - Administration of Switches

Some data are relevant for the sub-switch only, and some are relevant for the physical switch itself. If some attribute is required to be same within the entire physical node, this attribute is "switch-wide" and can only be updated for the physical node from the System dialog (e.g. DTB Server Access Code). Therefore, from the System dialog some data can only be updated for the physical node, while others can be updated for the sub-switch. If data is updated for the physical node, every sub-switch is also updated with the new value automatically. However, if sub-switch-related data is updated (from the Object View for the sub-switch in the System dialog), this change will only affect the related sub-switch; other sub-switches will not be updated (e.g. Preferred Route Index, Country, Area Code, CO Number etc.)

Adding new sub-switches can be done from the new Sub-Switch Data tab in the System dialog. It is possible to add a sub-switch only to those switches where the VNR Physical Switch flag has already been set.

It is possible to add/delete sub-switches even for the uploaded switches after Virtual Nodes have been added/deleted to/from the switch.

However, after any sub-switch Add/delete operation an Upload All for the physical node has to be started. Before starting the Upload All, the sub-switch data for that physical node have to be updated depending on the virtual node information in the switch (the sub-switch number should be the same as the number of virtual nodes on the switch, and the Virtual Node Access Code and Virtual Node ID should match accordingly.)

If you want to delete a sub-switch, this can be done from the Sub-Switch Data tab in the System dialog (choose entry, click on the cross at the right and click on Save). However, directly after adding or removing a sub-switch an Upload All should be started, and the user should verify that the sub-switch data match the virtual node configuration of the switch.

The deletion of uploaded sub-switches actually means removing the corresponding virtual node from the physical node; therefore, this administration job can also be done from the Virtual Nodes (KNDEF) dialog. If the verify check done prior to the removal of a switch is passed in this screen, the user can delete that virtual node. A Del-KNDEF AMO is produced to delete the virtual node on the physical node, and the virtual node is deleted from the numbering plan; after this step, the sub-switch and all of its data at the CDB are automatically removed as well.

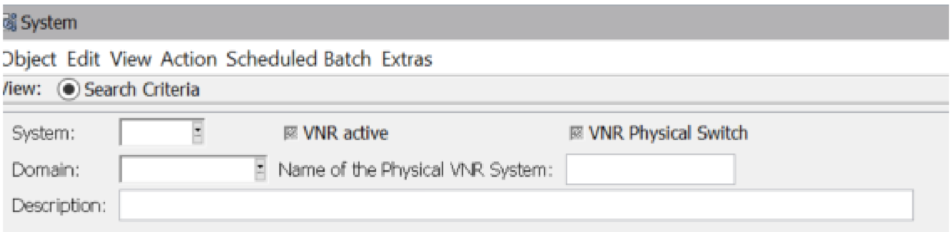
An Upload (PBX, LCR , All or Delta) can only be initiated from the object that represents the VNR Physical Switch, not from the objects that represent sub-switches. Thus, it is not possible to start an upload for a specific sub-switch. The entire VNR switch is uploaded at the same time.

VNR Active, VNR Physical Switch and Name of the Physical System are read-only fields.

The VNR Active field is updated according to the uploaded data from the switch and defines whether the switch is VNR or non-VNR.

The VNR Physical Switch Field indicates whether the system is a physical VNR System. If this is checked, this indicates that the system is VNR and a physical node (not a sub-switch).

The Name of the Physical System field displays the physical system name. For physical systems (VNR or non-VNR), this field displays the name of the system itself. These two fields are different for sub-switches only, and it indicates the physical switch of that sub-switch.



View: ● Search Criteria

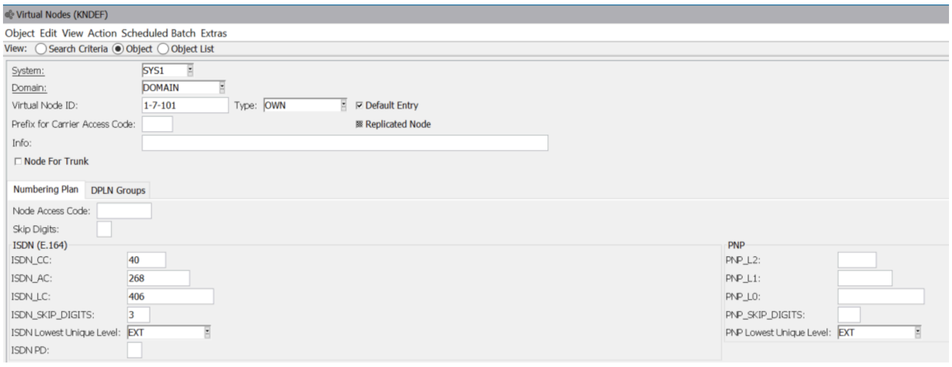
System:
☒ VNR active
☒ VNR Physical Switch
Domain:
Name of the Physical VNR System:
Description:

Figure 79: Generic Data and Sub-Switch tab for a New System in Configuration Management

5.8.4 Special handling of Virtual Nodes (KNDEF)

Since a sub-switch can contain one virtual node only (1-to-1 mapping), there must be a special handling for Virtual Nodes (KNDEF) in case that "VNR Physical Switch" is active on the physical node:

Virtual Nodes will be handled in the sub-switch level. Every sub-switch (since actually itself is a Virtual Node) will contain only one Virtual Node. In order to add a new Virtual Node to a Physical System, user can add the Virtual Node to any Subswitch on the Physical Node. This is only needed for creation of the Virtual Node on the Switch. After the Virtual Node is created, the matching sub-switch should be added to the Physical System and Upload All should be started on the Physical Switch. As the Upload finishes there will be again one Virtual node on each sub-switch of the system.



View: ○ Search Criteria ● Object ○ Object List

System: SYS1
Domain: DOMAIN
Virtual Node ID: 1-7-101 Type: OWN ☑ Default Entry
Prefix for Carrier Access Code: ☒ Replicated Node
Info:
☐ Node For Trunk

Node Access Code:
Skip Digits:

ISDN (E.164)
ISDN_CC: 40
ISDN_AC: 268
ISDN_LC: 406
ISDN_SKIP_DIGITS: 3
ISDN Lowest Unique Level: EXT
ISDN PD:

PNP
PNP_L2:
PNP_L1:
PNP_L0:
PNP_SKIP_DIGITS:
PNP Lowest Unique Level: EXT

Figure 80: Virtual Nodes (KNDEF) Dialog in Configuration Management

The data for the virtual nodes are entered by the upload of the CM. They can be displayed, modified and deleted.

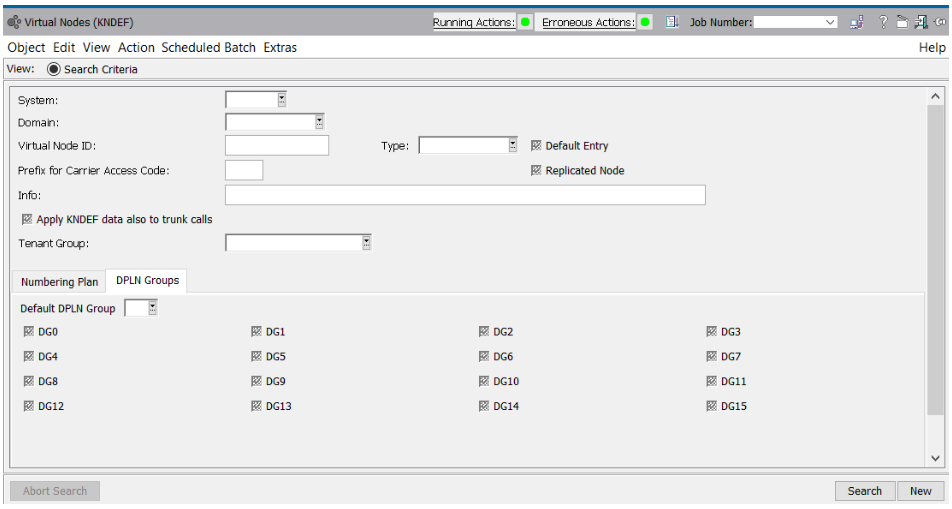


Figure 81: Virtual Nodes (KNDEF) Dialog - DPLN Groups tab in Configuration Management

5.8.4.1 Adding a Virtual Node

When a new virtual node is to be added to such VNR Physical Switch, additional action is required in order to create the mapping to the corresponding sub-switch which will represent newly created virtual node:

- Add a new virtual node in CM dialog Virtual Nodes (KNDEF) where the System Name is any of the subswitches of that Physical Node.
- Open the **Sub-Switch Data** tab in the CM dialog **System** and create a new sub-switch that will represent the new virtual node. Put this new sub-switch into one of the existing domains or a new domain (but one different from the sub-switches of the same Physical Node).
- Open the CM dialog **System** and initiate an Upload All for the affected Physical Switch.

5.8.4.2 Modifying an existing Virtual Node

As modification operations for existing virtual nodes are very limited, (on AMO level) existing behavior will remain.

5.8.4.3 Deleting an existing Virtual Node

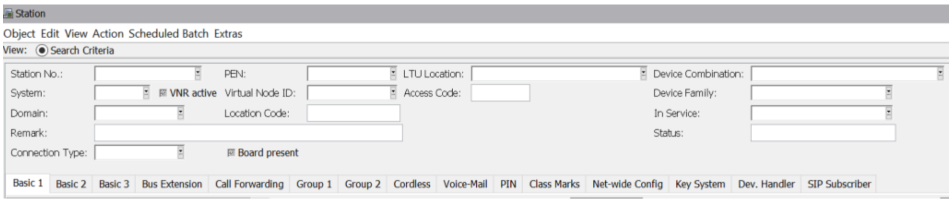
In the new version the deletion of a certain virtual node automatically triggers the deletion of corresponding sub-switch as well.

Since the deletion of any Virtual Node is very restrictive (all subscribers on this virtual node must be deleted before the node can be deleted), CM follows these restrictions. Only if all prerequisites for such a deletion are met, CM will delete the corresponding sub-switch as well.

5.8.5 Station Dialog in Configuration Management

The view of the data in the station dialog is still the same for non-VNR systems. No value is displayed in the Access Code field, even if the code for the OWNNODE was assigned. This one is not part of the station number.

For VNR-systems, the code for the OWNNODE is displayed in the Access Code field, as this is also part of the station number assigned in the AMO SBCSU. This is shown also in the field Station No.:



View: ● Search Criteria

☒ VNR active

☒ Board present

Figure 82: Station Dialog in Configuration Management

5.8.6 Restrictions

There are some restrictions for sub-switches.

1) UPLOAD: Upload of sub-switches cannot be initiated from sub-switches; physical switches are used instead. (Scheduled Uploads will not be available for the sub-switches either.) If the user wants to start an upload, it can be started for the physical switch; during the upload all sub-switches on that physical node are updated at the same time. Therefore, it is not possible to execute an upload for only one sub-switch.
2) Administration of Physical Nodes:
   a) In case of a search operation from the System dialog, both physical switches and sub-switches will be listed. However, it will not be possible to modify the data of sub-switches from this dialog except for some fields: VMS System, VM Server, Preferred Route Index, Country. Area Code, CO Number, Node Code can be set for sub-switches. For other fields, the user can only make changes on the Physical Switch. In order to modify a sub-switch from the System dialog, you can make changes on the Physical Switch where the sub-switches are defined. If a change is made on a physical switch, all the sub-switches defined on this switch will be updated with the relevant data.
   b) The administration on the other dialogs is only possible for sub-switches and not for the VNR Physical Switches. If the user wants to create or move a station, etc., the VNR Physical Switch will not be listed as a potential destination system.

5.9 PIN Distribution Program

This section describes the function and operation of the PIN distribution program installed on the OpenScape 4000 Manager server.

5.9.1 Introduction

The PIN distribution program facilitates automatic distribution of PINs by way of the OpenScape 4000 Manager. Distribution of PINs to other switches in the network can be scheduled accordingly, e.g., at night.

The PIN distribution program is a component of the XIE/API package ASxie and is installed in the directory /opt/xie/dmsie/pindist.

5.9.2 Administration

In order for the PIN distribution program to function properly, the logging of deleted records from the upd_pin table in the OpenScape 4000 Common Database (CDB) must be active. This logging can be enabled on the OpenScape 4000 Manager Server as follows:

1) Execute the script /opt/xie/dmsie/bin/ujgedelupd.sh -y. This sets the pin_upd flag in the admin table of the CDB to 001, thereby enabling the logging of deleted records via CM.

2) Stop the Cserver and then restart it (execute /opt/cm/bin/cs_control restart).

Script "pindist.sh"

During the installation of ASxie, the start script pindist.sh is installed in the directory /opt/xie/dmsie/pindist. This script is used to perform the following actions:

Start Script Menu:

```
AUTOMATIC PIN DISTRIBUTION

1 - Activate
2 - Deactivate
3 - State
4 - List of protocol file
5 - End

Select: _
```

Activate

Automatic distribution of PINs is activated. The start time (hour and minutes) for automatic PIN distribution must be specified in this dialog.

```
Time for automatic PIN distribution:

-----------------------------------

Start time for daily PIN distribution (hh:mm): 23:45
```

Deactivate

Automatic distribution of PINs is deactivated (entry removed from the UNIX cron table).

State

If PIN distribution has been activated, the start time is displayed:

```
State of automatic PIN distribution:

----------------------------

Hour : 23
Minute : 45

Continue with RETURN key
```

List protocol file

The log file ("protocol file") from the last PIN distribution is displayed on the screen. The log contains execution-related messages and, if applicable, error messages in plain text.

Example of Log File:

```
20.09.03 04:00: BEGIN PIN DISTRIBUTION ...
Number of switches: 4
Select all PIN modifications since 2003-01-09 04:00:36
Number of Inserts: 1
Number of updates: 0
Number of Deletes: 1
Extension: 45678   Switch: GUD1 new PIN created
Extension: 45678   Switch: ERD1 new PIN created
Extension: 45678   Switch: SIE1 new PIN created
Extension: 45670   3 records deleted
Send AMO's to PABX network
Update file InsertedPins.dat
20.09.03 04:02: END      PIN DISTRIBUTION
```

End

End of processing; return to main menu.

5.9.3 Notes Regarding Use

When PINs are modified, the changes are not automatically distributed to all switches! If an existing PIN is to be changed, either OpenScape Configuration Management must be used to make the change on all switches, or the PIN on a given switch must be deleted and a new PIN created.

PINs with pin type "G04" (pkz_pin) or "G05" (wkz_pin) or "C66" (Cordless E PIN) are not distributed to all switches. If flag PKZ_PIN=YES is set in the file /var/xie/pindist/Extensions.dat, PINs of type "G04" (pkz_pin) are also distributed.

The same extensions must exist on all switches. If this is not the case, in each switch a specific extension can be defined in the file /var/xie/pindist/Extensions.dat. (For each switch, the file contains a line showing the switch name and extension, separated by a blank space). For these switches, newly added PINs are then generally stored under the extension specified in the file "Extensions.dat" . If the word "IGNORE" appears instead of an extension, no PINs are distributed to this switch. If there are no entries specified in the file (default), it is assumed that all the switches in the PABX network comprise the same extensions.

File "Extensions.dat" in Directory "/var/xie/pindist": Example 1

```
# Allocation Table SWITCH -> DIRECTORY NUMBER
# --------------------------------------------
#
# Syntax: <Switch><spaces><extension>
#
#         <Switch>     ... Switch name (max. 4 characters)
#         <spaces>     ... One or more blank spaces
#         <Extension>  ... Extension (max. 6 characters) or
#IGNORE if no PINs are to be distributed to this switch
#
#(Comment lines begin with the character '#')
#
SIE1 4711
SIE2 4711
SIE3 4711
SIE4 IGNORE
# If, "Master Switch" is specified, only new PINs will be
 distributed for this switch
MASTER_SWITCH=SIE1
# PKZ PINs are also to be distributed:
PKZ_PIN=YES
```

3

In the example above, only those PINs that were entered under the number "4711" on switch SIE1 are stored on switches "SIE2" and "SIE3" under extension "4711", and the PINs are not distributed to switch "SIE4".

If, for example, all PINs for a given switch are to be distributed, then different virtual numbers must be specified for each switch in the file extensions.dat.

File "Extensions.dat" in Directory "var/xie/pindist": Example 2

```
# Allocation Table SWITCH -> DIRECTORY NUMBER
# --------------------------------------------
#
# Syntax: <Switch><spaces><extension>
#
#         <Switch>     ... Switch name (max. 4 characters)
#         <spaces>     ... One or more blank spaces
#         <Extension>  ... Extension (max. 6 characters) or
#IGNORE if no PINs are to be distributed to this switch
#
#(Comment lines begin with the character '#')
#
SIE1 4711
SIE2 4712
SIE3 4713
SIE4 IGNORE
# If, "Master Switch" is specified, only new PINs will be
 distributed for this switch
MASTER_SWITCH=SIE1
# PKZ PINs are also to be distributed:
PKZ_PIN=YES
```

In this example, all PINs that were entered on switch SIE1 are stored on switches "SIE2" and "SIE3" under the extensions "4712" and "4713", respectively, and the PINs are not distributed to switch "SIE4".

In the event of large data volumes (e.g., > 20,000 PINs) or heavy system loads, the connection to the XIE server process may be interrupted due to a timeout (message "server timeout, no connection to xieserver" in the log file).

In that case, the parameter "SERVER_TIMEOUT" in the file /opt/xie/dmsie/CLaccess/xieserver.cfg must be increased from 28800 to 36000, for example.

After making this change, the xieserver must be restarted (i.e., first stop the server by executing /opt/xie/dmsie/bin/xieserver.sh stop, and then restart it with /opt/xie/dmsie/bin/xieserver.sh start).

The following steps must be taken when "upgrading" to a new OpenScape 4000 version:

1) Immediately before beginning the "upgrade", start the PIN distribution program.
2) Do not assign or modify any new or existing PINs.
3) Make a backup copy of the files /var/xie/pindist/Extension.dat and /var/xie/pindist/InsertedPins.dat
4) Perform the OpenScape upgrade procedure.
5) Restore the files /var/xie/pindist/Extension.dat and /var/xie/pindist/InsertedPins.dat from the backups.
6) The date in the file /var/xie/pindist/LastRuntime.ini must be set to the current date (following the "upgrade"; format: "YYYY-MM-DD HH:MM:SS"). This prevents previously distributed PINs from being processed again.
7) The PIN distribution program can now be activated.

The following steps must be taken when adding a new switch:

1) Save a copy of the file "Extensions.dat", naming it "Extensions.dat.save".
2) Rename the file "LastRuntime.ini" to "LastRuntime.ini.save".
3) For all switches, the directory number in the file "Extensions.dat" must be set to "IGNORE".
4) Add the new switch with the corresponding extension to the files "Extension.dat" and "Extensions.dat.save".
5) Activate the PIN distribution program; all PINs are then distributed to the new switch.
6) Following the distribution of PINs to the new switch, the file "Extensions.dat.save" must be copied back to "Extensions.dat" and the file "LastRuntime.ini.save" to "LastRuntime.ini".

The following steps must be taken when deleting a switch:

1) Deactivate the PIN distribution program.
2) Delete the switch (if applicable, create the same switch again?)
3) Set the date in the file /var/xie/pindist/LastRuntime.ini to the current date (following the deletion; format "YYYY-MM-DD HH:MM:SS"). This prevents previously distributed PINs from being deleted on the other switches!
4) The PIN distribution program can now be activated again.

5.9.4 Internal Processing

The following components were developed as part of the implemented solution:

The shell script "pindist.sh" is responsible for:

- Administration of PIN distribution (activation/deactivation and status)
- Adding/removing the PIN distribution program "pindist" to/from the cron table
- Displaying the log file

The C++ program "pindist" handles the actual distribution of PINs to all switches:

- The program uses the XIE class library XIE-API to communicate with the OpenScape/HiPath 4000.
- "SELECT switch_name FROM SWITCH" is used to read all switch names and save them in a list.
- The switches and extensions specified in the file "Extensions.dat" are read and saved in a list.
- "SELECT_UPDATES" is used to read all modified data records from ODF PIN as of a specific point in time (The first program call reads all the records, and this point in time corresponds to the last execution of "pindist").
- In the case of an "UPDATE" record (i.e., a PIN has been modified), there is no activity -- UPDATE instructions are not permissible for DMS-API objects of type PIN (DMS-API error message: 3754 - PIN and PIN Type cannot be changed).
- In the case of an "INSERT" record (i.e., a PIN has been added), an "INSERT" instruction is sent for each switch connected to the OpenScape 4000 Manager (by calling the XIE-API C++ method). In this way, the "pin_num" is set to the same new value on all switches. If a switch is listed in the file "Extensions.dat", the extension specified in "Extensions.dat" is used for the INSERT; otherwise, the extension from the corresponding "SELECT_UPDATES" record is used. In addition, the fields unique_key, domain, switch_name, extension, pin_num, pin_type, pin_class, pinindiv and user_create from the inserted records are stored in the file "InsertedPins.dat".
- In the case of a "DELETE" record (i.e., a PIN has been deleted), the data in the file "InsertedPins.dat" are used as the basis for deleting all records with the same domain and pin_num and pin_typ and pin_class (likewise by calling the corresponding XIE-API method). The deleted records are also deleted from the file "InsertedPins.dat".
- Upon completion of processing of all records associated with "SELECT_UPDATES", the current date and time are recorded in "LastRuntime.ini". The next time "pindist" is called, this date and time information is used as the reference basis for the "SELECT_UPDATES" call.

5.9.5 Directory Structure

During the installation of ASxie, the following files are installed in the directory /opt/xie/dmsie/pindist:

Table 3: Installation Files

Directory/File	Description
Extensions.dat.sample	Sample allocation table SWITCH ==>EXTENSION
pindis.sh	Shell script, responsible for administration
pindis	Main program

At runtime, the following files are created in the directory /var/xie/pindist:

Table 4: Files Created at Runtime

Directory/File	Description
LastRuntime.ini	File containing timestamp from previous execution (ASCII file with format: YYYY-MM-DD HH:MM:SS)
InsertedPins.dat	Table containing current PINs (this information required when deleting PINs)
pindist.prot	Log file from previous execution
Extensions.dat	Allocation table SWITCH ==> EXTENSION

In the xieserver configuration file /opt/xie/dmsie/CLaccess/xieserver.cfg, the following parameters are assigned default values as shown:

Table 5: xieserver Configuration Parameters

Parameter	Value	Description
MAX_CLIENTS	10	Max. number of concurrent XIE-Clients
PORT	2011	TCP/IP port number -- cannot be changed!
SERVER_TIMEOUT	1800	Timeout in seconds; No. of seconds the XIE server waits for requests from the client before clearing down the connection. For large data volumes (> 20,000 PINs), the timeout value must be increased, e.g., to 18000 seconds. After making this change, the xieserver must be restarted (/opt/xie/dmsie/bin/xieserver.sh stop to stop, then /opt/xie/dmsie/bin/xieserver.sh start to restart).

6 System parameters monitoring using OpenScape FM Client Agent

System parameters monitoring using OpenScape FM (Fault Management) Client Agent is possible on OpenScape 4000 Manager and Assistant.

NOTICE: This procedure must be performed again when updating with Major, Minor or FixRelease or when a reinstallation of Assistant/Manager is done manually or automatically (when disk full mechanism is triggered).

The local system management agent of OpenScape FM must be installed to monitor system parameters, such as CPU, file system, memory usage or the network load of OpenScape 4000 Assistant/Manager.

Follow the steps below to install and configure the OpenScape FM client agent:

1) Open the OpenScape FM installation zip and locate the two following files: `setup_agent_osfm.sh` and `setup_agent_osfm.jar`.

These files must be copied to a temporary location on the Manager/Assistant (e.g. `/tmp/`).

To install the Agent:

a) Open a SSH connection to the Manager or Assistant and navigate to the location where the files have been copied.

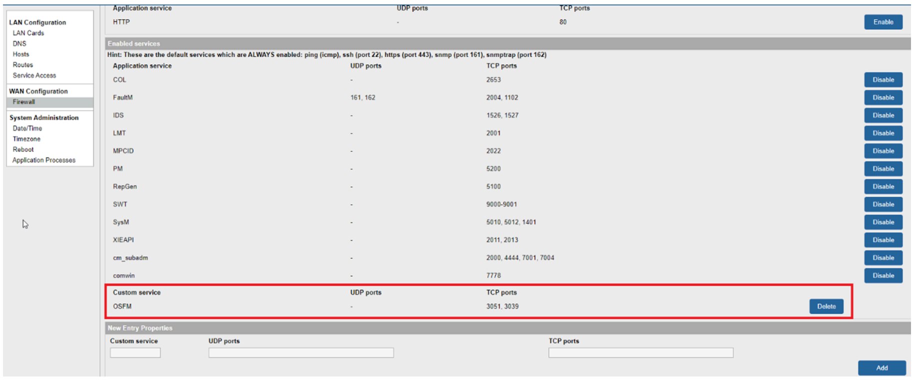
b) Run the installation script using the following command:

```
sh ./setup_agent_osfm.sh
```

c) Follow the on-screen instructions to complete the installation.

Once the installation is completed, the Agent is up and running.

2) For the communication between the Agent installed and OpenScape FM, the 3051 and 3039 ports must be open on the Manager/Assistant. This can be performed in the Webmin area of Manager/Assistant, under the **Firewall** section.



Application service	UDP ports	TCP ports	
HTTP	-	80	Enable

Enabled services

Hint: These are the default services which are ALWAYS enabled: ping (icmp), ssh (port 22), https (port 443), snmp (port 161), snmptrap (port 162)

Application service	UDP ports	TCP ports	
COL	-	2653	Disable
FaultM	161, 162	2004, 1102	Disable
IDS	-	1526, 1527	Disable
LMT	-	2001	Disable
MPCID	-	2022	Disable
PM	-	5200	Disable
RepGen	-	5100	Disable
SWT	-	9000-9001	Disable
SysM	-	5010, 5012, 1401	Disable
XIEAPI	-	2011, 2013	Disable
cm_subadm	-	2000, 4444, 7001, 7004	Disable
comwin	-	7778	Disable

Custom service	UDP ports	TCP ports	
OSFM	-	3051, 3039	Delete

New Entry Properties

Custom service	UDP ports	TCP ports

Figure 83: Enabling the 3051 and 3039 ports in Webmin

3) After successful installation of the Agent, a new host object should be available in the OpenScape FM client tree.

   If the host is not listed in the client tree, it must be added manually.

   To add a host manually:

   a) In the OpenScape FM client, right-click on **Network Topology**, then select **New** > **Host**.

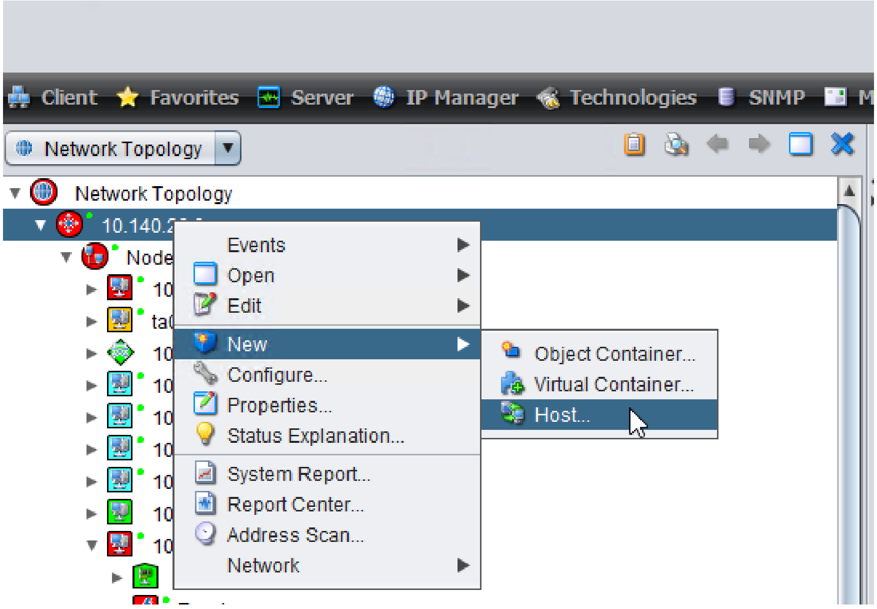


Figure 84: Adding the host in the OpenScape FM client tree

   b) Enter the IP address of Manager/Assistant in the **IP address** field.

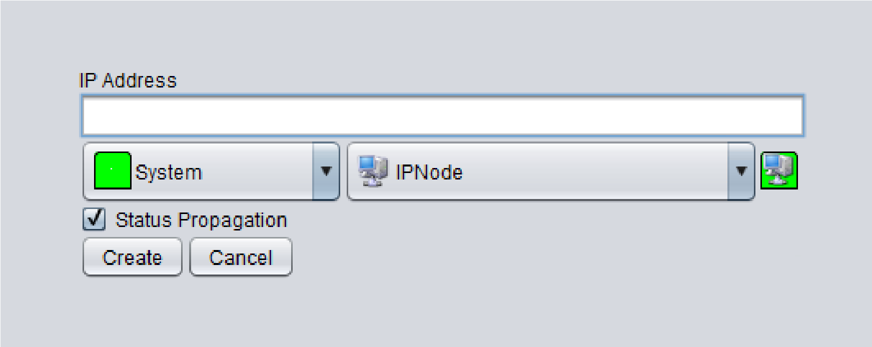


Figure 85: Entering the IP address of Manager/Assistant

4) Once the host appears in the OpenScape FM client tree, the auto-discovery process must be initiated to list all the properties monitored by OpenScape FM.

To start the auto-discovery process:

a) In the OpenScape FM client, right-click on the host, then select **Host** > **Start Discovery**.

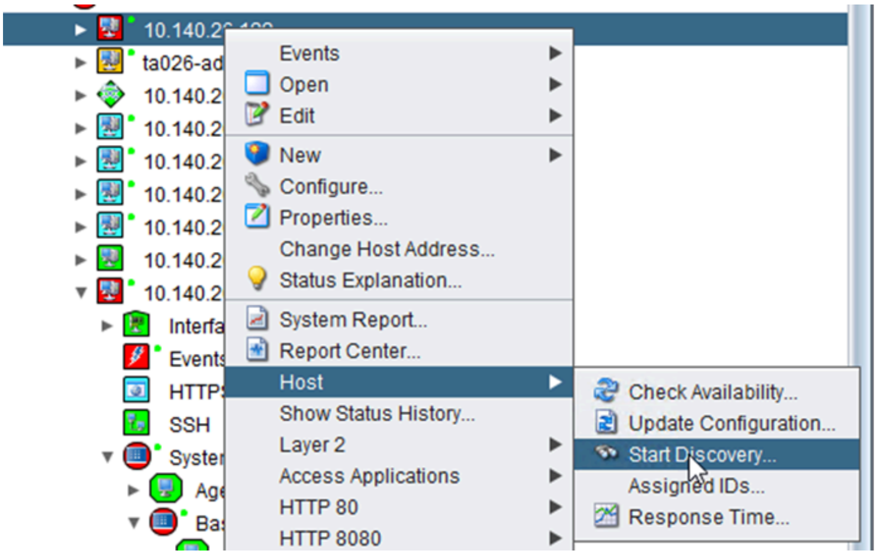


Figure 86: Starting the Discovery process

b) When the discovery process finishes, a new **System Management** entry is created under the OpenScape FM client tree.

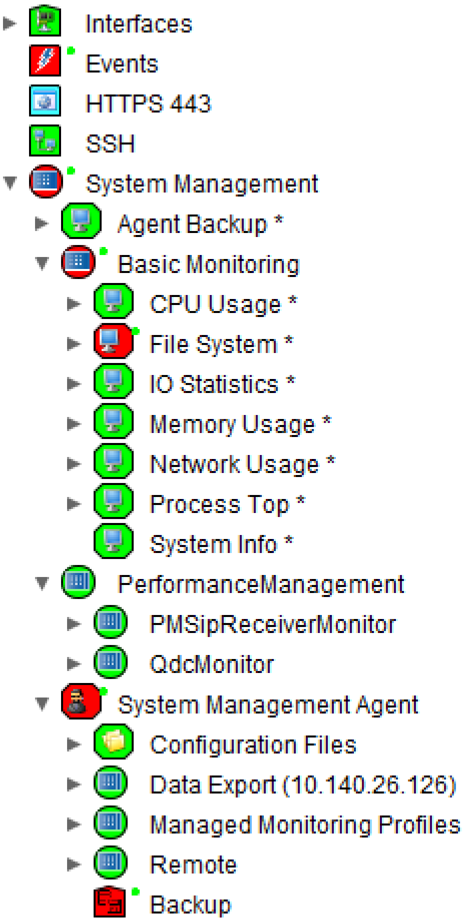


Figure 87: System Management entry in OpenScape FM client tree

6.1 Configure certificate for TLS in OpenScape FM Agent

In order to configure the certificate for TLS in OpenScape FM Agent, the keytool command will be used (this is part of the Java installation).

For example, a certificate including the private key in the keystore and alias `mycert1` is found in `/tmp/thecert.p12`.

Running the following command will configure the certificate for the Agent to use:

```
keytool -importkeystore -srckeystore /tmp/thecert.p12 -
srcalias mycert1 -destalias InternalWebServer -destkeystore
INSTALLDIR/ssma/conf/trustedcerts.jks
```

The agent certificate will be stored in the keystore `INSTALLDIR/ssma/conf/trustedcerts.jks` with the alias `InternalWebServer`.

The password for the keystore and private key are stored in `INSTALLDIR/system.properties`:

```
javax.net.ssl.keyStorePassword=xxxxxxx
javax.net.ssl.trustStorePassword=xxxxxxx
```

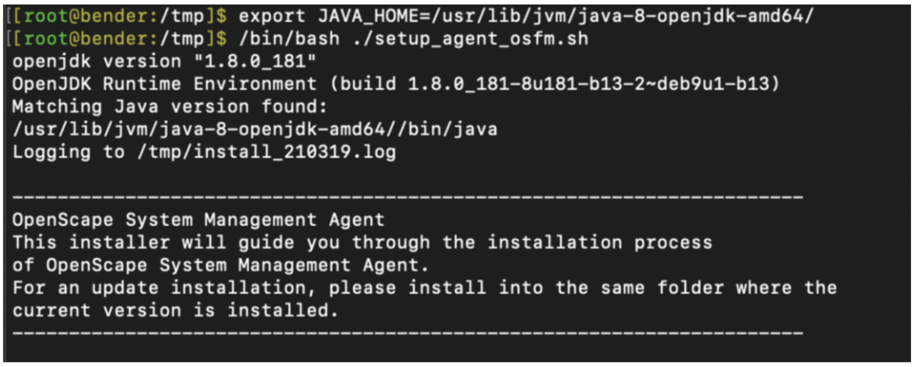
NOTICE:

Both the keystore and the private key need to have the same password. A private key without a password will not work. The password, specified in `system.properties`, is used for keystore and private key.

Some special characters like **!** will be escaped using the backslash. These are not part of the password.
At each password change the Agent must be restarted to take account of the new password.

6.2 Troubleshooting

1) If Java is not found, you can set the environment variable `JAVA_HOME` to point to the desired Java installation, as displayed in the figure below.

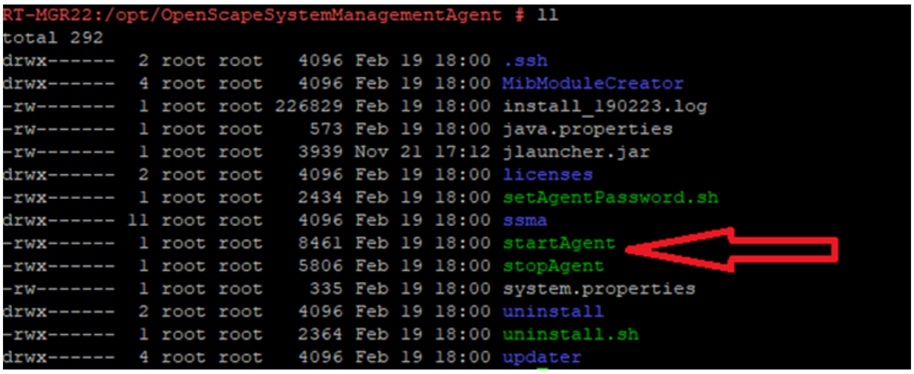


```
[[root@bender:/tmp]$ export JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64/
[[root@bender:/tmp]$ /bin/bash ./setup_agent_osfm.sh
 openjdk version "1.8.0_181"
 OpenJDK Runtime Environment (build 1.8.0_181-8u181-b13-2~deb9u1-b13)
 Matching Java version found:
 /usr/lib/jvm/java-8-openjdk-amd64//bin/java
 Logging to /tmp/install_210319.log

 ----------------------------------------------------------------------
 OpenScape System Management Agent
 This installer will guide you through the installation process
 of OpenScape System Management Agent.
 For an update installation, please install into the same folder where the
 current version is installed.
 ----------------------------------------------------------------------
```

2) OpenScape FM requires ICMP to retrieve data from the Agent. Therefore, you must ensure that the OS used for the OpenScape FM instance is not blocking it. Some firewall rules might need to be defined in certain OS.

3) If System Management is not discovered by the OpenScape FM, you must check if the Agent is running on the Manager or on the Assistant.

By default, the Agent starts after system installation or reboot. If there is no service running for the Agent, it can be started manually, by using the scripts available in the location where the Agent has been installed in Manager/Assistant (e.g. the default location of the Agent: `/opt/OpenScapeSystemManagementAgent`).



```
RT-MGR22:/opt/OpenScapeSystemManagementAgent # ll
total 292
drwx------  2 root root   4096 Feb 19 18:00 .ssh
drwx------  4 root root   4096 Feb 19 18:00 MibModuleCreator
-rw-------  1 root root 226829 Feb 19 18:00 install_190223.log
-rw-------  1 root root    573 Feb 19 18:00 java.properties
-rw-------  1 root root   3939 Nov 21 17:12 jlauncher.jar
drwx------  2 root root   4096 Feb 19 18:00 licenses
-rwx------  1 root root   2434 Feb 19 18:00 setAgentPassword.sh
drwx------ 11 root root   4096 Feb 19 18:00 ssma
-rwx------  1 root root   8461 Feb 19 18:00 startAgent
-rwx------  1 root root   5806 Feb 19 18:00 stopAgent
-rw-------  1 root root    335 Feb 19 18:00 system.properties
drwx------  2 root root   4096 Feb 19 18:00 uninstall
-rwx------  1 root root   2364 Feb 19 18:00 uninstall.sh
drwx------  4 root root   4096 Feb 19 18:00 updater
```

7 OpenScape 4000 SNMP Management

This chapter describes the configuration and startup of the SNMP agents on OpenScape 4000, and the scripts "read_filter.ksh" and "set_filter.ksh" used for time-controlled filtering of OpenScape 4000 Proxy Agent alarm messages.

7.1 Scope of Validity

This chapter describes the administration of the SNMP on OpenScape 4000, including verification of installation, configuration and startup.

7.2 General Information

The OpenScape 4000 SNMP Proxy Agent facilitates the management of OpenScape/HiPath 4000 systems based on the Simple Network Management Protocol (SNMP). SNMP is the standard network management protocol used in the Internet world. As an underlying principle of Internet management, agents are used to collect network management data and forward this data to a central network management system.

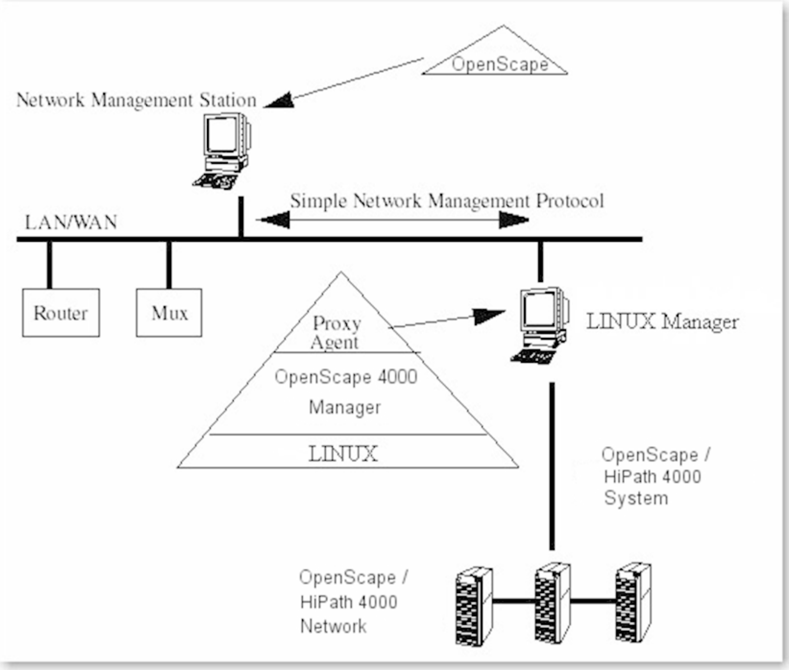

OpenScape
Network Management Station
Simple Network Management Protocol
LAN/WAN
Router
Mux
Proxy Agent
OpenScape 4000 Manager
LINUX
LINUX Manager
OpenScape / HiPath 4000 System
OpenScape / HiPath 4000 Network

Figure 88: Component Structure of OpenScape SNMP Management

An OpenScape/HiPath 4000 network comprises a number of OpenScape/ HiPath 4000 systems, which are administered by the OpenScape 4000 Manager. The OpenScape 4000 SNMP Proxy Agent is part of the OpenScape 4000 Manager installation package. The OpenScape 4000 system (AMO interface) and the OpenScape 4000 Manager together form the information base for the OpenScape 4000 SNMP Proxy Agent. The OpenScape 4000 SNMP Proxy Agent models and/or makes available the information required for network management in a Management Information Base (MIB). The MIB is monitored or evaluated by a network management system. In addition, the OpenScape 4000 SNMP Proxy Agent forwards SNMP traps (e.g., alarm messages) to the network management system (system on which the OpenScape network management software resides).

7.3 OpenScape 4000 SNMP Proxy Agent

The OpenScape 4000 SNMP Proxy Agent (packages: ASsnmp, ASfm) is installed automatically with the installation of the OpenScape 4000 Manager platform.

7.3.1 Description of Contents

The OpenScape 4000 SNMP Agent comprises several subagents. The subagents constitute a logical component (MIB) of the Emanate Master Agent, i.e., they receive SNMP requests (SNMP-Get, SNMP-Set etc.) from the Emanate Master Agent, and send the results back to the SNMP requester via the Master Agent.

The OpenScape 4000 SNMP Agent comprises the following subagents and processes:

1) systemagt : The System Subagent administers the list of known OpenScape 4000 containing system information, and notifies other components of the OpenScape 4000 SNMP Agent when changes are detected in this list. The Manager station (OpenScape) is informed of changes by means of traps.

2) alarmagt : The purpose of this agent is to make OpenScape 4000 alarms and/or alarm filter configurations available. The Alarm Agent sends traps when there are changes in the alarm states.

3) erroragt : This agent provides information about errors/faults that occur in the OpenScape/HiPath 4000 network.

4) softagt : The Software Subagent provides information about software versions and installed patches.

5) hardagt : With the help of the Hardware Subagent, information about the hardware configuration of an OpenScape/HiPath 4000 system can be retrieved via SNMP.

6) topoagt : The Topology Subagent provides information about the network structure.

7) sqlagt : Through the use of the SQL Subagent, a wide range of information in the OpenScape 4000 Manager database can be queried directly via SNMP.

8) disagt : The task of the Discovery Subagent is to collect the basic information about an OpenScape/HiPath 4000 system (HW, SW, topology, alarm configuration) directly via the AMO interface, and then convert this information into a form that can be processed by the other subagents.

9) commonagt: The Common Agent providing information for Common Management Portal (system versions, cpu usage, memory usage, backup states, CM upload states).

10) hipathmgragt: The Supervisor Agent used for Management of the OpenScape 4000 Manager (process management, setting intervals for batch execution, setup filesytem usage monitoring).

11) mib2agt: This subagent provides information based on RFC-1213 (http://www.ietf.org/rfc/rfc1213.txt).

NOTICE: A detailed description of the information provided by the various subagents can be found in the Management Information Base (MIB).

7.3.2 Installation Verification

Upon successful installation of the OpenScape 4000 SNMP Proxy Agent, the subagents systemagt, alarmagt, erroragt, softagt, hardagt, topoagt, sqlagt, disagt, commonagt, hipathmgragt, and mib2agt are started automatically.

To verify that the subagents are running properly, you can perform the following check:

```
ps -ef | grep agt
```

If all agent processes are running, the display will look something like this:

```
root 6524 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
systemagt
root 7065 1 0 May16 ? 00:00:05 /opt/hipath_agents/bin/
alarmagt
root 7084 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
erroragt
root 7108 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
softagt
root 7125 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
hardagt
root 7146 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
topoagt
root 7163 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
sqlagt
root 7180 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
disagt
root 18575 1 0 Jun06 ? 00:00:00 mib2agt
root 18577 18570 0 Jun06 ? 00:00:31 hipathmgragt
root 18581 18563 0 Jun06 ? 00:00:00 commonagt
root 27971 1 0 May25 ? 00:00:00 /opt/hipath_agents/bin/
portagt
```

If not all subagent processes are running, it is possible that the SNMP Agent was not installed correctly.

Perform the following tests

Check whether the EMANATE Master Agent is running:

```
ps -ef | grep snmpdm
```

If the Master Agent is running, the following will be displayed:

```
root 18548 18540 0 Jun06 ? 00:00:00 snmpdm -d
```

7.4 Configuring Communities and Traps

The SNMP agent needs to be configured in order to send SNMP traps (events) to OpenScape FM and to allow OpenScape FM read and write operations.

This configuration can be done from the user interface of the Fault Management -> SNMP Configurator. In the local profile.

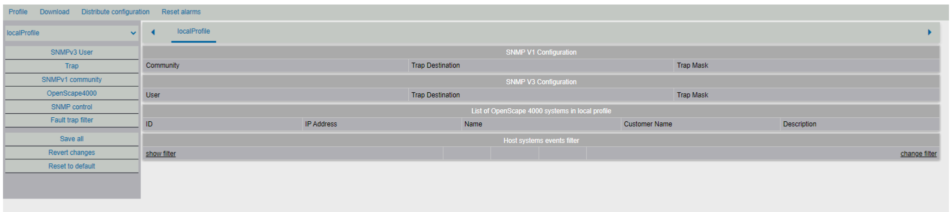


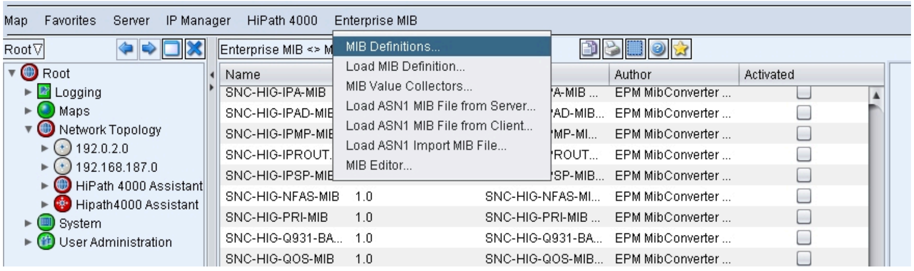
Figure 89: SNMP Configuration Data Example

NOTICE: The same community string (e.g., 'mib' as above) has to be set in OpenScape FM (context menu entry "..SNMP parameters ..") after adding a OpenScape 4000 Manager system to the network topology. If community strings don't match, the OpenScape 4000 Manager will not be discovered as type OpenScape 4000 Manager (PC symbol appears only).

In order to see all trap messages that can be produced by the OpenScape4000 Manager/Assistant in OpenScapeFM, it is necessary to activate the SIEMENS-PN-MIB (can be downloaded under "Download MIB files --> Download the definition (.mib) file for the Hipath 4000 MIB, Figure 6-2) via Enterprise MIB->MIB Definitions in OpenScapeFM. Please note that this MIB also includes HiPath4000 alarm traps which are allready handled by the HiPath4000 PlugIn. The activation of the entire SIEMEMS-PN-MIB may result in duplicate entries in the Event Browser. Therefore, you have to use Event Configuration to deactivate unneeded traps.

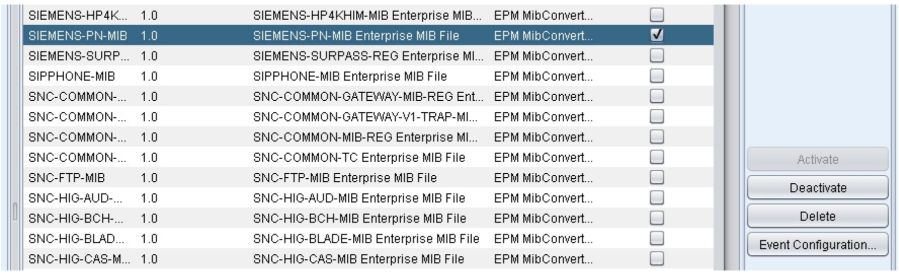
7.4.1 Step By Step:

1) Open the **OpenScapeFM** client window.
2) Open the MIB Definitions - **Enterprise MIB -> MIB Definitions**.



Name			Author	Activated
SNC-HIG-IPA-MIB		'A-MIB ...	EPM MibConverter ...	□
SNC-HIG-IPAD-MIE		'AD-MIB...	EPM MibConverter ...	□
SNC-HIG-IPMP-MIE		'MP-MI...	EPM MibConverter ...	□
SNC-HIG-IPROUT.		'ROUT...	EPM MibConverter ...	□
SNC-HIG-IPSP-MIE		'SP-MIB...	EPM MibConverter ...	□
SNC-HIG-NFAS-MIB	1.0	SNC-HIG-NFAS-MI...	EPM MibConverter ...	□
SNC-HIG-PRI-MIB	1.0	SNC-HIG-PRI-MIB ...	EPM MibConverter ...	□
SNC-HIG-Q931-BA...	1.0	SNC-HIG-Q931-BA...	EPM MibConverter ...	□
SNC-HIG-QOS-MIB	1.0	SNC-HIG-QOS-MIB...	EPM MibConverter ...	□

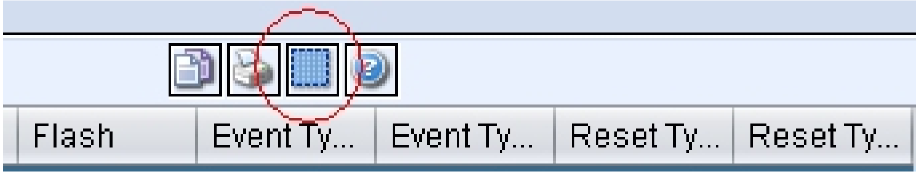
3) Select the **SIEMENS-PN-MIB Enterprise MIB** file and click the **Activate** button.



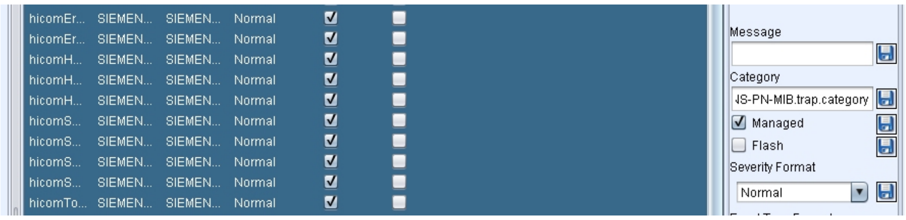
SIEMENS-HP4K...	1.0	SIEMENS-HP4KHIM-MIB Enterprise MIB...	EPM MibConvert...	□
SIEMENS-PN-MIB	1.0	SIEMENS-PN-MIB Enterprise MIB File	EPM MibConvert...	☑
SIEMENS-SURP...	1.0	SIEMENS-SURPASS-REG Enterprise MI...	EPM MibConvert...	□
SIPPHONE-MIB	1.0	SIPPHONE-MIB Enterprise MIB File	EPM MibConvert...	□
SNC-COMMON-...	1.0	SNC-COMMON-GATEWAY-MIB-REG Ent...	EPM MibConvert...	□
SNC-COMMON-...	1.0	SNC-COMMON-GATEWAY-V1-TRAP-MI...	EPM MibConvert...	□
SNC-COMMON-...	1.0	SNC-COMMON-MIB-REG Enterprise MI...	EPM MibConvert...	□
SNC-COMMON-...	1.0	SNC-COMMON-TC Enterprise MIB File	EPM MibConvert...	□
SNC-FTP-MIB	1.0	SNC-FTP-MIB Enterprise MIB File	EPM MibConvert...	□
SNC-HIG-AUD-...	1.0	SNC-HIG-AUD-MIB Enterprise MIB File	EPM MibConvert...	□
SNC-HIG-BCH-...	1.0	SNC-HIG-BCH-MIB Enterprise MIB File	EPM MibConvert...	□
SNC-HIG-BLAD...	1.0	SNC-HIG-BLADE-MIB Enterprise MIB File	EPM MibConvert...	□
SNC-HIG-CAS-M...	1.0	SNC-HIG-CAS-MIB Enterprise MIB File	EPM MibConvert...	□

4) Click the **Event Configuration** button to display the **Event Configuration** window.

5) Click **Select All Entries**.



6) Uncheck the **Managed** checkbox and click the **Save** button.



hicomEr...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomEr...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomH...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomH...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomH...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomS...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomS...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomS...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomS...	SIEMEN...	SIEMEN...	Normal	☑	□
hicomTo...	SIEMEN...	SIEMEN...	Normal	☑	□

Message

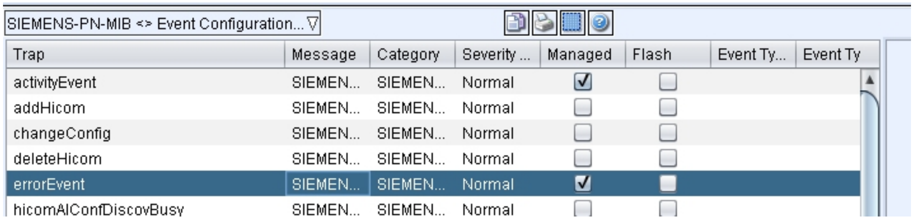
Category
IS-PN-MIB.trap.category

☑ Managed

□ Flash

Severity Format
Normal

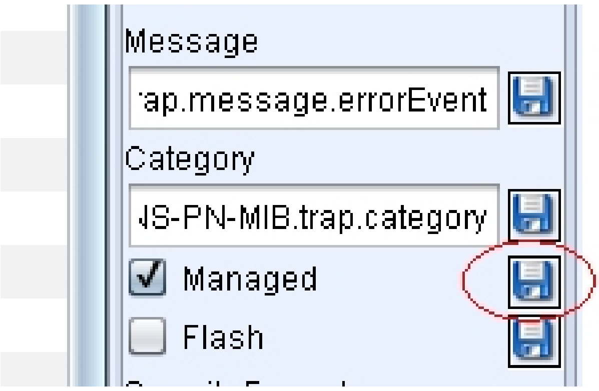
7) Select **activityEvent**, **errorEvent**, and **syslogMessage** in the **Managed** column.



SIEMENS-PN-MIB <> Event Configuration...

Trap	Message	Category	Severity ...	Managed	Flash	Event Ty...	Event Ty
activityEvent	SIEMEN...	SIEMEN...	Normal	☑	□		
addHicom	SIEMEN...	SIEMEN...	Normal	□	□		
changeConfig	SIEMEN...	SIEMEN...	Normal	□	□		
deleteHicom	SIEMEN...	SIEMEN...	Normal	□	□		
errorEvent	SIEMEN...	SIEMEN...	Normal	☑	□		
hicomAlConfDiscovBusy	SIEMEN...	SIEMEN...	Normal	□	□		

8) Click the **Save** button.



Message
'ap.message.errorEvent

Category
IS-PN-MIB.trap.category

☑ Managed

□ Flash

7.5 Relevant AMO Commands

Some of the data made available by the individual subagents via the MIB is retrieved directly from the OpenScape 4000 Manager database. A large portion of this data, however, is obtained directly from the output of various AMO commands and stored in a separate area of the OpenScape 4000 Manager database during the discovery process. Table 8 lists the relevant AMOs and the data extracted from them.

Table 6: Data Extracted from AMOs

AMO	Extracted Information	Subagent
APS	Program system, part number	softagt

AMO	Extracted Information	Subagent
BCSM	Module, Slot addr., Soll-BG, HW-Abk., Ist-BG, Firmware, Rev. level, BG-Zustand	hardagt
BCSU	LTU, LTG, Soll-BG, Ist-BG, Type, Rev. level, Firmware, BG-Zustand	hardagt
BUEND	Trunk Grp. No., Trunk Grp. Name, Max. No., Device Type	topoagt
CDSM	Cabinet address, Mounting unit, Slot, Ist-BG, HW-Abk., Rev. level, Firmware	hardagt
CDSU	Cabinet address, Mounting unit, Slot, Ist-BG, HW-Abk., Rev. level, Firmware	hardagt
CONSY	Shelfno., Frame, PID1, PID2, PID3, LTU	hardagt
DDSM	Controller, Type, Size, SS-NO, GRAN	hardagt
PATCH / PATAD	Patch group, Patch number, Activation state, HD/RAM	softagt
TACSU	Lage, GER, BUNR, SATZNR, INBETR, KNNR, ALARMNR	topoagt
TDCSU	Lage, GER, BUNR, BKANAL, BKGR, INBETR, ALARMNR	topoagt
TSCSU	LAGE, GER, BUNR, SATZNR, INBETR, KNNR, ALARMNR	topoagt
VADSM	ALARMGRUPPE, ALARMNR, SCHWELL1, SCHWELL2, ZEIT1, ZEIT2, NAME	erroragt
VADSU	ALARMGRUPPE, ALARMNR, SCHWELL1, SCHWELL2, ZEIT1, ZEIT2, NAME	erroragt
KNTOP	ltg, ltu, slot, satznr, bkanalgrp, p_nodeindex, p_ltg, p_ltu, p_slot, p_satznr, p_bkanalgp, p_nodeno, bunr	topoagt
KNDEF	vknnr, def_vknnr	topoagt
APRT	ipaddr	hardagt
ZAND (FUNCT)	KNNR, LANGUAGE	systemagt
SBCSU	tel_nr, pen	hardagt
PERSI	location	hardagt
GRA	Upload Alarm Mirror, Reset Alarm	Alarmagent

7.6 Time-controlled Alarm Messages

This section describes the installation, configuration, administration and basic usage of the scripts read_filter.ksh and set_filter.ksh, which can be used for time-controlled filtering of alarm messages from the OpenScape 4000 Proxy Agents.

7.6.1 General Information

The implementation of time-controlled OpenScape 4000 alarm messages constitutes an enhancement of the OpenScape 4000 Proxy Agent. One of the tasks of the OpenScape 4000 Proxy Agent is to forward OpenScape 4000 alarm messages to OpenScape Fault Management (FM). By enhancing the SNMP Proxy Agent to include time-controlled OpenScape 4000 alarm messages, the forwarding and indication of specific OpenScape 4000 alarm messages can be activated and/or deactivated at configurable times. This enhancement was implemented based on the existing filtering mechanism of the SNMP Proxy Agent for alarm messages.

The filter handling can be done via SNMP get/set requests or by scripts:

- /opt/hipath_agents/bin/read_filter.ksh
- /opt/hipath_agents/bin/set_fileter.ksh

These scripts are only wrapping SNMP get/set requests with âprivate" community and managing cron entries for snmp traps filtering based on the configuration files given as aguments for these scripts.

Examples of such configuration files are in:

- /opt/hipath_agents/bin/conf/activate.cnf
- /opt/hipath_agents/bin/conf/filter_demo.cnf
- /opt/hipath_agents/bin/conf/feiertag_demo.cnf

To use this scipts it is neccessary to have configured SNMP v1 "private" community string configured (see Section 6.4, "Configuring Communities and Traps").

7.6.2 Program Execution

The mechanism that is used to control the alarm filters essentially consists of two scripts. The task of the script read_filter.ksh is to read the execution file activate.cnf, which defines the activation and deactivation times of the alarm messages being filtered. The name of the execution file is fixed. The activation times defined for the filters in this file are combined with the corresponding parameters (filter file, holiday file, activation flag) to form an instruction and stored as a cron job. Various different files can be used for the filters and holidays. The naming of these files is not critical. However, like the execution file activate.cnf, the files must reside in the directory /opt/hipath_agents/conf. If the cron job written to the cron table by the script read_filter.ksh is activated, the script set_filter.ksh is called. This script performs two functions: a) it activates and/or deactivates the filters for the alarm messages via a SNMP set, based on the parameters in the cron job, and b) it maintains the file filter_state, which preserves the states of the set filters for other specific purposes.

It is important to note that each filter file in the execution file is viewed as a type of filter group. Once they are set, the filters in each filter group/filter file can only be deactivated via the same filter group/filter file. Similarly, filters are not reset if they were set by a different filter group/filter file. For example, suppose that six (6) alarm filters were set via 2 filter files "filtergrp1[1,2,3,4]" ,"filtergrp2 [3,4,5,6]". In the event of a deactivation via filter file "filtergrp1", only alarm filters 1,2 will be reset, since alarm filters 3 and 4 are also contained in the filter file "filtergrp2."

NOTICE: When a filter is set via this mechanism, the previous status of the filter is overwritten in all cases.

7.6.3 Notes Regarding Application

A prerequisite for using this software is that the agents, as well as the Emanate Master Agent, must be running at the specified activation times. In addition, the write community in the file set_filter.ksh must be set in accordance with the configuration of the Emanate Master Agent.

The software can be activated by performing the following two steps:

1) Configure the execution file "activate.cnf" and the various filters and holiday files; refer to Section 6.6.4, "Execution File", Section 6.6.5, "Alarm Filter File" and Section 6.6.6, "Holiday File".

2) Start the script read_filter.ksh.

Anytime a change is made in the configuration files, the script read_filter.ksh must be executed again, to make sure that the cron table is always up to date.

7.6.3.1 Example of Configuration

Let's assume that for the system with Pabx_id 10002, an alarm filter for the alarm of Group 3, Class 33, priority major is to be set every Monday at 10:00 a.m., except on a holiday. In addition, it is to be reset on a holiday Tuesday at 12:00 noon.

The configuration is as follows:

Filter file "filter.cnf":

100002 3 33 2 // Alarm to be filtered

The holiday file is not relevant in this case, but must be present in any case:

Holiday file "feiertag.cnf":

// This is the holiday file 01.11.2005 // All Saintsâ Day 24.12.2005 // Christmas Eve

In order to activate/reactivate the filters at the designated times, the following entries must be made in the execution file "activate.cnf":

Mo 10:00 filter.cnf holiday.cnf false true Tu 12:00 filter.cnf holiday.cnf true false

After configuring the execution file, the script read_filter.ksh must be run, e.g., with the command "/opt/hipath_agents/bin/read_filter.ksh"

This instruction generates the following additional entries in the cron table:

00 10 * * 1 /opt/hipath_agents/bin/set_filter.ksh filter.cnf holiday.cnf false true 00 12 * * 2 /opt/hipath_agents/bin/set_filter.ksh filter.cnf holiday.cnf true false

At the corresponding times, the script set_filter.ksh is called in order to set/reset the corresponding filters.

7.6.3.2 Administration of Scripts

The following variables in the scripts read_filter.ksh and set_filter.ksh influence the behavior of the scripts:

Community:

The community in the file set_filter.ksh must corresponding to the settings in the Emanate Master. This community must have write access to the OpenScape 4000 MIB. The default value is "private". The default can be changed after installation.

DBG_FLAG:

If this flag is set to 0 (ON) in the scripts, various debugging information is output to the file /tmp/set_filter.log or /tmp/read_filter.log. This function can be deactivated by setting the value to 1 (OFF).

7.6.4 Execution File

Each line in the execution file /opt/hipath_agents/conf/activate.cnf defines a deactivation time or an activation time. Make sure that the individual time values do not coincide; otherwise, errors may occur during execution.

The execution file is set up as follows:

// Comment

or

DayOfWeek { mo | tu | we | th | fr | sa | su | all } Time {HH:MM} AlarmFilterFile HolidayFile HolidayFlag{true|false} ActivationFlag{true|false}

The entries in a holiday file must be entered manually by the customer. For example:

mo 10:00 filter.cnf holiday.cnf false true

This means that the alarms in the file filter.cnf will be activated every Monday at 10:00 a.m., unless it is a holiday as specified in the holiday file holiday.cnf.

all 10:00 filter.cnf holiday.cnf true false

In this case, the alarms in the file filter.cnf will be deactivated every day at 10:00 a.m., if the day is a holiday as specified in the holiday file holiday.cnf.

7.6.5 Alarm Filter File

Each line in an alarm filter file defines an alarm for which the filter is activated/ deactivated in accordance with the script.

The format is as follows:

// Comment

or

PabxId AlarmGroup AlarmNumber Priority // Comment

The values for the Priority field are:

1 -> minor

2 -> major

3 -> device

The entries in the alarm filter file must be done manually by the customer.

Example:

```
// This is the filter file
10 1 1 1 // KOELN CC Restart Minor
10 1 1 2 // KOELN CC Restart Major
```

7.6.6 Holiday File

Each line in a holiday file defines a holiday. The format is as follows:

// Comment

or

DD.MM.YYYY // Comment

where DD stands for Day, MM for Month and YYYY for Year

The entries in the holiday file must be done manually by the customer.

Example:

```
// This is the holiday file
01.11.2005 // All Saints' Day
24.12.2005 // Christmas Eve
25.12.2005 // Christmas Day
26.12.2005 // Day after Christmas
31.12.2005 // New Year's Eve
01.01.2006 // New Year's Day
```

7.6.7 Alarm Filter handling over SNMP

Apart from using the internal scripts for filtering OpenScape 4000 proxy alarm trap messages, you can use SNMP set requests for permanent filter definitions.

The filter can be defined via SNMP set requests in the following OID format, setting to '4' (integer):

.1.3.6.1.4.1.231.7.2.1.2.3.1.6.pabxid.AlGroup.AlSubID.AlPriority

Where AlPriority is defined as: 1 .. minor, 2 .. major, 3 .. device.

After the creation of such an entry the filter is automatically switched on.

The same SNMP set request with setting to '6' (integer) will delete this filter from the table of filters.

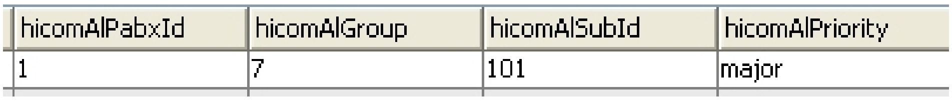
To switch the filter on/off, you can use an SNMP set request on the following OID:

.1.3.6.1.4.1.231.7.2.1.2.3.1.5.pabxid.AlGroup.AlSubID.AlPriority

The setting to '2' (integer) switches the alarm OFF, and the setting to '1' (integer) switches the alarm ON.

Example:

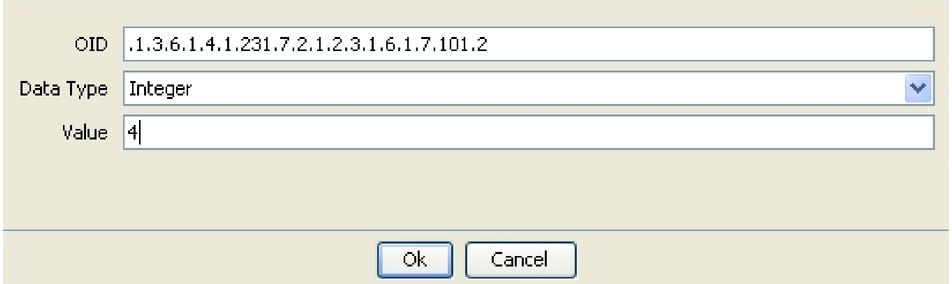
You want to filter the trap for the following alarm (Manager alarm SWA_ACTIVATION_FAILED):



hicomAlPabxId	hicomAlGroup	hicomAlSubId	hicomAlPriority
1	7	101	major

Figure 90: Filter for Alarm

To do so, set the following request:



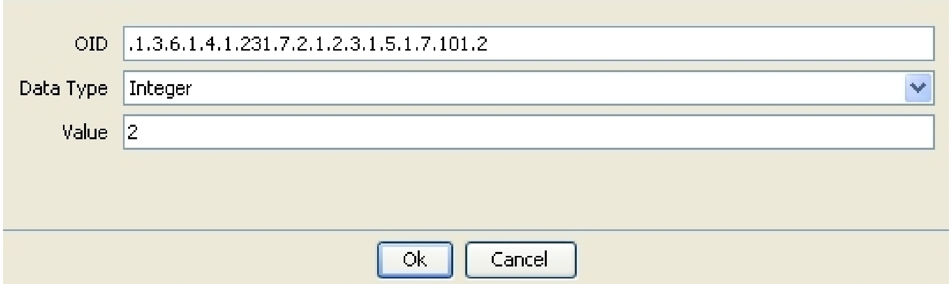
OID .1.3.6.1.4.1.231.7.2.1.2.3.1.6.1.7.101.2

Data Type Integer

Value 4

Figure 91: SNMP Request Setting Example

To switch off this filter, set the value to '2' (integer):



OID .1.3.6.1.4.1.231.7.2.1.2.3.1.5.1.7.101.2

Data Type Integer

Value 2

Figure 92: SNMP Request Setting Example

The list of the defined filters and their states is defined in the SNMP hicomFiltAlConfTable with OID .1.3.6.1.4.1.231.7.2.1.2.3.

7.7 Setting Up Local Alarms in OpenScape 4000 Manager

You must edit the file /opt/ncc/bin/options and uncomment the line

```
#STORE_LOG=ON;export STORE_LOG
```

to

```
STORE_LOG=ON;export STORE_LOG
```

This activates the following new alarms generated on the OpenScape 4000 Manager:

```
RETRY EXCEEDED: Col could not fetch CDR file
NOT ENOUGH SPACE: No Space for Performance Management
```

```
SWITCH ACCESS FAILING: Polling of OpenScape/HiPath failed
 (activation project specific)
DB FULL: Informix DB reached high water
INFORMIX: General DB problems
DISK FULL: No Disk space
AFR DB SPACE : Database Threshold reached: Inserting error
 messages into Database table "lerror" was stopped
AFR STOPPED : No alarm and error messages will be received
 because AFR was stopped on RMX side
AFR FAULT : An error occured during analysis of received
 AFR message
AUTOLCK: User account automatically locked
BACKUP FAILED : An error occured during data backup
RESTORE FAILED : An error occured during restore of data
DISK FULL : Disc space has reached threshold level
THRESH. EXCEEDED : Database of PM has reached threshold
 level
```

NOTICE: There are more alarms that can be generated on Manager. To activate these alarms see Chapter 6.8.2, "Enhanced SNMP alarms for Monitoring of the Manager".

7.8 Monitoring of Manager via SNMP – HiPath Supervisor Agent

The HiPath Supervisor agent offers SNMP support for OpenScape 4000 Manager, by which it is possible to monitor resources of the Manager itself.

The SNMP agent offers the remote monitoring of

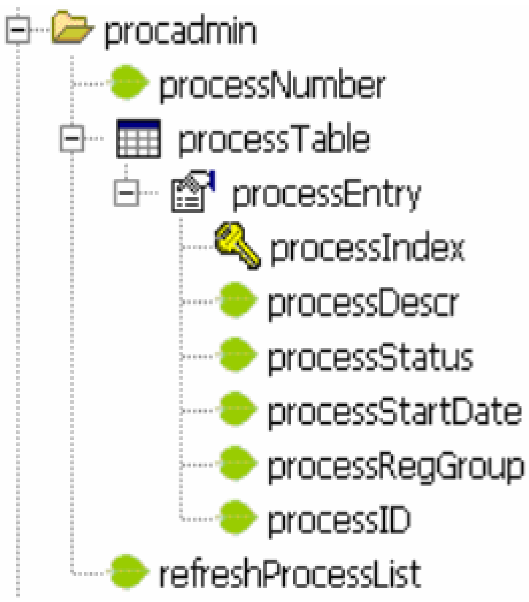
- Systems processes on the manager
- Disk file system monitoring
- Proxy agents handling
- Database threshold reached for PM
- LogM
- LMT status overview
- COL backup settings to activate or deactivate
- dipasBatch parameter settings
- Checking errors and alarms.

The HiPath Supervisor agent works with the OpenScape 4000 MIB, (Management Information Base; refer to Section 6.8.1).

The MIB can be downloaded from the SNMP Configurator, refer to Section 6.4.

7.8.1 MIB table for HiPath 4000 Supervisor Agent

hipath4000Supervisor	**Description**



HiPath Supervisor agent offers the possibility to display lists of information about system processes and their states.

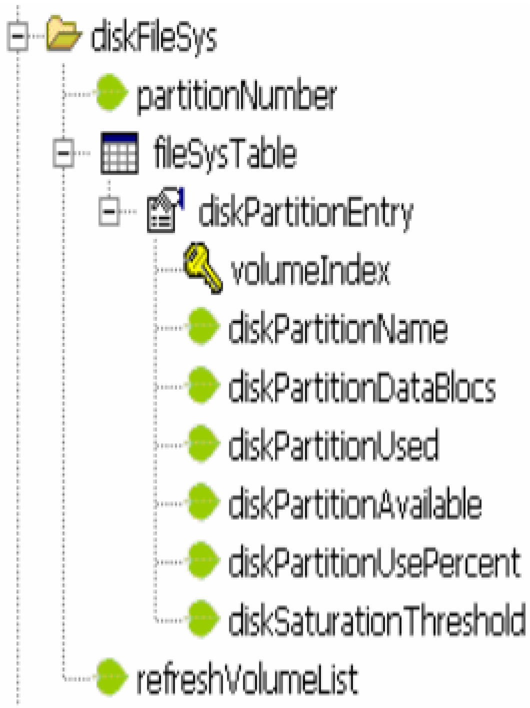
The results are transferred to the SNMP **processTable** with the size defined in **processNumber**.

processEntry contains information about particular processes controlled by **procadmin** – there are the following items:

- **processIndex** is a unique value for each process. Its value ranges between ’1’ and the value for processNumber . The value for each process must kept constant at least from one reinitialization of the process entity's to the next reinitialization.
- **processDescr** is a text string containing information about the process. This string should include the name of the process shown by procadmin.
- **processStatus** is the status of the process shown by procadmin.
- **processStartDate** shows the date and time when the process was started.
- **processRegGroup** is the registration group to which the process belongs
- **processID** is the ID of the process provided by the operating system. If any process is not running, there is the ’record about pid’ in table with the value ’0’.

All rows in **processTable** are kept in memory. For each query ’get’ or ’get-next’, current data are returned, but the number of processes remains unchanged. The query type of ’get’ is possible only for items which were already loaded by a ’get-next’.

In case any **processRegGroup** is uninstalled, an empty row will be processed in the table, with a zero pid. For reloading the whole table, it is necessary to set the **refreshProcessList** value to ’1’.



diskFileSys serves as instrument for monitoring disk partition filesystem and watching over occupancy of partition volume.

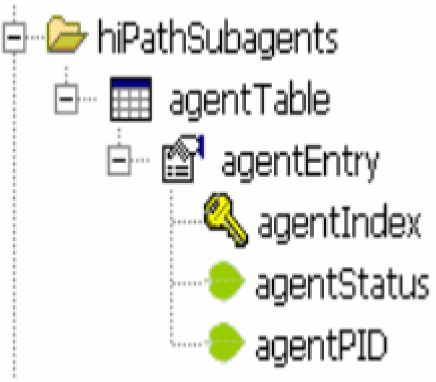
The **fileSysTable** table is derived from information observed by system command df -kP , number of rows is determined by **partitionNumber** and contains the following columns:

- **volumeIndex** is a unique value for each volume. Its value ranges between ’1’ and the value of **partitionNumber**. The value for each volume must remain constant at least from one reinitialization of the volumes entity's to the next reinitialization.
- **diskPartitionName** is the name of the disk partition
- **diskPartitionDataBlocs** is the data size of the volume on the disk partition (in kB)
- **diskPartitionUsed** is the filled space on disk partition (in kB)
- **diskPartitionAvailable** is the available space on the disk partition (in kB)
- **diskPartitionUsePercent** is the value of free space in percentage on the disk partition
- **diskSaturationThreshold** is the threshold value which informs about saturation of partial harddisk volume in percentage. There are scannings in 30 sec. intervals if **diskPartitionUsePercent** is equal or exceeds the **diskSaturationThreshold** value.

  Afterwards trap messages are send.

  diskSaturationThreshold can be set using SNMP request in range from 0 - 100%. When a customer set the threshold to 0, saturation monitoring will be deactivated for this partition.

Reinitialization of **fileSysTable** can be initiated by setting ’1’ in **refreshVolumeList** .



- **hiPathSubagents** makes it possible to monitor and handle the status for the following SNMP daemons:
  - systemagt (1)
  - alarmagt (2)
  - erroragt (3)
  - softagt (4)
  - hardagt (5)
  - topoagt (6)
  - sqlagt (7)
  - disagt (8)
  - portagt (9)
  - mib2agt (10)
- **agentIndex** is a unique value for each subagent.
- **agentStatus** is a status of particular subagent. Can be used for stopping/starting subagent. Setting one of the following status ’running’ (1), ’stopped’ (2), ’restart’ (3) is possible by means of SNMP set request.
- **agentPID** is a process ID of the particular subagent.

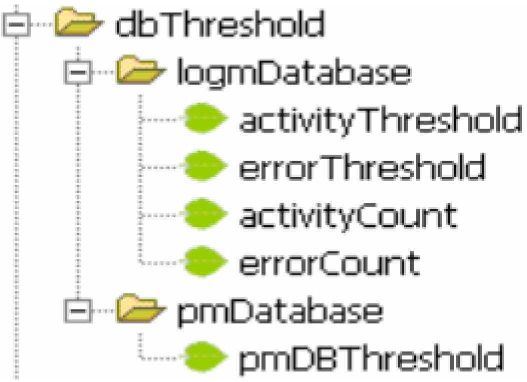
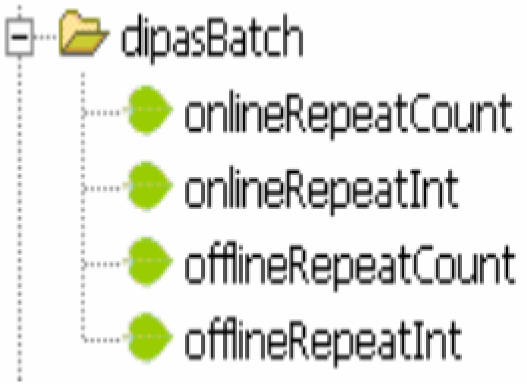
There is any refresh possibility for **agentTable**.

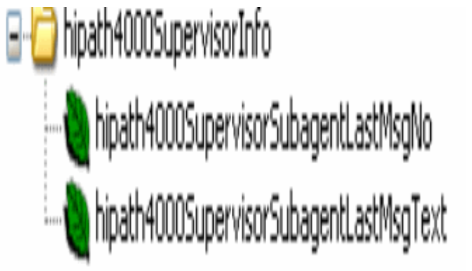
The operations ’start/restart’ may cause a restart or may be caused by a restart of some other proxy agent, because of dependencies between the agents. Following dependences exists:

1) *sqlagent* and portagent work independetly. They can be restarted separately without impact to the other subagents.

2) *softagt , topoagt , hardagt , alarmagt , erroragt , and disagt* depend on the system agent. So they are automatically restarted in case of restart systemagt. In this case the set_request does not wait for restart of all proxy agents, it just initiates the restart and if restart is successfully initiated, it returns as succeed. This is because of system agent needs about one minute for starting process, and then the other subagents are started.

3) The discovery agent (*disagt*) depends on *softagt , topoagt , hardagt , erroragt*. So the disagt is automatically restarted in case of restart one of this agents.

 dbThreshold logmDatabase activityThreshold errorThreshold activityCount errorCount pmDatabase pmDBThreshold	**logmDatabase** - **activityThreshold** is threshold set for the activity table of LogM database. - **errorThreshold** is threshold set for the error table of LogM database. - **activityCount** is number of entries for the activity table of LogM database. - **errorCount** is number of entries for the error table of LogM database. **pmDatabase** - **pmDBThreshold** Threshold set for the error table of LogM database. When a threshold level is reached in the database, the appropriate trap will be sent. **Lmt** shows the table of administration groups managed by LMT. It contains information about the particular administration group. - **adminGroupID** is a unique ID for each admin group. Its values range between 1 and the value for numberOfAdminGroups . The value for each admin group must keep constant at least from one reinitialization of the group entity to the next reinitialization. - **licenseReduction** is license reduction done by LMT in percentage. Reinitialization can be initiated by setting ’1’ for **refreshAdminGroupsList**.
 dipasBatch onlineRepeatCount onlineRepeatInt offlineRepeatCount offlineRepeatInt	- **colBackup** indicates a status of backup AScol component. It can be changed by setting request to value – ’activated’ (1) or – ’deactivated’ (2) **dipasBatch** - **onlineRepeatCount** Repeat count for online batch processing (FAMOS connection). - **onlineRepeatInt** Repeat interval in minutes for online batch processing (FAMOS connection). - **offlineRepeatCount** Repeat count for offline batch processing (file transfer). - **offlineRepeatInt** Repeat interval in minutes for offline batch processing (file transfer).

 hipath4000SupervisorInfo hipath4000SupervisorSubagentLastMsgNo hipath4000SupervisorSubagentLastMsgText	The hiPath Supervisor subagent checks for exceptions, errors and warnings when running. The following options are available: • **hipath4000SupervisorSubagentLastMsgNo** is the last message, warning or error number issued by the Supervisor subagent. • **hipath4000SupervisorSubagentLastMsgText** is the last message, warning or error text issued by the Supervisor subagent.

7.8.2 Enhanced SNMP alarms for Monitoring of the Manager

Together with the enhanced OpenScape Manager agent, additional alarms for monitoring processes on the Manager itself are introduced. These alarms are processed by the *alarmagt*.

So you can see them in alarm/error tables, and you can receive alarm/error traps about the alarms in the defined trap destinations. Then these alarms can be handled in OpenScape FM or another SNMP client.

7.8.2.1 Configure the Manager to Send Alarms

To enable the manager to send these alarm traps, you have to apply the following configuration steps:

1) Configure Communities and trap destinations as described in chapter Section 6.4, "Configuring Communities and Traps".
2) Enable manager alarms monitoring by uncommenting one line in `/opt/ncc/bin/options`:

   Change
   ```
   #MANAGER_TRAP=ON; export MANAGER_TRAP
   ```
   into
   ```
   MANAGER_TRAP=ON; export MANAGER_TRAP
   ```

7.8.2.2 Enhanced Alarms Generated on the Manager

License Management Tool Alarms

LMT_CDW_UPDATE	LMT cannot update codeword for the switch
LMT_LICENSE_REDUCTION	LMT starts license reduction in one of the admin groups
LMT_GLOBAL_ALARM_THRESHOLD	Threshold alarm is set for one of the admin groups
LMT_GLOBAL_ALARM	"Global alarm" is set in LMT
LMT_GLOBAL_WARNING_THRESHOLD	Threshold warning is set for one of the admin groups
LMT_GLOBAL_WARNING	"Global warning" is set in LMT

NOTICE: List of all admin groups and their states can be gathered by SNMP gets on lmt table in the enhanced OpenScape 4000 MIB.

Procadmin Alarms

The process administrator daemon **procadmin** (daemons in the MIB **processTable**) generates alarms in case of any of the daemon observed is in inactive state.

Format of the alarm is PROCM_DAEMONNAME e.g. PROCM_CMPROC_CCS.

NOTICE: List of all observed daemons and their states can be gathered via SNMP gets on **processTable** table in the enhanced OpenScape 4000 MIB.

Database Tables Alarms

LOGM_ACTIVITY_TABLE_THRESHOLD	threshold reached in the activity table of LogM database
LOGM_ERROR_TABLE_THRESHOLD	threshold reached in the error table of LogM database
PM_DATABASE_THRESHOLD	threshold reached in the PM database

NOTICE: Thresholds can be set via SNMP in dbThreshold group of the enhanced OpenScape 4000 MIB.

OpenScape 4000 Manager backup alarms

HBR_DATA_BACKUP	data backup failed

In case of logical backup fails the alarms have the format HBR_LOGICAL_BACKUPUNIT e.g. HBR_LOGICAL_CDB

FM_COMMANDFILE_SEND

AMO job cannot be sent to the switch.

SSO_REPLICATION

Smart switch over replication was not successful.

SWA_ACTIVATION_FAILED

Activation of the Major/Minor/FixRelease or Hotfix failed.

CM_DB_SYNCH

Database synchronization with the switch was not successful.

PM_REPORT

Performance management time controlled report was not successful.

Collection agent alarms

COL_FETCH	reception (fetch) from the switch not successful
COL_RECEIVE	conversion (transform) in received file not successful
COL_OUTPUT_FILE_PROD	production of the output file not successful
COL_PARTITION_FILLED	fetching deactivated because of full COL-Backup directory

License Management alarms

LICM_LICENSE_EXCEEDED	OpenScape 4000 license has exceeded.

License Management generates alarms based on the state of port counters and theirs thresholds. The following alarms can be generated:

- LICM_PORTCOUNT_EXCEEDED
- LICM_OS4K_PORTCOUNT_WARN_REACHED

DISK_SATURATION_THRESHOLD

Threshold on one of the monitored partitions is reached.

NOTICE: Partition thresholds can be set via SNMP in fileSysTable of the new OpenScape 4000 MIB.

8 SNMP Features/Extensions

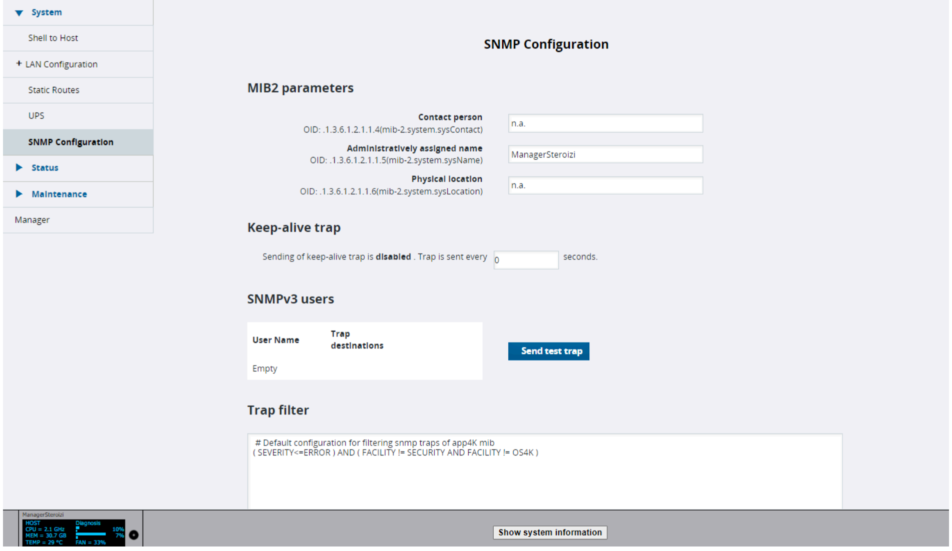
This chapter describes requirements and the architecture of the OpenScape 4000 Manager and Assistant V10R1 – SNMP features.

8.1 Improved Alarm and Error Handling in 4K

With this feature user will be able to do following:

1) Configure SNMPv3 parameters for all hosts from Assistant
2) Review SNMPv3 setup on the host portal
3) Configure hostMIB trap filter for all hosts from Assistant
4) Review hostMIB trap filter setup on the host portal
5) Stop sending error traps from host portal
6) Configure keep-alive traps interval for all hosts and stop sending of all SNMP trap messages from all hosts and RMX in Assistant GUI
7) Review keep-alive trap on host portal
8) Send test trap from host portal
9) Save configuration of SNMPv3 parameters, keep-alive trap, trap filter on all hosts by one click from Assistant/Manager.
10) Reset All alarms raised on RMX by one click from Assistant/Manager.
11) Download Host 4000 MIB from Assistant/Manager
12) Setup MIB2 parameters for each host from Assistant
13) Backup/Restore of SNMP setting on each host
14) Use Host 4000 MIB on NMS for understanding error messages
15) Use MIB-2 for hardware monitoring
16) Use hicom MIB (not HIM) for getting list of hosts/IP addresses in 4K area
17) Use MIB2 for getting contact/name/location information from host
18) Use OpenScapeFM with 4K Host 4000 MIB and new hicom MIB

8.1.1 Host Portal SNMP Overview



SNMP Configuration

MIB2 parameters

Contact person
OID: .1.3.6.1.2.1.1.4(mib-2.system.sysContact): n.a.

Administratively assigned name
OID: .1.3.6.1.2.1.1.5(mib-2.system.sysName): ManagerSteroizi

Physical location
OID: .1.3.6.1.2.1.1.6(mib-2.system.sysLocation): n.a.

Keep-alive trap

Sending of keep-alive trap is **disabled** . Trap is sent every 0 seconds.

SNMPv3 users

User Name	Trap destinations
Empty	

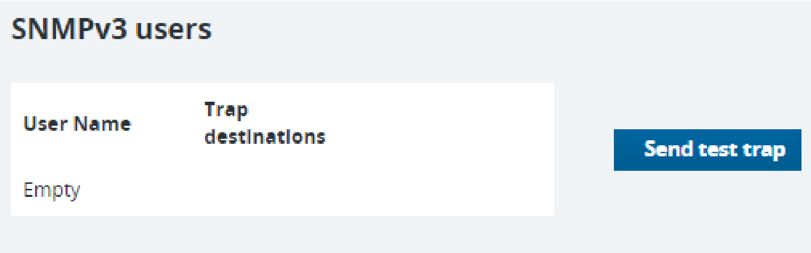
Trap filter

```
# Default configuration for filtering snmp traps of app4K mib
( SEVERITY<=ERROR ) AND ( FACILITY != SECURITY AND FACILITY != OS4K )
```

Figure 93: Host Portal SNMP

8.1.1.1 SNMPv3 Users

The SNMPv3 users and their trap destinations configured on the host can be seen in the SNMP configuration view of the host portal. These users can be used to access the MIBs supported on the host (hostMIB, MIB2, ...). The trap destinations are IP addresses where the SNMP notification messages from the host will be sent to.



SNMPv3 users

User Name	Trap destinations
Empty	

Figure 94: SNMP Users & Trap Destinations Example

The configuration of these parameters including the passwords used for authorization and authentication can be made centrally from Assistant. Such SNMPv3 users are created on all hosts with read-only access to the MIB2.

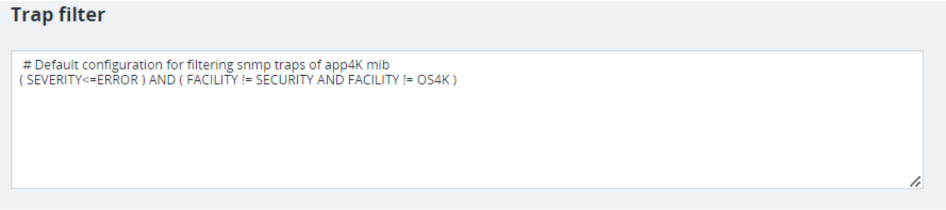
The SNMP engine on the hosts is configured to send SNMPv3 encrypted, unacknowledged traps. Therefore, the engineID is not needed for receiving traps from 4K hosts.

You can request the sending of a test trap to defined destinations by clicking on the "Test trap" button. Test traps (.1.3.6.1.4.1.32804.1.9.1.10.13.0.1 - hostTestDebugEv) will be sent to all defined trap destinations encrypted by the appropriate user-key.

You can switch on/off the sending of SNMP traps from the host or centrally on all hosts from the Assistant.

8.1.1.2 Trap Filter

You can display the filter used by the SNMP engine on the host and then decide which events should not be send as SNMP traps to predefined trap destinations. This filter can be specified using the Assistant GUI.



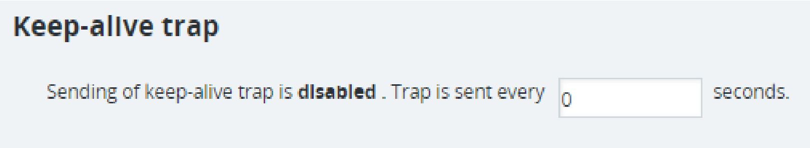
Trap filter

```
# Default configuration for filtering snmp traps of app4K mib
( SEVERITY<=ERROR ) AND ( FACILITY != SECURITY AND FACILITY != OS4K )
```

Figure 95: Trap Filter Example

8.1.1.3 Keep-Alive Trap

Some of the NMS are using so called keep-alive traps to monitor whether the system is up and running. A keep-alive trap is just some info message; if it is not received by the NMS whithin the specified time interval, NMS reports a critical error on the monitored node.



Keep-alive trap

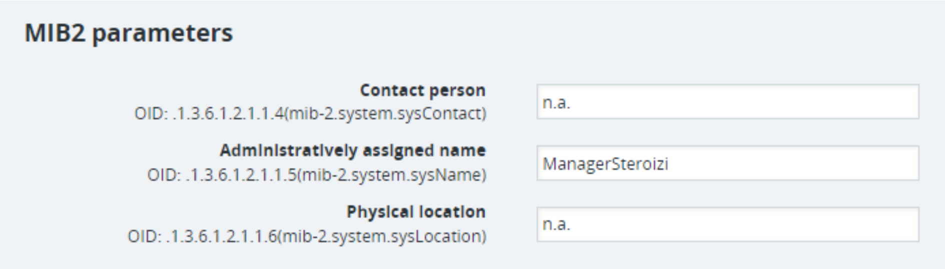
Sending of keep-alive trap is **disabled** . Trap is sent every 0 seconds.

Figure 96: Keep-Alive Trap Filter Example

By default the keep-alive traps are deactivated (empty or 0). The time intervals for sending keep-alive traps can be configured centrally from the Assistant so that traps (.1.3.6.1.4.1.32804.1.9.1.10.13.0.2 - hostKeepAliveInfoEv) are sent every X seconds.

8.1.1.4 MIB2 Parameters

Each host will provide information about the mib-2 module via SNMP. The MIB2 allows users to set up 3 parameters from the system part. These parameters will later be used by NMS to detect the system information required for service:



MIB2 parameters

Contact person
OID: .1.3.6.1.2.1.1.4(mib-2.system.sysContact): n.a.

Administratively assigned name
OID: .1.3.6.1.2.1.1.5(mib-2.system.sysName): ManagerSteroizi

Physical location
OID: .1.3.6.1.2.1.1.6(mib-2.system.sysLocation): n.a.

Figure 97: MIB2 Parameters Example

- sysContact
  - The textual identification of the contact person for this managed node, together with information on how to contact this person.
- sysName
  - An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.
- sysLocation
  - The physical location of this node.

  These MIB2 parameters can be setup after the installation of the node:
- For OpenScape 4000 host systems (node A, node B, Qorum node) these parameters can be set via the Assistant System Management.
- For Softgate-based APs and Softgate-based AP-E, the sysLocation values are distributed automatically based on the information specified in the RMX database (AMOs UCSU).
- For IPDA based AP-E systems, these values can be set via the Assistant System Management on AP-E.

The MIB2 standard also allows to change these values via SNMP set requests. However, in order to maintain a consistent setup between the RMX, the Assistant database and the MIB2, this case is not supported; writing these values via SNMP is not possible.

The sysName and sysLocation values are part of each SNMP trap generated by the host system.

MIB2 sysDescr

The system description value from MIB2 (OID .1.3.6.1.2.1.1.1) on the host includes the exact identification of the system. This value can be used by SNMP NMS to get a better understanding of the purpose of the host system and its hardware platform; it can also be used to join it with the subsystems (hosting software) in the topology view (HPA500 Board Recognition).

This value can be read by a SNMP get request from the user. Its value is part of each SNMP trap generated by the host system.

The value of sysDescr is automatically set during the installation and changed based on the configuration of the host,hosting applications and SW update actions.

The syntax for the host base systems (nodeA,nodeB,nodeQ) is as follows:

```
Hardware Type;Deployment Type;Business Name;Version
```

(e.g.: VM; Simplex; OpenScape 4000; V7_R2.10.0)

The syntax for AP-based host systems is as follows:

```
Hardware Type;Deployment Type (LTU:ltu_number);Business
 Name;Version
```

(e.g.: VM; Standalone SoftGate (LTU:21); OpenScape 4000 SoftGate; V7_R2.10.0)

List of values:

- Hardware Type – type of the hardware where the system is installed, it can be:
  - VM
  - OSA500i
  - OSA500a
  - DSCXL
  - ecoserver
  - Standard PC
- Deployment Type
  - Host NodeA
  - Host NodeB
  - Quorum Node
  - Softgate
  - Survivable Softgate
  - AP Emergency
- Business Name
  - OpenScape4000
  - OpensScape4000 Softgate
  - ......
- Version – SWRM syntax based version of the host system (Vmajor_minor.fixReleae.hotFix e.g. V7_R2.40.1)

The possible values of the sysDescr have to be documented in the SNMP service manual.

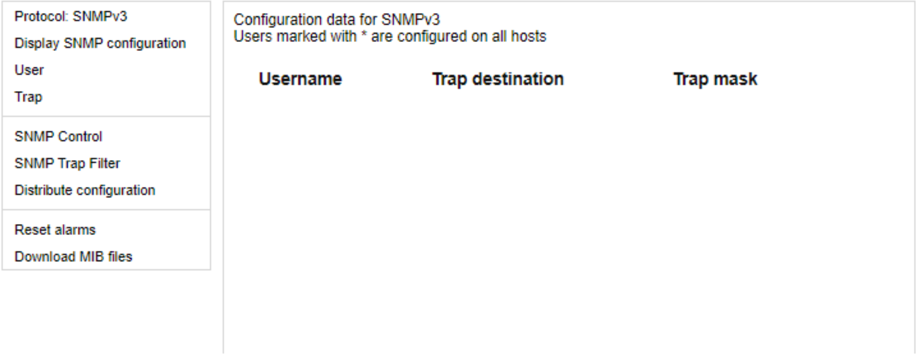
8.1.2 Assistant GUI SNMP

From the Assistant SNMP configurator, you can:

- Configure host SNMPv3 parameters
- Create Trap filter and distribute it into all hosts
- Activate/Deactivate host keep-alive traps on all hosts
- Setup MIB2 parameters
- Download host MIB file

8.1.2.1 Trap Filters

You can use the GUI in the SNMP Configurator -> Trap Filter -> Host System Events for the definition of the trap filter for host systems.



Configuration data for SNMPv3
Users marked with * are configured on all hosts

Username	Trap destination	Trap mask

Figure 98: Host System Events Example

In the Trap Filter GUI, you can define rules for filtering traps on the host systems. The definition is written in a multiline text area using expressions that must have the correct syntax. The syntax is verified so you cannot save a filter with syntax errors.

This configuration can contain:

- Comments – all texts from character # to the end of line. A comment can start at the beginning of a line or in the middle.
- Conditions on separate lines

Using these conditions you can specify what has to be filtered out (which traps should not be sent by the host systems). So each trap meeting the condition set from this file is filtered out.

Conditions can contain:

- keywords: SEVERITY, FACILITY, OID, MSG, TRAP_ID
- operators {=, !=, <, >, <=, >=} for SEVERITY
- operators {=, !=} for FACILITY, OID, TRAP_ID
- operators {MATCH, NOT MATCH} for MSG
- logical operators AND, OR
- brackets, can be nested ((... OR ...) AND ...)

Keyword options:

- valid SEVERITY values are: {emergency, alert, critical, error, warning, notice, info, debug}
- valid FACILITY values are: {os4k, kernel, user, mail, daemon, security, syslog}, where os4k are traps generated by os4k processes.
- valid OID values are strings inside the "" which can contain a * character at the end. This character stands for an arbitrary count of any characters.
- valid MSG values are strings inside the "" which can contain special characters for regular expressions. Here the regex syntax is supported.
- valid TRAP_ID values are strings inside the "" marks. Special characters (wildcards) are not supported. The TRAP_ID value is compared with predefined values and must match one of them. If it does not match any, a predefined TRAP ID error is logged in the parsing file.

> **NOTICE:** The difference between the wildcards in OID and MSG is that in an OID string you use the character *; for the same meaning in an MSG string you must use .* because . stands for an arbitrary character and * for its repetition.

Other rules:

- All keywords, logical operators and facility and severity values are case insensitive.
- Strings in quotation marks are case sensitive.
- Priority of AND, OR is the same, so use brackets if you need to determine priority.
- Brackets can be nested several times, e.g. ((...)...(...)...(...(...)...)).
- Logical operation between lines is OR.

Correct examples of configuration file:

(SEVERITY < Error) AND (FACILITY = OS4K)

SEVERITY < INFO

FACILITY = MAIL OR FACILITY = SYSLOG

OID = "154.121.45.74.1.1.2.3.*"

MSG MATCH "Message 123.*"

MSG NOT MATCH ".*temperature.*"

TRAP_ID = "tooHighTemperatureOfBoard" # trap with given ID must exist of course

Incorrect usage (each line contains some error):

# undefined operation <> and undefined binary minus

(SEVERITY <> ERROR OR FACILITY - USER)

# for FACILITY only operators = and != are allowed

(FACILITY > USER)

# compare operator cannot be used twice for one severity / facility

(ALERT > SEVERITY > NOTICE)

# wrong order, first the keyword SEVERITY must be used and it is compared to its value,

# correct is (SEVERITY > NOTICE)

(NOTICE < SEVERITY)

# unsupported operation for OID

OID > "127.5.5.4.1"

# character * cannot be inside of string. Must be at the end.

OID = "154.2.1.54.7.8.4.*.1.2.1"

# missing quotation marks.

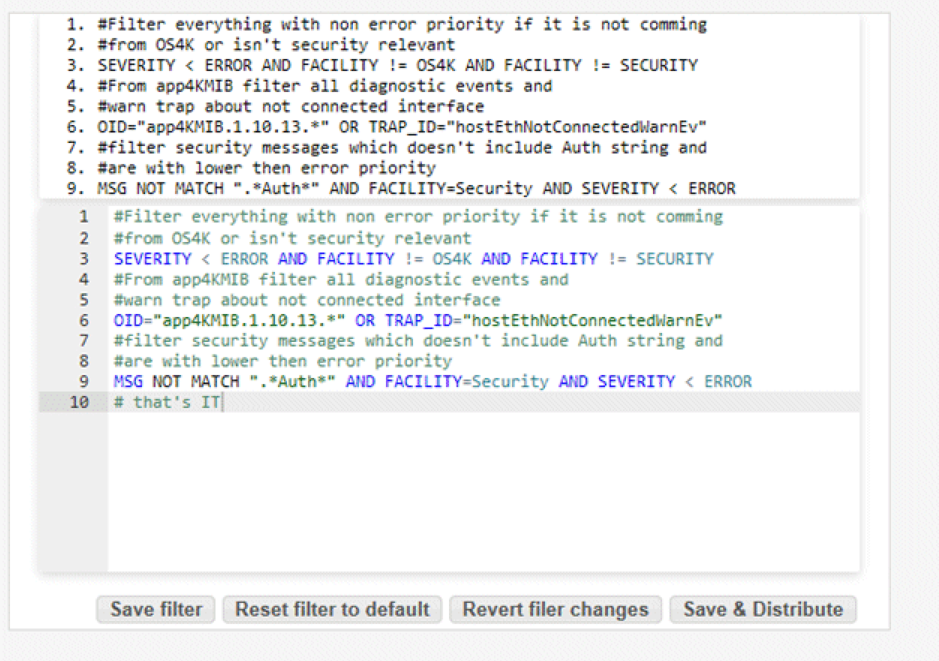
MSG MATCH 1234:

# character * cannot be interpreted as wild card.

# You cannot expect wildcard behaviour for TRAP_ID.

TRAP_ID = "highTemperature*"

When the GUI of the Trap Filter is opened, the last saved filter is displayed on top.



```
#Filter everything with non error priority if it is not comming
#from OS4K or isn't security relevant
SEVERITY < ERROR AND FACILITY != OS4K AND FACILITY != SECURITY
#From app4KMIB filter all diagnostic events and
#warn trap about not connected interface
OID="app4KMIB.1.10.13.*" OR TRAP_ID="hostEthNotConnectedWarnEv"
#filter security messages which doesn't include Auth string and
#are with lower then error priority
MSG NOT MATCH ".*Auth*" AND FACILITY=Security AND SEVERITY < ERROR
```

```
#Filter everything with non error priority if it is not comming
#from OS4K or isn't security relevant
SEVERITY < ERROR AND FACILITY != OS4K AND FACILITY != SECURITY
#From app4KMIB filter all diagnostic events and
#warn trap about not connected interface
OID="app4KMIB.1.10.13.*" OR TRAP_ID="hostEthNotConnectedWarnEv"
#filter security messages which doesn't include Auth string and
#are with lower then error priority
MSG NOT MATCH ".*Auth*" AND FACILITY=Security AND SEVERITY < ERROR
# that's IT
```

Figure 99: Host System Events - Last Saved Filter Example

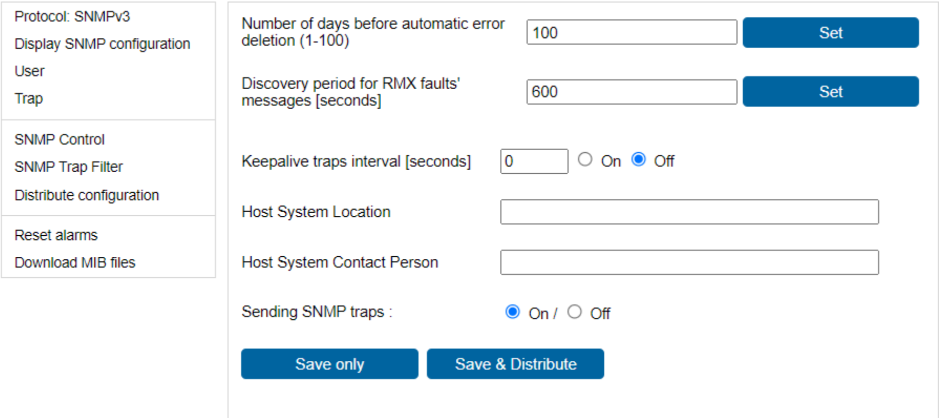
Action buttons description:

- Save filter – The filter is stored and text from the editable area is copied to the top.
- Reset filter to default – You can reset the filter to the default configuration predefined during the OS4k installation.
- Revert file changes – The last saved configuration is restored.
- Save & Distribute - The filter is stored and you are redirected to the Distribute Configuration page where you can distribute it into all hosts in the 4K area.

Before the distribution starts, you can specify which data should be distributed (Distribution to hosts).

8.1.2.2 SNMP Control Parameters

In the SNMP Control GUI you can activate the sending of keep-alive traps from all hosts, activate/deactivate the sending of error traps from the entire 4K area, and setup the location and contact person for hosts of the active/standby/quorum nodes. The contact and location will be used for the MIB2 sysLocation and sysContact settings.



Number of days before automatic error deletion (1-100) 100

Discovery period for RMX faults' messages [seconds] 600

Keepalive traps interval [seconds] 0 ○ On ● Off

Host System Location

Host System Contact Person

Sending SNMP traps : ● On / ○ Off

Figure 100: SNMP Configurator Save Example

- You can specify how often the trap should be generated.
- You can use the radio button to deactivate the SNMP trap sending from the host.
- You can define the physical location of the host system.
- You can define a service contact person for the host system.

Action buttons description:

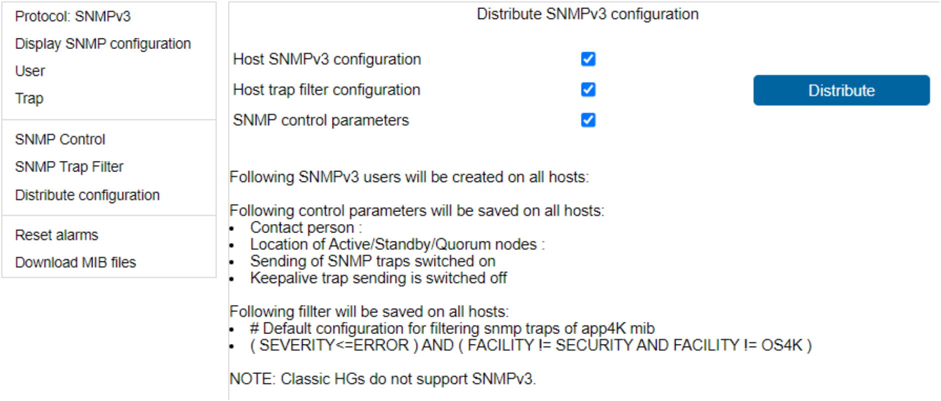
- Save only - Saves keep-alive,location,contact person and sending of traps information in the Assistant database.
- Save & Distribute - Saves keep-alive,location,contact person and sending of traps information in the Assistant database; you are redirected to the Distribute Configuration page where you can distribute the information to all hosts in the 4K area.

8.1.2.3 Distribution to Hosts

You can use the SNMP configurator -> Distribute Configuration GUI for saving configuration changes to the hosts system.

The following configuration changes can be saved to connected hosts:

- SNMPv3 setting
- Host filter setting
- SNMP control settings



Protocol: SNMPv3
Display SNMP configuration
User
Trap
SNMP Control
SNMP Trap Filter
Distribute configuration
Reset alarms
Download MIB files

Distribute SNMPv3 configuration

Host SNMPv3 configuration ☑
Host trap filter configuration ☑
SNMP control parameters ☑

Distribute

Following SNMPv3 users will be created on all hosts:

Following control parameters will be saved on all hosts:
- Contact person :
- Location of Active/Standby/Quorum nodes :
- Sending of SNMP traps switched on
- Keepalive trap sending is switched off

Following fillter will be saved on all hosts:
- # Default configuration for filtering snmp traps of app4K mib
- (SEVERITY<=ERROR) AND (FACILITY != SECURITY AND FACILITY != OS4K)

NOTE: Classic HGs do not support SNMPv3.

Figure 101: SNMP Configurator Distribute Example

Before the distribution starts, you can also select which configuration should be distributed to the connected hosts.

Clicking on the Distribute button will start the distribution process; this may take several seconds. During the distribution, all data selected are configured and saved on all nodes in the 4K area (except on IPDA-based APE systems).

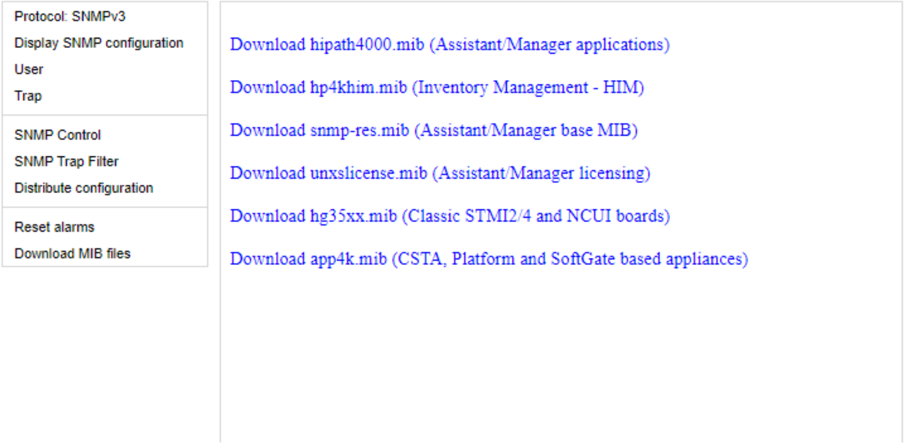
NOTICE: It is mandatory to have the NGS IP address setup on for the distribution to AP, APEs.

8.1.2.4 Reset All Alarms Raised on RMX or Assistant

You can use the SNMP Configurator -> Reset Alarms option from the menu on the left to reset all alarms (set to off status) raised on the RMX or Assistant.

8.1.2.5 Download MIB file

You can download a new Host 4000 MIB file together with all MIB files supported by the systems in the 4000 area from the SNMP Configurator -> Download MIB files:



Protocol: SNMPv3
Display SNMP configuration
User
Trap
SNMP Control
SNMP Trap Filter
Distribute configuration
Reset alarms
Download MIB files

Download hipath4000.mib (Assistant/Manager applications)

Download hp4khim.mib (Inventory Management - HIM)

Download snmp-res.mib (Assistant/Manager base MIB)

Download unxslicense.mib (Assistant/Manager licensing)

Download hg35xx.mib (Classic STMI2/4 and NCUI boards)

Download app4k.mib (CSTA, Platform and SoftGate based appliances)

Figure 102: SNMP Configurator Download Example

8.1.3 Host 4000 MIB

The new Host 4000 MIB (ASN-1 syntax notation) is structured like this:

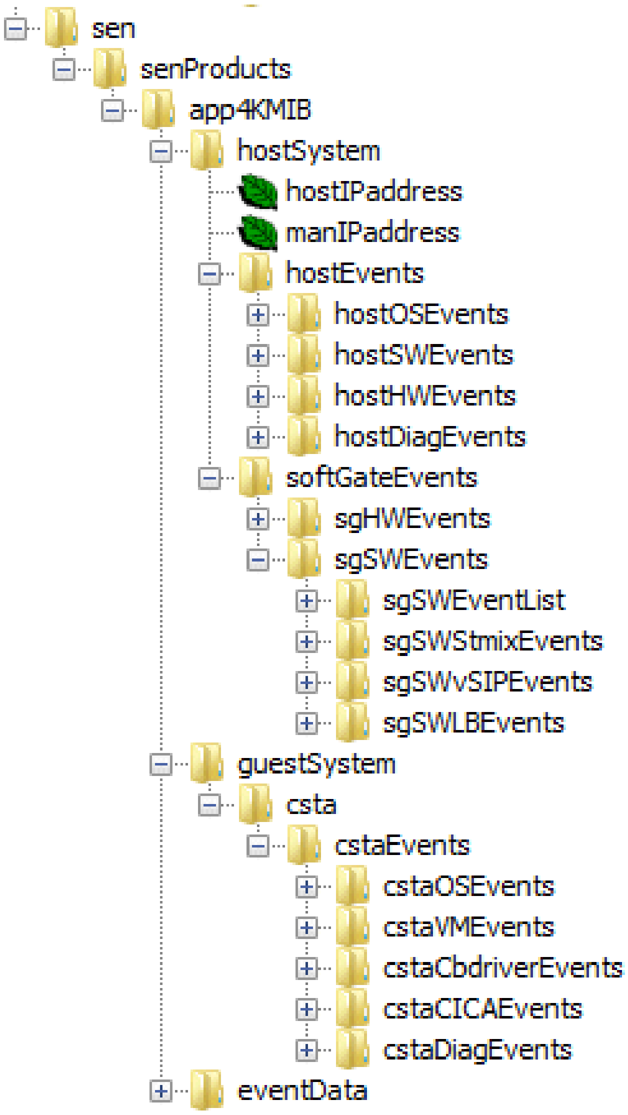


Figure 103: Host 4000 MIB Structure

hostSystem - Host system of OpenScape 4000 appliance

- hostEvents - Group of events produced by applications and monitoring processes running on appliance of OpenScape 4000 host system
  - hostOSEvents - Events which can be produced by Operating System of OpenScape 4000 host system
  - hostSWEvents - Events from host sofware applications and deamons
  - hostHWEvents - Hardware events reported by the host system
  - hostDiagEvents - Events used for diagnostic purposes

- softGateEvents - Group of events produced by softgate system and softgate relevant hardware
    - sgHWEvents - Hardware events produced by Softgate system running on host.
    - sgSWEvents - Software events produced by SoftGate system running on host.

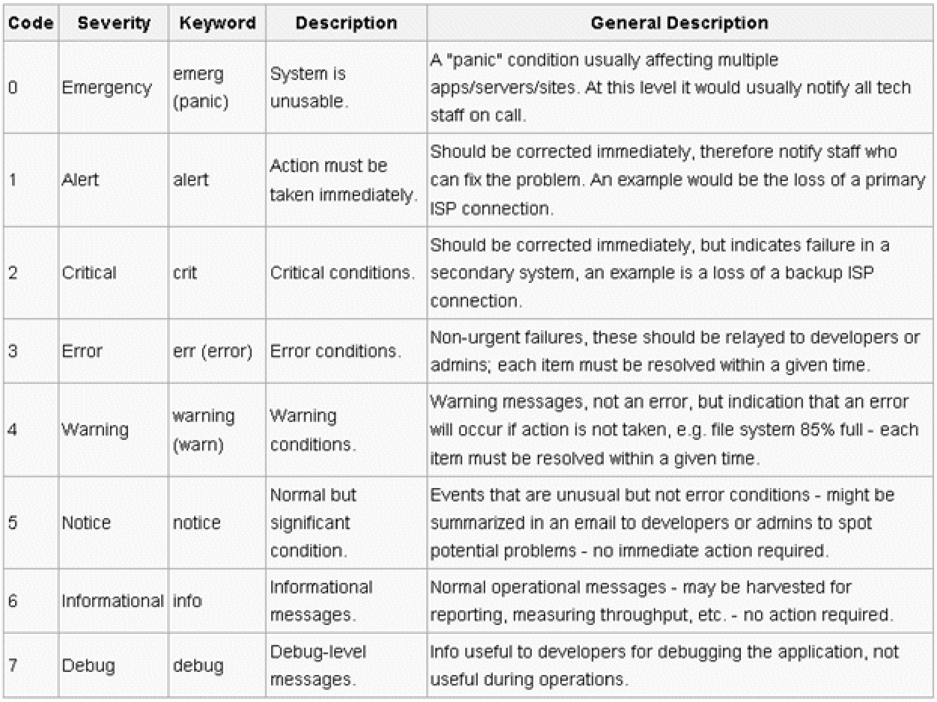
guestSystem - Operating system or application hosted on OpenScape 4000 host appliance

- csta - CSTA guest system running on OpenScape4000 appliance
    - cstaEvents - Events produced by CSTA
        - cstaOSEvents - Events from Operating System of CSTA
        - cstaVMEvents - Events related to VM of CSTA
        - cstaCbdriverEvents - Events related to CSTA cbdriver software
        - cstaCICAEvents - CICA related events
        - cstaDiagEvents - CSTA diagnostic events

        Additionally each event/trap includes the following data as variable bindings:
- evSeverity - severity (priority) level
- sysDescr – system description from host's MIB2
- sysName – system name from host's MIB2
- sysLocation – system location from host's MIB2
- hostIPaddress – IP address of the host which is generating the trap
- manIPaddress – clan IP address of HiPath4000 Assistant which is used for administration/management of SNMP setting
- eventDateTime – date and time when the event occurred
- evDescr - detailed text of the event message

8.1.3.1 SeverityLlevel (evSeverity)

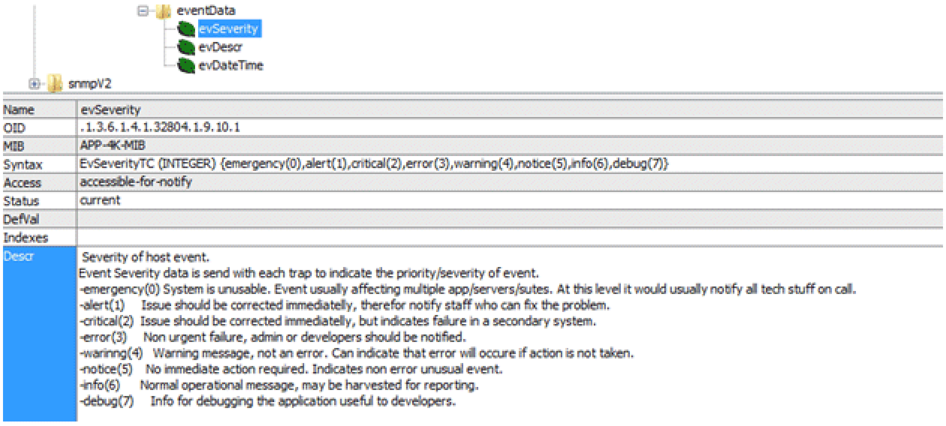
The host 4000 MIB includes severities from syslog-ng (RFC 5424).



Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	Alert	alert	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	Critical	crit	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	Error	err (error)	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	Warning	warning (warn)	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	Notice	notice	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	Informational	info	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	Debug	debug	Debug-level messages.	Info useful to developers for debugging the application, not useful during operations.

Figure 104: Host 4000 MIB Structure - Severity Level (1)

Host 4000 MIB Structure - Severity Level (2)



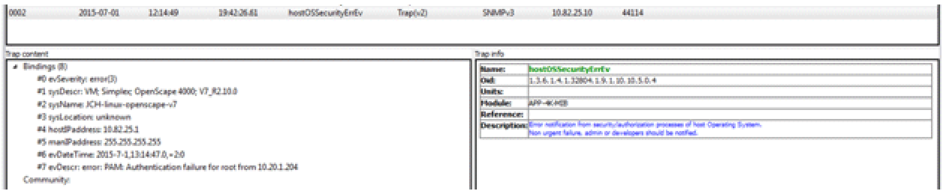
Name	evSeverity
OID	.1.3.6.1.4.1.32804.1.9.10.1
MIB	APP-4K-MIB
Syntax	EvSeverityTC (INTEGER) {emergency(0),alert(1),critical(2),error(3),warning(4),notice(5),info(6),debug(7)}
Access	accessible-for-notify
Status	current
DefVal	
Indexes	
Descr	Severity of host event. Event Severity data is send with each trap to indicate the priority/severity of event. -emergency(0) System is unusable. Event usually affecting multiple app/servers/sutes. At this level it would usually notify all tech stuff on call. -alert(1) Issue should be corrected immediatelly, therefor notify staff who can fix the problem. -critical(2) Issue should be corrected immediatelly, but indicates failure in a secondary system. -error(3) Non urgent failure, admin or developers should be notified. -warinng(4) Warning message, not an error. Can indicate that error will occure if action is not taken. -notice(5) No immediate action required. Indicates non error unusual event. -info(6) Normal operational message, may be harvested for reporting. -debug(7) Info for debugging the application useful to developers.

Figure 105: Host 4000 MIB Structure - Severity Level (2)

8.1.3.2 hostOSEvents

The hostOSEvents trap uses a generic trap model, i.e. it is not obvious from the trap name what kind of error occurred. Each trap includes an evDescr as a trap variable binding which has to be used to find the reason for the error. Only the trap severity (priority) and facility (which OS subsytem produced the trap) can be found based on the trap name.

E.g. here is log from a trap receiver that caught a hostOSSecurityErrEv trap - it is obvious that this is error was produced by the security subSystem of the operating system; however to find out the exact reason you have to check the evDecr variable binding:



```
0002    2015-07-01    12:14:49    19:42:26.61    hostOSSecurityErrEv    Trap(v2)    SNMPv3    10.82.25.10    44114
```

Trap content

```
◢ Bindings (8)
    #0 evSeverity: error(3)
    #1 sysDescr: VM; Simplex; OpenScape 4000; V7_R2.10.0
    #2 sysName: JCH-linux-openscape-v7
    #3 sysLocation: unknown
    #4 hostIPaddress: 10.82.25.1
    #5 manIPaddress: 255.255.255.255
    #6 evDateTime: 2015-7-1,13:14:47.0,+2:0
    #7 evDescr: error: PAM: Authentication failure for root from 10.20.1.204
  Community:
```

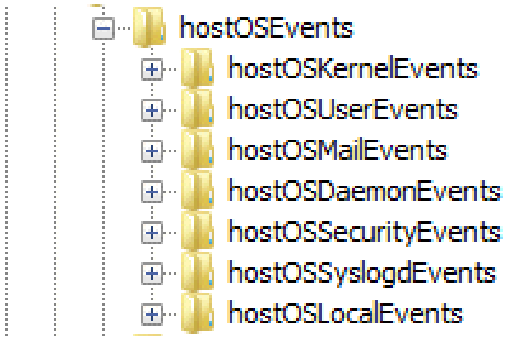
Trap info

Name:	hostOSSecurityErrEv
Oid:	1.3.6.1.4.1.32804.1.9.1.10.10.5.0.4
Units:	
Module:	APP-4K-MIB
Reference:	
Description:	Error notification from security/authorization processes of host Operating System. Non urgent failure, admin or developers should be notified.

Figure 106: hostOSEvents - Log

The SNMP engine is preset to send traps messages from the operating system with severity errors up-to emerg only. The messages with lower priority are not sent as snmp traps.

The hostOSEvents includes the following categories of traps:



```
⊟ hostOSEvents
    ⊞ hostOSKernelEvents
    ⊞ hostOSUserEvents
    ⊞ hostOSMailEvents
    ⊞ hostOSDaemonEvents
    ⊞ hostOSSecurityEvents
    ⊞ hostOSSyslogdEvents
    ⊞ hostOSLocalEvents
```

Figure 107: hostOSEvents Categories

- hostOSKernelEvents - Host operating system kernel messages
- hostOSUserEvents - Host operating system application/service messages
- hostOSMailEvents - Host operating system mail system messages
- hostOSDaemonEvents - Messages from system daemons Host operating system
- hostOSSecurityEvents - Host operating system security/authorization messages
- hostOSSyslogdEvents - Messages generated internally by syslogd of the host operating system
- hostOSLocalEvents - Messages generated by an administrator or applications from the host operating system

8.1.3.3 hostSWEvents

Software-based events which can be produced by OpenScape4000 processes/ monitoring applications running on host:

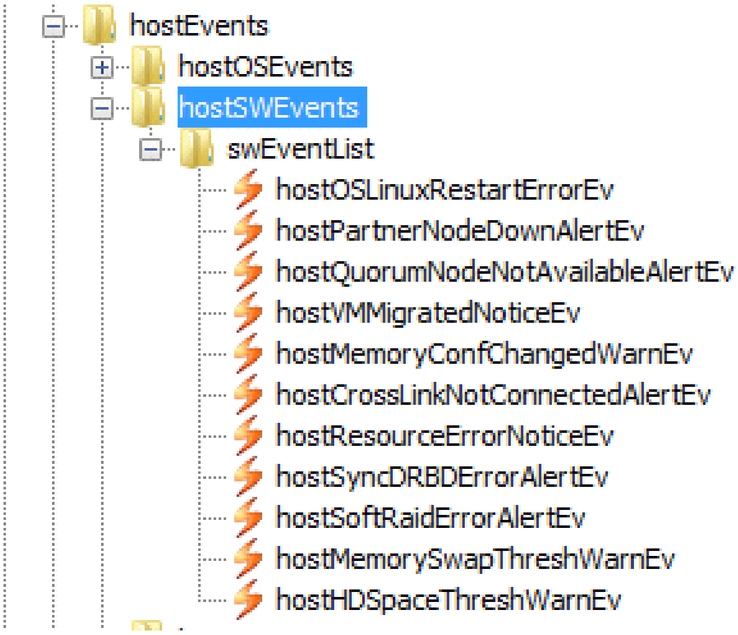

hostEvents
hostOSEvents
hostSWEvents
swEventList
hostOSLinuxRestartErrorEv
hostPartnerNodeDownAlertEv
hostQuorumNodeNotAvailableAlertEv
hostVMMigratedNoticeEv
hostMemoryConfChangedWarnEv
hostCrossLinkNotConnectedAlertEv
hostResourceErrorNoticeEv
hostSyncDRBDErrorAlertEv
hostSoftRaidErrorAlertEv
hostMemorySwapThreshWarnEv
hostHDSpaceThreshWarnEv

Figure 108: hostSWEvents

- hostOSLinuxRestrtErrorEv - Host operating system restart.
- hostPartnerNodeDownAlertEv - Duplex System: one node is out of service
- hostQuorumNodeNotAvailableAlertEv - Separate Duplex System: Quorum node is not available
- hostVMMigratedNoticeEv - VM was migrated via vMotion to an other physical Server
- hostMemoryConfChangedWarnEv - Memory configuration of VM was changed
- hostCrossLinkNotConnectedAlertEv - Cross-Link not connected. Check connector and duplex systems.
- hostResourceErrorNoticeEv - Error of system application, info only - check functionality of the resource
- hostSyncDRBDErrorAlertEv - DRBD Error, check duplex functionality
- hostSoftRaidErrorAlertEv - SoftRaid Error, check recovery HD generation
- hostMemorySwapThreshWarnEv - System is swapping - check RAM usage
- hostHDSpaceThreshWarnEv - Hard Drive Space - value is over threshold

8.1.3.4 hostHWEvents

Hardware-based events which can be produced by OpenScape4000 processes/ monitoring applications running on host:

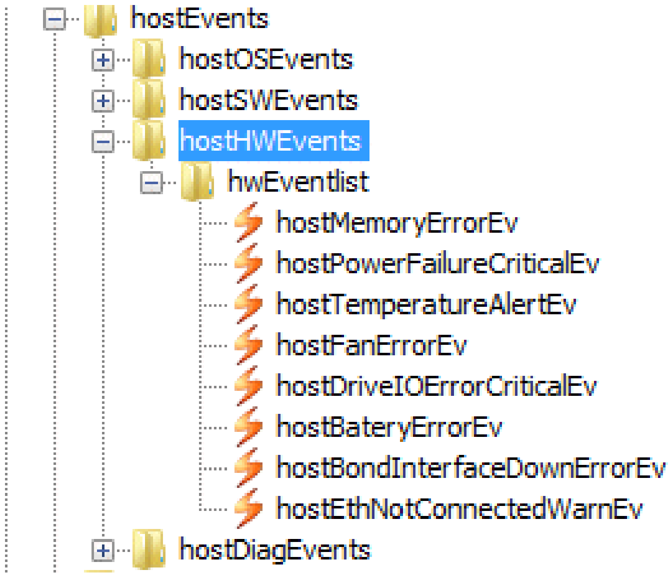


Figure 109: hostHWEvents

- hostMemoryErrorEv - Memory error, replacement of memory needed
- hostPowerFailureCriticalEv - Power failure AC/DC, replacement of PSU is needed
- hostTemperatureAlertEv - CPU temperature is over threshold
- hostFanErrorEv - FAN error - FAN needs to be replaced
- hostDriveIOErrorCriticalEv - Drive I/O Error - check HD/SSD
- hostBateryErrorEv - Replacement of BIOS battery is needed
- hostBondInterfaceDownErrorEv - Bond Interfaces:redundant interface down, check connectivity
- hostEthNotConnectedWarnEv - Ethernet Interface configured but not connected

8.1.3.5 hostDiagEvents

The SNMP traps used as diagnostic traps. This part only comprises 2 traps:

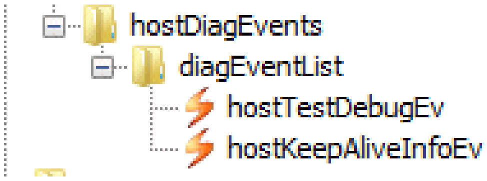
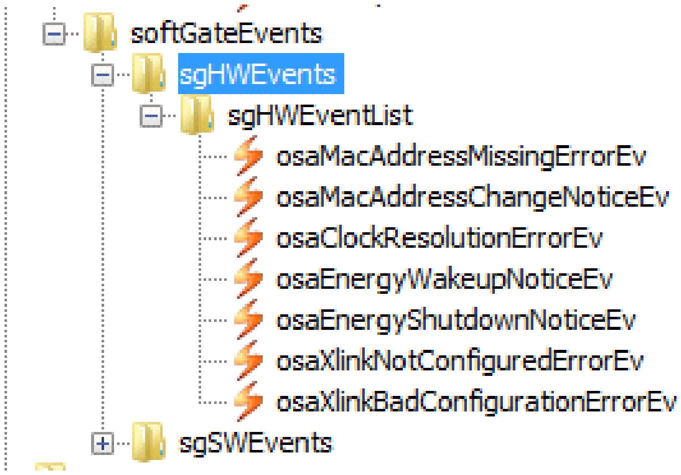


Figure 110: hostDiagEvents

- hostKeepAliveInfoEv– the periodically generated trap based on the keep-alive interval setup. If this is received by the NMS, it means the system is up and running.
- hostTestDebugEv– trap generated when the user clicks on the Test button in the SNMP configuration of the portal. It is only used for testing whether the SNMP engine is working and sending traps to predefined trap destinations.

8.1.3.6 sgHWEvents

The hardware-based events produced by the Softgate system running on the host operating system:



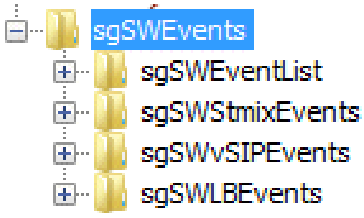
softGateEvents
sgHWEvents
sgHWEventList
osaMacAddressMissingErrorEv
osaMacAddressChangeNoticeEv
osaClockResolutionErrorEv
osaEnergyWakeupNoticeEv
osaEnergyShutdownNoticeEv
osaXlinkNotConfiguredErrorEv
osaXlinkBadConfigurationErrorEv
sgSWEvents

Figure 111: sgHWEvents

- osaMacAddressMissingErrorEv - Configuration Problem OSA module - MAC address missing
- osaMacAddressChangeNoticeEv - Configuration Problem OSA module - MAC address change
- osaClockResolutionErrorEv - Clock resolution too bad for OSA usage
- osaEnergyWakeupNoticeEv - Energy saving is active: start-up after wakeup
- osaEnergyShutdownNoticeEv - Energy saving is active: shutdown started
- osaXlinkNotConfiguredErrorEv - Xlink Lan-Interface is not configured
- osaXlinkBadConfigurationErrorEv - Xlink Interface is the same as the IPDA Interface e.g. xlink Lan-Interface is not configured or bad IP address

8.1.3.7 sgSWEvents

Software-based events produced by the SoftGate system running on the host. They are split into 4 categories:



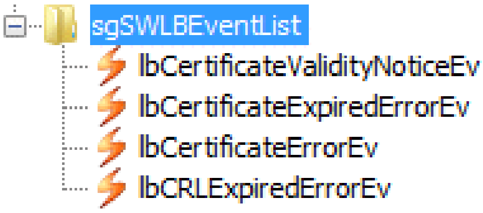
sgSWEvents
sgSWEventList
sgSWStmixEvents
sgSWvSIPEvents
sgSWLBEvents

Figure 112: sgSWEvents

- sgSWLBEvents - OpenSIPS Load Balancer events
- sgSWvSIPEvents - vHG3500 (SIP) events
- sgSWStmixEvents - STMIX events
- sgSWEventList - the rest of software events produced by Softgate system

sgSWLBEvents

OpenSIPS Load Balancer events:



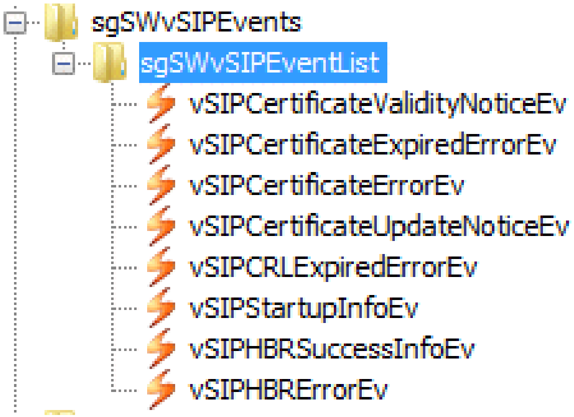
sgSWLBEventList
lbCertificateValidityNoticeEv
lbCertificateExpiredErrorEv
lbCertificateErrorEv
lbCRLExpiredErrorEv

Figure 113: sgSWLBEvents

- lbCertificateValidityNoticeEv - OpenSIPS Load Balancer security active and SPE Certificate ends
- lbCertificateExpiredErrorEv - OpenSIPS Load Balancer security active and SPE Certificate expired
- lbCertificateErrorEv - OpenSIPS Load Balancer security active and there are problems with SPE Certificate
- lbCRLExpiredErrorEv - OpenSIPS Load Balancer security active and CRL (certificate revocation list) expired

sgSWvSIPEvents

vHG3500 (SIP) events:



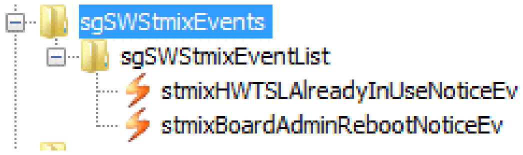
sgSWvSIPEvents
sgSWvSIPEventList
vSIPCertificateValidityNoticeEv
vSIPCertificateExpiredErrorEv
vSIPCertificateErrorEv
vSIPCertificateUpdateNoticeEv
vSIPCRLExpiredErrorEv
vSIPStartupInfoEv
vSIPHBRSuccessInfoEv
vSIPHBRErrorEv

Figure 114: sgSWvSIPEvents

- vSIPCertificateValidityNoticeEv - SPE active and SPE Certificate ends
- vSIPCertificateExpiredErrorEv - SPE active and SPE Certificate expired
- vSIPCertificateErrorEv - SPE active and there are problems with SPE Certificate
- vSIPCertificateUpdateNoticeEv - SPE active and SPE Certificate has been updated
- vSIPCRLExpiredErrorEv - SPE active and CRL (certificate revocation list) expired
- vSIPStartupInfoEv - vHG3500 startup event
- vSIPHBRSuccessInfoEv - HBR ip address configured in AMO. Automatic configuration restore has finished successfully
- vSIPHBRErrorEv - HBR ip address configured in AMO, but bad credentials or bad address.Automatic configuration restore has failed

sgSWStmixEvents

STMIX events:



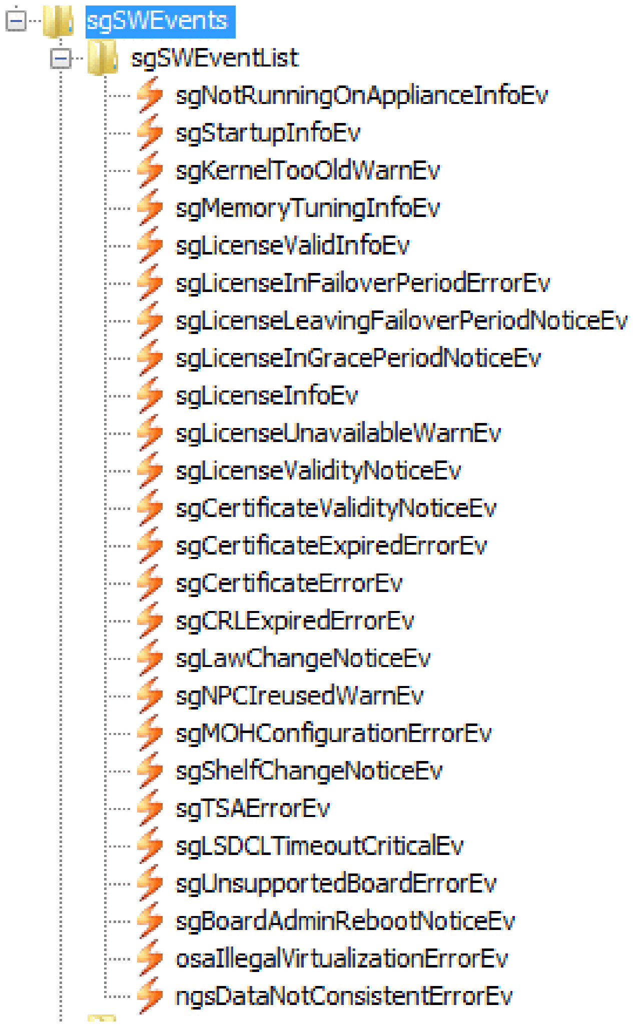
- sgSWStmixEvents
  - sgSWStmixEventList
    - stmixHWTSLAlreadyInUseNoticeEv
    - stmixBoardAdminRebootNoticeEv

Figure 115: sgSWStmixEvents

- stmixHWTSLAlreadyInUseNoticeEv - Timeslot already in use, will be automatically cleared in SG or STMIX by RTO
- stmixBoardAdminRebootNoticeEv - Board is intentionally rebooted

sgSWEventList

The rest of the software events produced by the Softgate system which are not specific for given board types:



- sgSWEvents
  - sgSWEventList
    - sgNotRunningOnApplianceInfoEv
    - sgStartupInfoEv
    - sgKernelTooOldWarnEv
    - sgMemoryTuningInfoEv
    - sgLicenseValidInfoEv
    - sgLicenseInFailoverPeriodErrorEv
    - sgLicenseLeavingFailoverPeriodNoticeEv
    - sgLicenseInGracePeriodNoticeEv
    - sgLicenseInfoEv
    - sgLicenseUnavailableWarnEv
    - sgLicenseValidityNoticeEv
    - sgCertificateValidityNoticeEv
    - sgCertificateExpiredErrorEv
    - sgCertificateErrorEv
    - sgCRLExpiredErrorEv
    - sgLawChangeNoticeEv
    - sgNPCIreusedWarnEv
    - sgMOHConfigurationErrorEv
    - sgShelfChangeNoticeEv
    - sgTSAErrorEv
    - sgLSDCLTimeoutCriticalEv
    - sgUnsupportedBoardErrorEv
    - sgBoardAdminRebootNoticeEv
    - osaIllegalVirtualizationErrorEv
    - ngsDataNotConsistentErrorEv

Figure 116: sgSWEventList

- sgNotRunningOnApplianceInfoEv - SoftGate is not running on an appliance

- sgStartupInfoEv - Info about platform, displayed during start-up. SG on VM, UNKNOWNVM, OSA500A, OSA500I, DSCXL2, COTS or unknown.
- sgKernelTooOldWarnEv - Kernel is too old for SG usage
- sgMemoryTuningInfoEv - On SoftGate HW with 4 GB memory webservice will be automatically disabled after 7 days to reduce memory consumption.
- sgLicenseValidInfoEv - Softgate License is valid info.
- sgLicenseInFailoverPeriodErrorEv - Probably licensing server CLA not reachable.
- sgLicenseLeavingFailoverPeriodNoticeEv - Licensing server CLA reachable again.
- sgLicenseInGracePeriodNoticeEv - SoftGate is in Grace Period regarding the license.
- sgLicenseInfoEv - Message from CsCM.
- sgLicenseUnavailableWarnEv - SoftGate license not available
- sgLicenseValidityNoticeEv - Period of validity of SoftGate license.
- sgCertificateValidityNoticeEv - SPE active and SPE Certificate ends.
- sgCertificateExpiredErrorEv - SPE active and SPE Certificate expired
- sgCertificateErrorEv - SPE active and there are problems with SPE Certificate
- sgCRLExpiredErrorEv - SPE active and CRL (certificate revocation list) expired
- sgLawChangeNoticeEv - Law configuration changed for Slot.
- sgNPCIreusedWarnEv - IPDA Port reuse.
- sgMOHConfigurationErrorEv - Music on hold configuration problem.
- sgShelfChangeNoticeEv - SoftGate shelf type or shelf config has changed, SoftGate will reboot automatically.
- sgTSAErrorEv - TSA Error
- sgLSDCLTimeoutCriticalEv - Restart of SoftGate due to timeout of native lsdcl.
- sgUnsupportedBoardErrorEv - Board type is not supported in SoftGate (even you can configure it in AMO).
- sgBoardAdminRebootNoticeEv - Board is intentionally rebooted
- osaIllegalVirtualizationErrorEv - Illegal virtualization for board or module.
- ngsDataNotConsistentErrorEv - NGS address is configured and NCUI payload ip from RMX boarddata differ from NGS database.

8.1.3.8 cstaEvents

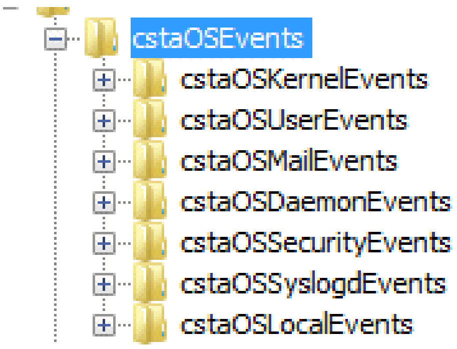
The CSTA running inside of the active node of the OpenScape4000 was also extended in V7R2 by sending SNMPv3 traps from its operating system and CSTA processes.

cstaOSEvents

The cstaOSEvents trap uses a generic trap model, i.e. it is not obvious from the trap name what kind of error occurred. Each trap includes an evDescr as a trap variable binding which has to be used to find the reason for the error. Only the trap severity (priority) and facility (which OS subsytem produced the trap) can be found based on the trap name.

The SNMP engine is preset to send traps messages from the sperating system with severity error up-to emerg only. The messages with lower priority are not send as snmp traps.

The cstaOSEvents includes following categories of traps:



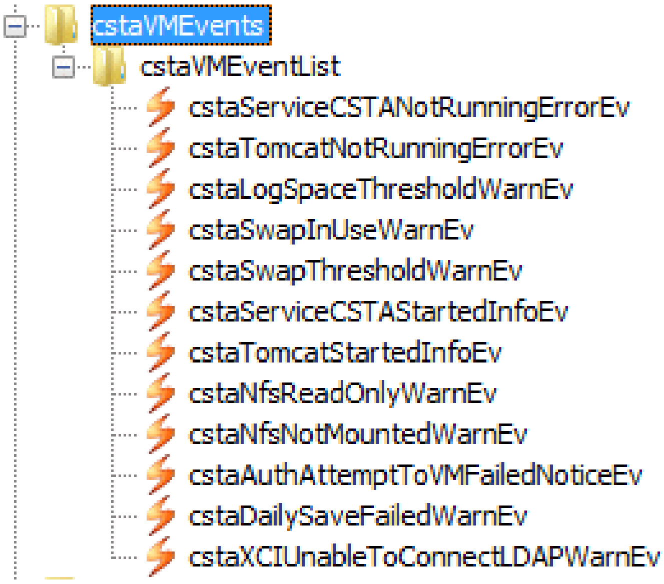
cstaOSEvents
cstaOSKernelEvents
cstaOSUserEvents
cstaOSMailEvents
cstaOSDaemonEvents
cstaOSSecurityEvents
cstaOSSyslogdEvents
cstaOSLocalEvents

Figure 117: cstaOSEvents

- cstaOSKernelEvents - CSTA operating system kernel messages
- cstaOSUserEvents - CSTA operating system application/service messages
- cstaOSMailEvents - CSTA operating system mail system messages
- cstaOSDaemonEvents - Messages from system daemons CSTA operating system
- cstaOSSecurityEvents - CSTA operating system security/authorization messages
- cstaOSSyslogdEvents - Messages generated internally by syslogd of the CSTA operating system
- cstaOSLocalEvents - Messages generated by an administrator or applications from CSTA operating system

cstaVMEvents

Events related to monitoring and processes of the Virtual Machine of CSTA:



cstaVMEvents
cstaVMEventList
cstaServiceCSTANotRunningErrorEv
cstaTomcatNotRunningErrorEv
cstaLogSpaceThresholdWarnEv
cstaSwapInUseWarnEv
cstaSwapThresholdWarnEv
cstaServiceCSTAStartedInfoEv
cstaTomcatStartedInfoEv
cstaNfsReadOnlyWarnEv
cstaNfsNotMountedWarnEv
cstaAuthAttemptToVMFailedNoticeEv
cstaDailySaveFailedWarnEv
cstaXCIUnableToConnectLDAPWarnEv

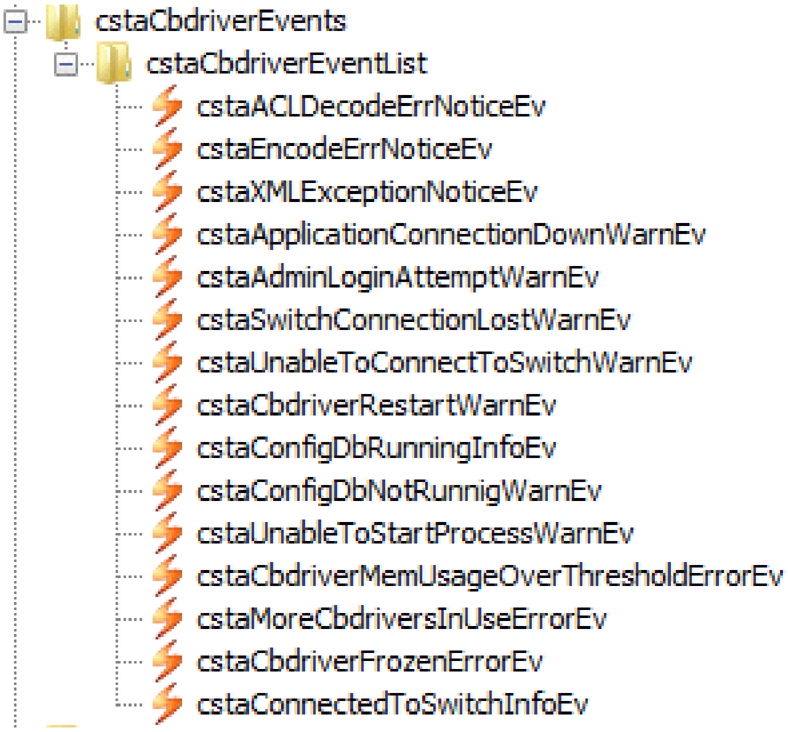
Figure 118: cstaVMEvents

- cstaServiceCSTANotRunningErrorEv - CSTA service not running

- cstaTomcatNotRunningErrorEv - Tomcat service not running
- cstaLogSpaceThresholdWarnEv - Log partition full over threshold
- cstaSwapInUseWarnEv - System is swaping
- cstaSwapThresholdWarnEv - Swap is full over threshold
- cstaServiceCSTAStartedInfoEv - CSTA service started
- cstaTomcatStartedInfoEv - Tomcat server started.
- cstaNfsReadOnlyWarnEv - NFS mounted read-only
- cstaNfsNotMountedWarnEv - NFS not mounted
- cstaAuthAttemptToVMFailedNoticeEv - Failed authentication attempt on VM
- cstaDailySaveFailedWarnEv - Daily automatic backup for reinstall failed
- cstaXCIUnableToConnectLDAPWarnEv - XCI unable to connect LDAP

cstaCdbDriverEvents

Events related to the CSTA cbdriver software:



cstaCbdriverEvents
- cstaCbdriverEventList
  - cstaACLDecodeErrNoticeEv
  - cstaEncodeErrNoticeEv
  - cstaXMLExceptionNoticeEv
  - cstaApplicationConnectionDownWarnEv
  - cstaAdminLoginAttemptWarnEv
  - cstaSwitchConnectionLostWarnEv
  - cstaUnableToConnectToSwitchWarnEv
  - cstaCbdriverRestartWarnEv
  - cstaConfigDbRunningInfoEv
  - cstaConfigDbNotRunnigWarnEv
  - cstaUnableToStartProcessWarnEv
  - cstaCbdriverMemUsageOverThresholdErrorEv
  - cstaMoreCbdriversInUseErrorEv
  - cstaCbdriverFrozenErrorEv
  - cstaConnectedToSwitchInfoEv

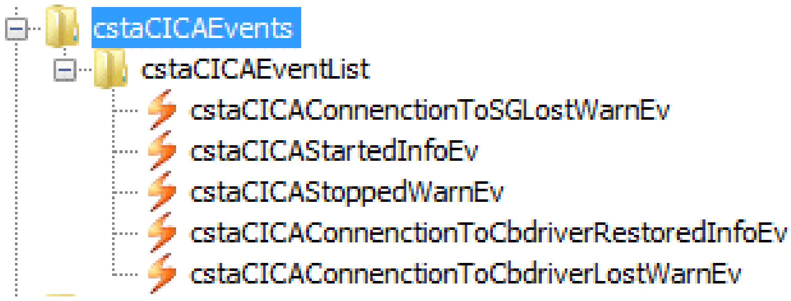
Figure 119: cstaCdbDriverEvents

- cstaACLDecodeErrNoticeEv - ACL decode error
- cstaEncodeErrNoticeEv - CSTA encode error
- cstaXMLExceptionNoticeEv - XML exception
- cstaApplicationConnectionDownWarnEv - Application connection down
- cstaAdminLoginAttemptWarnEv - Login attempt with Admin
- cstaSwitchConnectionLostWarnEv - Connection to switch lost
- cstaUnableToConnectToSwitchWarnEv - Unable to connect to switch, check AMO config
- cstaCbdriverRestartWarnEv - Cbdriver stopped with <error> - restarted
- cstaConfigDbRunningInfoEv - Configdb running
- cstaConfigDbNotRunnigWarnEv - Configdb not running
- cstaUnableToStartProcessWarnEv - Unable to start process - see evDescr of trap

- cstaCbdriverMemUsageOverThresholdErrorEv - Cbdriver uses memory over threshold, restart it
- cstaMoreCbdriversInUseErrorEv - More than N cbdrivers are in use
- cstaCbdriverFrozenErrorEv - Cbdriver process stuck in memory, kill it manually
- cstaConnectedToSwitchInfoEv - CSTA connection to switch established.

cstaCICAEvents

Events related to CICA:



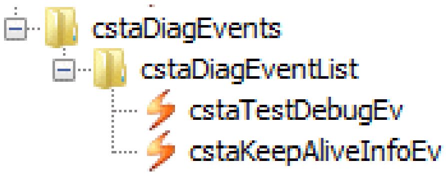
cstaCICAEvents
cstaCICAEventList
cstaCICAConnenctionToSGLostWarnEv
cstaCICAStartedInfoEv
cstaCICAStoppedWarnEv
cstaCICAConnenctionToCbdriverRestoredInfoEv
cstaCICAConnenctionToCbdriverLostWarnEv

Figure 120: cstaCICAEvents

- cstaCICAConnenctionToSGLostWarnEv - CICA conenction to SG lost
- cstaCICAStartedInfoEv - CICA started
- cstaCICAStoppedWarnEv - CICA stopped
- cstaCICAConnenctionToCbdriverRestoredInfoEv - CICA conenction to cbdriver restored
- cstaCICAConnenctionToCbdriverLostWarnEv - CICA conenction to cbdriver lost

cstaDiagEvents

Events used for CSTA diagnostic purposes:



cstaDiagEvents
cstaDiagEventList
cstaTestDebugEv
cstaKeepAliveInfoEv

Figure 121: cstaDiagEvents

- cstaTestDebugEv - Event used for testing of SNMP functionality on the CSTA.
- cstaKeepAliveInfoEv - Keep alive event send by CSTA software

8.1.4 Monitoring via SNMP Get

The Net-SNMP Agent active on each host of any 4K system provides a wide variety of performance information over the SNMP protocol.

In addition, the agent can be queried for a listing of the installed RPM packages on the system, a listing of currently running processes on the system, or the network configuration of the system.

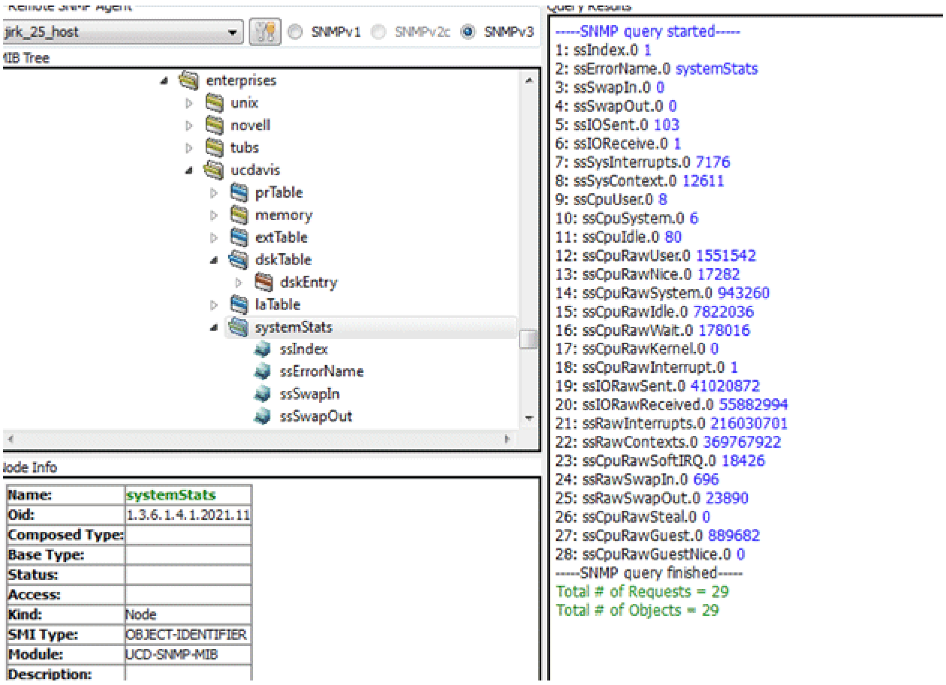
This section provides a brief overview of the data available via the SNMP Host Resources MIB, USDAVIS mib (UCD-SNMP-MIB, UCD-DISKIO-MIB) and IF-MIB.

8.1.4.1 UCD-SNMP-MIB

The majority of the system performance data is available in the UCD SNMP MIB.

Monitoring Processors Usage

The systemStats OID provides a number of counters around processor usage:



Name:	systemStats
Oid:	1.3.6.1.4.1.2021.11
Composed Type:	
Base Type:	
Status:	
Access:	
Kind:	Node
SMI Type:	OBJECT-IDENTIFIER
Module:	UCD-SNMP-MIB
Description:	

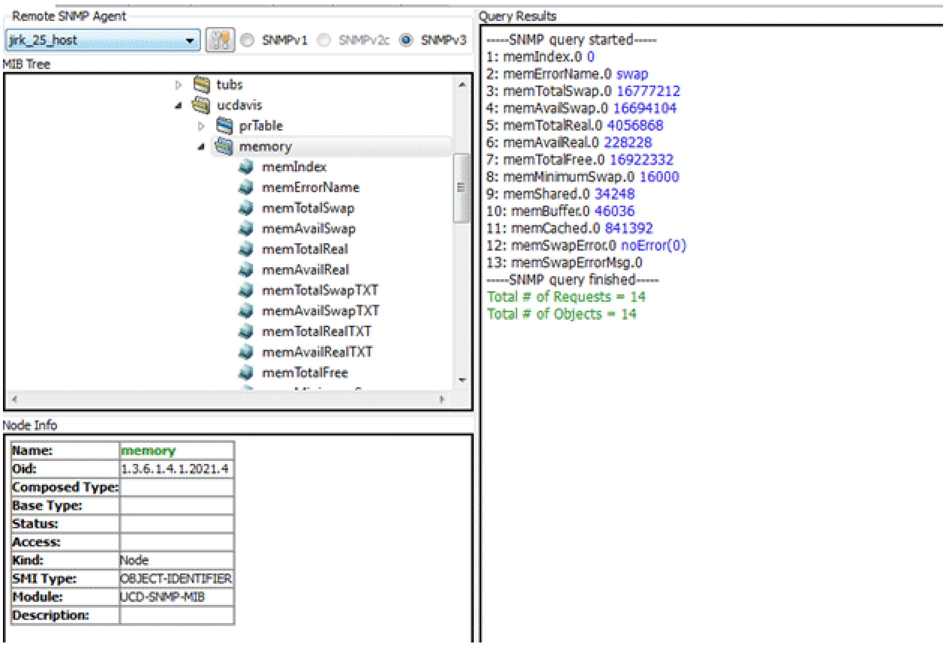
```
-----SNMP query started-----
1: ssIndex.0 1
2: ssErrorName.0 systemStats
3: ssSwapIn.0 0
4: ssSwapOut.0 0
5: ssIOSent.0 103
6: ssIOReceive.0 1
7: ssSysInterrupts.0 7176
8: ssSysContext.0 12611
9: ssCpuUser.0 8
10: ssCpuSystem.0 6
11: ssCpuIdle.0 80
12: ssCpuRawUser.0 1551542
13: ssCpuRawNice.0 17282
14: ssCpuRawSystem.0 943260
15: ssCpuRawIdle.0 7822036
16: ssCpuRawWait.0 178016
17: ssCpuRawKernel.0 0
18: ssCpuRawInterrupt.0 1
19: ssIORawSent.0 41020872
20: ssIORawReceived.0 55882994
21: ssRawInterrupts.0 216030701
22: ssRawContexts.0 369767922
23: ssCpuRawSoftIRQ.0 18426
24: ssRawSwapIn.0 696
25: ssRawSwapOut.0 23890
26: ssCpuRawSteal.0 0
27: ssCpuRawGuest.0 889682
28: ssCpuRawGuestNice.0 0
-----SNMP query finished-----
Total # of Requests = 29
Total # of Objects = 29
```

Figure 122: systemStats OID

In particular, the ssCpuRawUser, ssCpuRawSystem, ssCpuRawWait, and ssCpuRawIdle OIDs provide counters which are helpful when determining whether a system is spending most of its processor time in kernel space, user space, or I/O. ssRawSwapIn and ssRawSwapOut can be helpful when determining whether a system is suffering from memory exhaustion.

Monitoring Memory Usage

Memory information is available under the UCD-SNMP-MIB::memory OID, which provides similar data to the free command:



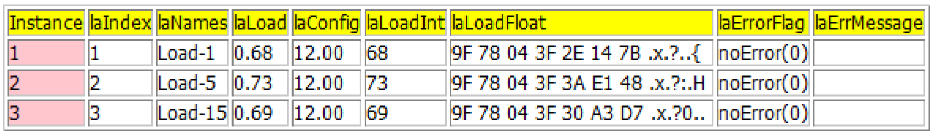
jirk_25_host ○ SNMPv1 ○ SNMPv2c ● SNMPv3

Name:	memory
Oid:	1.3.6.1.4.1.2021.4
Composed Type:	
Base Type:	
Status:	
Access:	
Kind:	Node
SMI Type:	OBJECT-IDENTIFIER
Module:	UCD-SNMP-MIB
Description:	

```
-----SNMP query started-----
1: memIndex.0 0
2: memErrorName.0 swap
3: memTotalSwap.0 16777212
4: memAvailSwap.0 16694104
5: memTotalReal.0 4056868
6: memAvailReal.0 228228
7: memTotalFree.0 16922332
8: memMinimumSwap.0 16000
9: memShared.0 34248
10: memBuffer.0 46036
11: memCached.0 841392
12: memSwapError.0 noError(0)
13: memSwapErrorMsg.0
-----SNMP query finished-----
Total # of Requests = 14
Total # of Objects = 14
```

Figure 123: Memory Stats

Load averages are also available in the UCD SNMP MIB. The SNMP table UCD-SNMP-MIB::laTable has a listing of the 1, 5, and 15 minute load averages:



Instance	laIndex	laNames	laLoad	laConfig	laLoadInt	laLoadFloat	laErrorFlag	laErrMessage
1	1	Load-1	0.68	12.00	68	9F 78 04 3F 2E 14 7B .x.?..{	noError(0)	
2	2	Load-5	0.73	12.00	73	9F 78 04 3F 3A E1 48 .x.?:.H	noError(0)	
3	3	Load-15	0.69	12.00	69	9F 78 04 3F 30 A3 D7 .x.?0..	noError(0)	

Figure 124: Load Averages

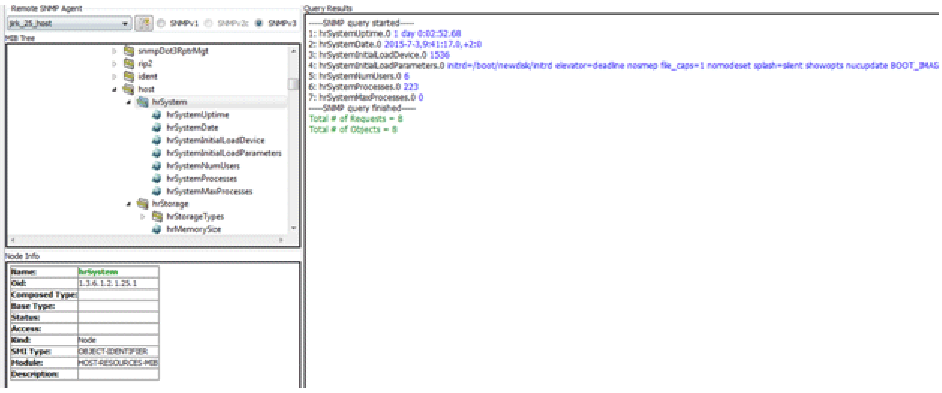
8.1.4.2 Host Resources MIB

The Host Resources MIB included with Net-SNMP displays information about the current hardware and software configuration of a host. The following OIDs are available under that MIB:

- HOST-RESOURCES-MIB::hrSystem - contains general system information such as uptime, number of users, and number of running processes
- HOST-RESOURCES-MIB::hrStorage - contains data on memory and file system usage
- HOST-RESOURCES-MIB::hrDevices - contains a listing of all processors, network devices, and file systems
- HOST-RESOURCES-MIB::hrSWRun - contains a listing of all running processes
- HOST-RESOURCES-MIB::hrSWRunPerf - contains memory and CPU statistics on the process table from HOST-RESOURCES-MIB::hrSWRun
- HOST-RESOURCES-MIB::hrSWInstalled - contains a listing of the RPM database

General System Information (hrSystem)

The hrSystem OID of HOST-RESOURCES-MIB provides general information about the system:



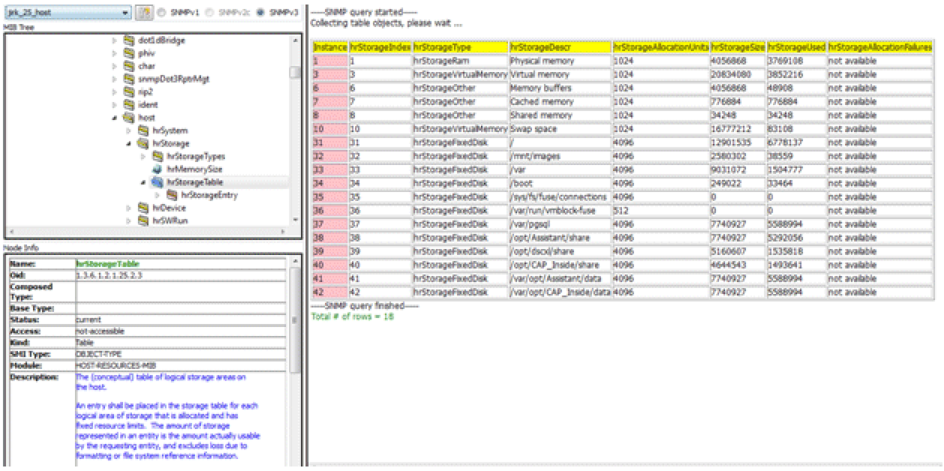
Name:	hrSystem
Oid:	1.3.6.1.2.1.25.1
Composed Type:	
Base Type:	
Status:	
Access:	
Kind:	Node
SMI Type:	OBJECT-IDENTIFIER
Module:	HOST-RESOURCES-MIB
Description:	

```
-----SNMP query started-----
1: hrSystemUptime.0 1 day 0:02:52.68
2: hrSystemDate.0 2015-7-3,9:41:17.0,+2:0
3: hrSystemInitialLoadDevice.0 1536
4: hrSystemInitialLoadParameters.0 initrd=/boot/newdisk/initrd elevator=deadline nosmep file_caps=1 nomodeset splash=silent showopts nucupdate BOOT_IMAG
5: hrSystemNumUsers.0 6
6: hrSystemProcesses.0 223
7: hrSystemMaxProcesses.0 0
-----SNMP query finished-----
Total # of Requests = 8
Total # of Objects = 8
```

Figure 125: hrSystem

File System and Disk Information (hrStorage)

The Host Resources MIB provides information about the size and usage of the file systems. Each file system (and also each memory pool) has an entry in the HOST-RESOURCES-MIB::hrStorageTable table:



Name:	hrStorageTable
Oid:	1.3.6.1.2.1.25.2.3
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Table
SMI Type:	OBJECT-TYPE
Module:	HOST-RESOURCES-MIB
Description:	The (conceptual) table of logical storage areas on the host. An entry shall be placed in the storage table for each logical area of storage that is allocated and has fixed resource limits. The amount of storage represented in an entity is the amount actually usable by the requesting entity, and excludes loss due to formatting or file system reference information.

```
-----SNMP query started-----
Collecting table objects, please wait ...
```

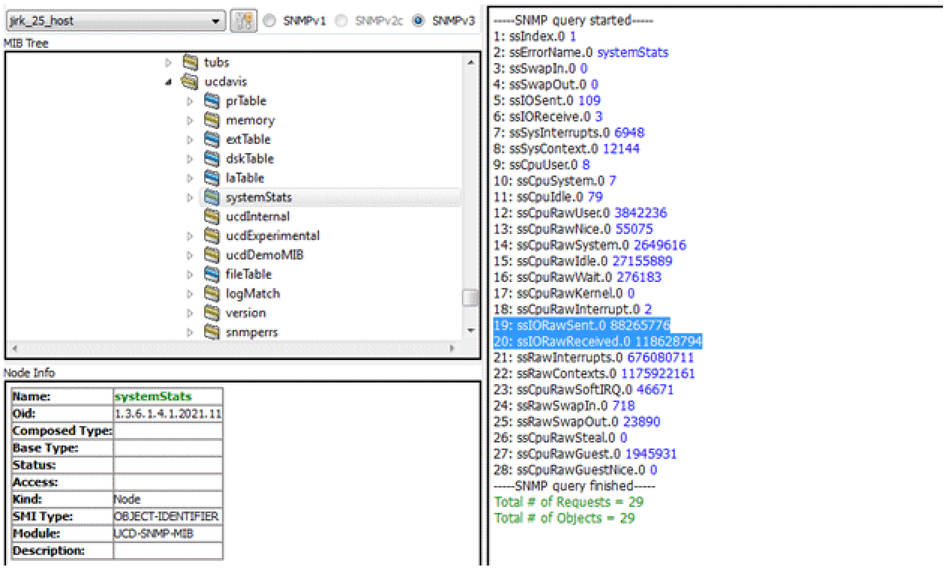
Instance	hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageAllocationUnits	hrStorageSize	hrStorageUsed	hrStorageAllocationFailures
1	1	hrStorageRam	Physical memory	1024	4056868	3769108	not available
3	3	hrStorageVirtualMemory	Virtual memory	1024	20834080	3852216	not available
6	6	hrStorageOther	Memory buffers	1024	4056868	48908	not available
7	7	hrStorageOther	Cached memory	1024	776884	776884	not available
8	8	hrStorageOther	Shared memory	1024	34248	34248	not available
10	10	hrStorageVirtualMemory	Swap space	1024	16777212	83108	not available
31	31	hrStorageFixedDisk	/	4096	12901535	6778137	not available
32	32	hrStorageFixedDisk	/mnt/images	4096	2580302	38559	not available
33	33	hrStorageFixedDisk	/var	4096	9031072	1504777	not available
34	34	hrStorageFixedDisk	/boot	4096	249022	33464	not available
35	35	hrStorageFixedDisk	/sys/fs/fuse/connections	4096	0	0	not available
36	36	hrStorageFixedDisk	/var/run/vmblock-fuse	512	0	0	not available
37	37	hrStorageFixedDisk	/var/pgsql	4096	7740927	5588994	not available
38	38	hrStorageFixedDisk	/opt/Assistant/share	4096	7740927	5292056	not available
39	39	hrStorageFixedDisk	/opt/dscxl/share	4096	5160607	1535818	not available
40	40	hrStorageFixedDisk	/opt/CAP_Inside/share	4096	4644543	1493641	not available
41	41	hrStorageFixedDisk	/var/opt/Assistant/data	4096	7740927	5588994	not available
42	42	hrStorageFixedDisk	/var/opt/CAP_Inside/data	4096	7740927	5588994	not available

```
-----SNMP query finished-----
Total # of rows = 18
```

Figure 126: hrStorage

The OIDs under HOST-RESOURCES-MIB::hrStorageSize and HOST-RESOURCES-MIB::hrStorageUsed can be used to calculate the remaining capacity of each mounted file system.

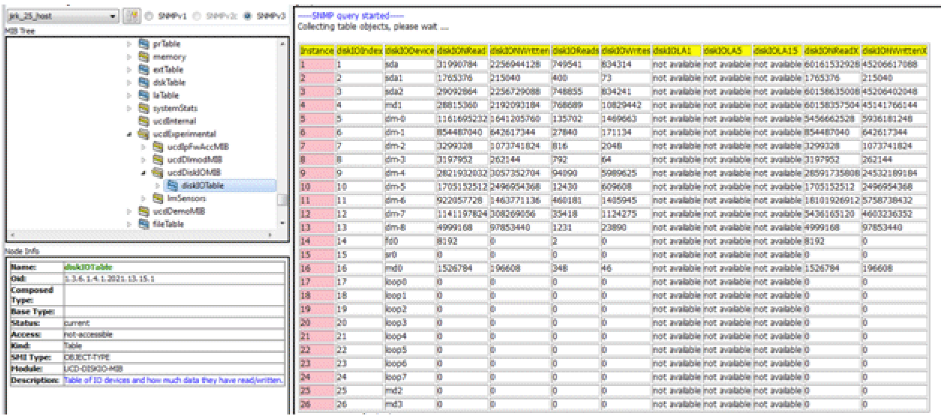
I/O data is available both in UCD-SNMP-MIB::systemStats (ssIORawSent.0 and ssIORawRecieved.0) and in UCD-DISKIO-MIB::diskIOTable. The latter provides much more granular data. Under this table you will find OIDs for diskIONReadX and diskIONWrittenX, providing counters for the number of bytes read from and written to the block device in question since the system boot:



Name:	systemStats
Oid:	1.3.6.1.4.1.2021.11
Composed Type:	
Base Type:	
Status:	
Access:	
Kind:	Node
SMI Type:	OBJECT-IDENTIFIER
Module:	UCD-SNMP-MIB
Description:	

```
-----SNMP query started-----
1: ssIndex.0 1
2: ssErrorName.0 systemStats
3: ssSwapIn.0 0
4: ssSwapOut.0 0
5: ssIOSent.0 109
6: ssIOReceive.0 3
7: ssSysInterrupts.0 6948
8: ssSysContext.0 12144
9: ssCpuUser.0 8
10: ssCpuSystem.0 7
11: ssCpuIdle.0 79
12: ssCpuRawUser.0 3842236
13: ssCpuRawNice.0 55075
14: ssCpuRawSystem.0 2649616
15: ssCpuRawIdle.0 27155889
16: ssCpuRawWait.0 276183
17: ssCpuRawKernel.0 0
18: ssCpuRawInterrupt.0 2
19: ssIORawSent.0 88265776
20: ssIORawReceived.0 118628794
21: ssRawInterrupts.0 676080711
22: ssRawContexts.0 1175922161
23: ssCpuRawSoftIRQ.0 46671
24: ssRawSwapIn.0 718
25: ssRawSwapOut.0 23890
26: ssCpuRawSteal.0 0
27: ssCpuRawGuest.0 1945931
28: ssCpuRawGuestNice.0 0
-----SNMP query finished-----
Total # of Requests = 29
Total # of Objects = 29
```

Figure 127: systemStats (ssIORawSent.0 and ssIORawRecieved.0)



Name:	diskIOTable
Oid:	1.3.6.1.4.1.2021.13.15.1
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Table
SMI Type:	OBJECT-TYPE
Module:	UCD-DISKIO-MIB
Description:	Table of IO devices and how much data they have read/written.

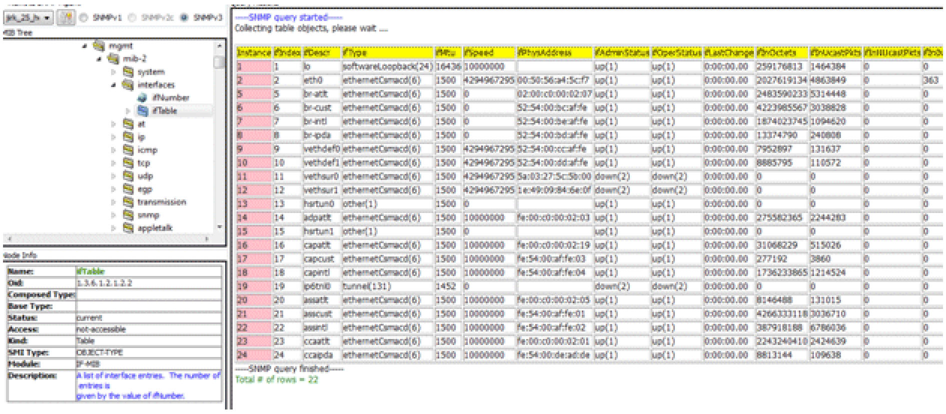
```
-----SNMP query started-----
Collecting table objects, please wait ...
```

Instance	diskIOIndex	diskIODevice	diskIONRead	diskIONWritten	diskIOReads	diskIOWrites	diskIOLA1	diskIOLA5	diskIOLA15	diskIONReadX	diskIONWrittenX
1	1	sda	31990784	2256944128	749541	834314	not available	not available	not available	60161532928	45206617088
2	2	sda1	1765376	215040	400	73	not available	not available	not available	1765376	215040
3	3	sda2	29092864	2256729088	748855	834241	not available	not available	not available	60158635008	45206402048
4	4	md1	28815360	2192093184	768689	10829442	not available	not available	not available	60158357504	45141766144
5	5	dm-0	1161695232	1641205760	135702	1469663	not available	not available	not available	5456662528	5936181248
6	6	dm-1	854487040	642617344	27840	171134	not available	not available	not available	854487040	642617344
7	7	dm-2	3299328	1073741824	816	2048	not available	not available	not available	3299328	1073741824
8	8	dm-3	3197952	262144	792	64	not available	not available	not available	3197952	262144
9	9	dm-4	2821932032	3057352704	94090	5989625	not available	not available	not available	28591735808	24532189184
10	10	dm-5	1705152512	2496954368	12430	609608	not available	not available	not available	1705152512	2496954368
11	11	dm-6	922057728	1463771136	460181	1405945	not available	not available	not available	18101926912	5758738432
12	12	dm-7	1141197824	308269056	35418	1124275	not available	not available	not available	5436165120	4603236352
13	13	dm-8	4999168	97853440	1231	23890	not available	not available	not available	4999168	97853440
14	14	fd0	8192	0	2	0	not available	not available	not available	8192	0
15	15	sr0	0	0	0	0	not available	not available	not available	0	0
16	16	md0	1526784	196608	348	46	not available	not available	not available	1526784	196608
17	17	loop0	0	0	0	0	not available	not available	not available	0	0
18	18	loop1	0	0	0	0	not available	not available	not available	0	0
19	19	loop2	0	0	0	0	not available	not available	not available	0	0
20	20	loop3	0	0	0	0	not available	not available	not available	0	0
21	21	loop4	0	0	0	0	not available	not available	not available	0	0
22	22	loop5	0	0	0	0	not available	not available	not available	0	0
23	23	loop6	0	0	0	0	not available	not available	not available	0	0
24	24	loop7	0	0	0	0	not available	not available	not available	0	0
25	25	md2	0	0	0	0	not available	not available	not available	0	0
26	26	md3	0	0	0	0	not available	not available	not available	0	0

Figure 128: diskIOTable

Network Information

The Interfaces MIB provides information on network devices. IF-MIB::ifTable provides an SNMP table with an entry for each interface on the system, the configuration of the interface, and various packet counters for the interface. The following example shows an ifTable on an OpenScape4000 active simplex node system running on VM:



Name:	ifTable
Oid:	1.3.6.1.2.1.2.2
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Table
SMI Type:	OBJECT-TYPE
Module:	IF-MIB
Description:	A list of interface entries. The number of entries is given by the value of ifNumber.

```
-----SNMP query started-----
Collecting table objects, please wait ...
```

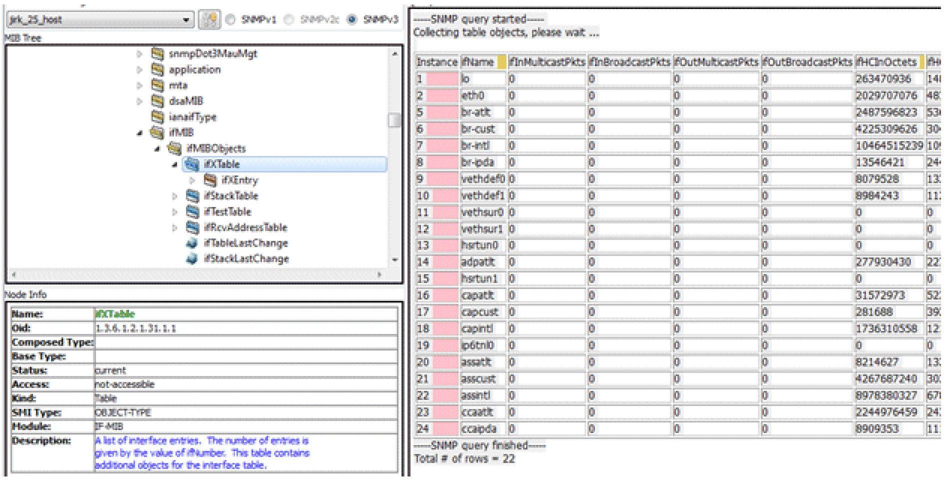
Instance	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUcastPkts	ifInNUcastPkts	ifIn
1	1	lo	softwareLoopback(24)	16436	10000000		up(1)	up(1)	0:00:00.00	259176813	1464384	0	0
2	2	eth0	ethernetCsmacd(6)	1500	4294967295	00:50:56:a4:5c:f7	up(1)	up(1)	0:00:00.00	2027619134	4863849	0	363
5	5	br-atlt	ethernetCsmacd(6)	1500	0	02:00:c0:00:02:07	up(1)	up(1)	0:00:00.00	2483590233	5314448	0	0
6	6	br-cust	ethernetCsmacd(6)	1500	0	52:54:00:bc:af:fe	up(1)	up(1)	0:00:00.00	4223985567	3038828	0	0
7	7	br-intl	ethernetCsmacd(6)	1500	0	52:54:00:be:af:fe	up(1)	up(1)	0:00:00.00	1874023745	1094620	0	0
8	8	br-ipda	ethernetCsmacd(6)	1500	0	52:54:00:bd:af:fe	up(1)	up(1)	0:00:00.00	13374790	240808	0	0
9	9	vethdef0	ethernetCsmacd(6)	1500	4294967295	52:54:00:cc:af:fe	up(1)	up(1)	0:00:00.00	7952897	131637	0	0
10	10	vethdef1	ethernetCsmacd(6)	1500	4294967295	52:54:00:dd:af:fe	up(1)	up(1)	0:00:00.00	8885795	110572	0	0
11	11	vethsur0	ethernetCsmacd(6)	1500	4294967295	5a:03:27:5c:5b:00	down(2)	down(2)	0:00:00.00	0	0	0	0
12	12	vethsur1	ethernetCsmacd(6)	1500	4294967295	1e:49:09:84:6e:0f	down(2)	down(2)	0:00:00.00	0	0	0	0
13	13	hsrtun0	other(1)	1500	0		up(1)	up(1)	0:00:00.00	0	0	0	0
14	14	adpatlt	ethernetCsmacd(6)	1500	10000000	fe:00:c0:00:02:03	up(1)	up(1)	0:00:00.00	275582365	2244283	0	0
15	15	hsrtun1	other(1)	1500	0		up(1)	up(1)	0:00:00.00	0	0	0	0
16	16	capatlt	ethernetCsmacd(6)	1500	10000000	fe:00:c0:00:02:19	up(1)	up(1)	0:00:00.00	31068229	515026	0	0
17	17	capcust	ethernetCsmacd(6)	1500	10000000	fe:54:00:af:fe:03	up(1)	up(1)	0:00:00.00	277192	3860	0	0
18	18	capintl	ethernetCsmacd(6)	1500	10000000	fe:54:00:af:fe:04	up(1)	up(1)	0:00:00.00	1736233865	1214524	0	0
19	19	ip6tnl0	tunnel(131)	1452	0		down(2)	down(2)	0:00:00.00	0	0	0	0
20	20	assatlt	ethernetCsmacd(6)	1500	10000000	fe:00:c0:00:02:05	up(1)	up(1)	0:00:00.00	8146488	131015	0	0
21	21	asscust	ethernetCsmacd(6)	1500	10000000	fe:54:00:af:fe:01	up(1)	up(1)	0:00:00.00	4266333118	3036710	0	0
22	22	assintl	ethernetCsmacd(6)	1500	10000000	fe:54:00:af:fe:02	up(1)	up(1)	0:00:00.00	387918188	6786036	0	0
23	23	ccaatlt	ethernetCsmacd(6)	1500	10000000	fe:00:c0:00:02:01	up(1)	up(1)	0:00:00.00	2243240410	2424639	0	0
24	24	ccaipda	ethernetCsmacd(6)	1500	10000000	fe:54:00:de:ad:de	up(1)	up(1)	0:00:00.00	8813144	109638	0	0

```
-----SNMP query finished-----
Total # of rows = 22
```

Figure 129: ifTable

However, as you can see the network speed (ifSpeed) is at the maximum value; so this value is not sufficient for network monitoring of OpenScape 4000 interfaces.

You have to use the IF-MIB:ifXTable which is an extension of ifTable.



Name:	ifXTable
Oid:	1.3.6.1.2.1.31.1.1
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Table
SMI Type:	OBJECT-TYPE
Module:	IF-MIB
Description:	A list of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.

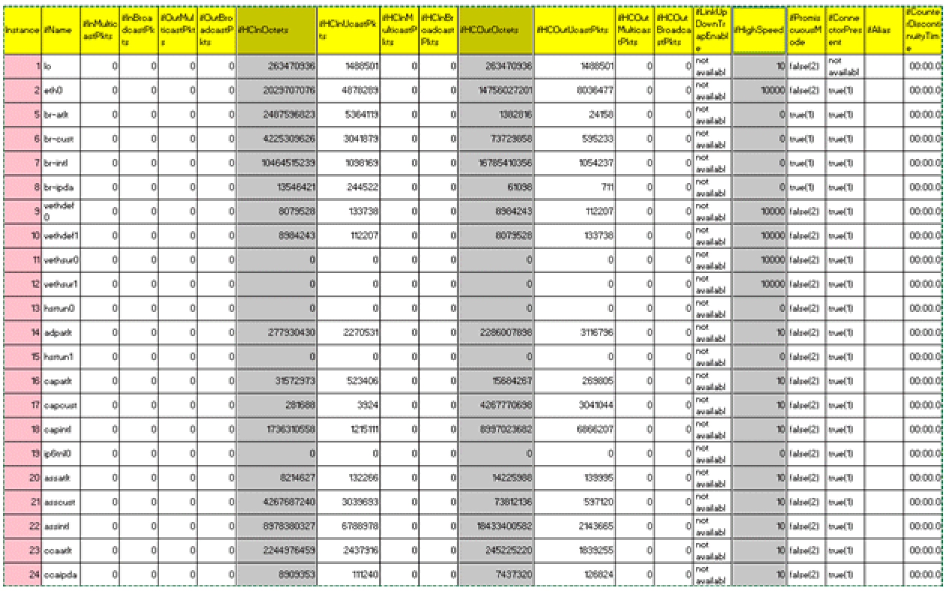
```
-----SNMP query started-----
Collecting table objects, please wait ...
```

Instance	ifName	ifInMulticastPkts	ifInBroadcastPkts	ifOutMulticastPkts	ifOutBroadcastPkts	ifHCInOctets	ifH
1	lo	0	0	0	0	263470936	14
2	eth0	0	0	0	0	2029707076	48
5	br-atlt	0	0	0	0	2487596823	53
6	br-cust	0	0	0	0	4225309626	30
7	br-intl	0	0	0	0	10464515239	10
8	br-ipda	0	0	0	0	13546421	24
9	vethdef0	0	0	0	0	8079528	13
10	vethdef1	0	0	0	0	8984243	11
11	vethsur0	0	0	0	0	0	0
12	vethsur1	0	0	0	0	0	0
13	hsrtun0	0	0	0	0	0	0
14	adpatlt	0	0	0	0	277930430	22
15	hsrtun1	0	0	0	0	0	0
16	capatlt	0	0	0	0	31572973	52
17	capcust	0	0	0	0	281688	39
18	capintl	0	0	0	0	1736310558	12
19	ip6tnl0	0	0	0	0	0	0
20	assatlt	0	0	0	0	8214627	13
21	asscust	0	0	0	0	4267687240	30
22	assintl	0	0	0	0	8978380327	67
23	ccaatlt	0	0	0	0	2244976459	24
24	ccaipda	0	0	0	0	8909353	11

```
-----SNMP query finished-----
Total # of rows = 22
```

Figure 130: ifXTable

Here the ifHighSpeed value can be used for finding correct interface speed:



Instance	ifName	ifInMulticastPkts	ifInBroadcastPkts	ifOutMulticastPkts	ifOutBroadcastPkts	ifHCInOctets	ifHCInUcastPkts	ifHCInMulticastPkts	ifHCInBroadcastPkts	ifHCOutOctets	ifHCOutUcastPkts	ifHCOutMulticastPkts	ifHCOutBroadcastPkts	ifLinkUpDownTrapEnable	ifHighSpeed	ifPromiscuousMode	ifConnectorPresent	ifAlias	ifCounterDiscontinuityTime
1	lo	0	0	0	0	263470936	1488501	0	0	263470936	1488501	0	0	not availabl	10	false(2)	not availabl		00:00:0
2	eth0	0	0	0	0	2029707076	4878289	0	0	14756027201	8036477	0	0	not availabl	10000	false(2)	true(1)		00:00:0
5	br-atk	0	0	0	0	2487536823	5364119	0	0	1382816	24158	0	0	not availabl	0	true(1)	true(1)		00:00:0
6	br-cust	0	0	0	0	4225309626	3041873	0	0	73729858	595233	0	0	not availabl	0	true(1)	true(1)		00:00:0
7	br-intl	0	0	0	0	10464515239	1098169	0	0	16785410356	1054237	0	0	not availabl	0	true(1)	true(1)		00:00:0
8	br-ipda	0	0	0	0	13546421	244522	0	0	61098	711	0	0	not availabl	0	true(1)	true(1)		00:00:0
9	vethdef0	0	0	0	0	8079528	133738	0	0	8984243	112207	0	0	not availabl	10000	false(2)	true(1)		00:00:0
10	vethdef1	0	0	0	0	8984243	112207	0	0	8079528	133738	0	0	not availabl	10000	false(2)	true(1)		00:00:0
11	vethsur0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	10000	false(2)	true(1)		00:00:0
12	vethsur1	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	10000	false(2)	true(1)		00:00:0
13	hsrtun0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00:0
14	adpatk	0	0	0	0	277930430	2270531	0	0	2286007898	3116796	0	0	not availabl	10	false(2)	true(1)		00:00:0
15	hsrtun1	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00:0
16	capatk	0	0	0	0	31572973	523406	0	0	15684267	269805	0	0	not availabl	10	false(2)	true(1)		00:00:0
17	capcust	0	0	0	0	281688	3924	0	0	4267770698	3041044	0	0	not availabl	10	false(2)	true(1)		00:00:0
18	capintl	0	0	0	0	1736310558	1215111	0	0	8997023682	6866207	0	0	not availabl	10	false(2)	true(1)		00:00:0
19	ip6tnl0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00:0
20	assatk	0	0	0	0	8214627	132266	0	0	14225988	139995	0	0	not availabl	10	false(2)	true(1)		00:00:0
21	asscust	0	0	0	0	4267687240	3039693	0	0	73812136	597120	0	0	not availabl	10	false(2)	true(1)		00:00:0
22	assintl	0	0	0	0	8978380327	6788978	0	0	18433400582	2143665	0	0	not availabl	10	false(2)	true(1)		00:00:0
23	ccaatk	0	0	0	0	2244976459	2437916	0	0	245225220	1839255	0	0	not availabl	10	false(2)	true(1)		00:00:0
24	ccaipda	0	0	0	0	8909353	111240	0	0	7437320	126824	0	0	not availabl	10	false(2)	true(1)		00:00:0

Figure 131: ifHighSpeed table

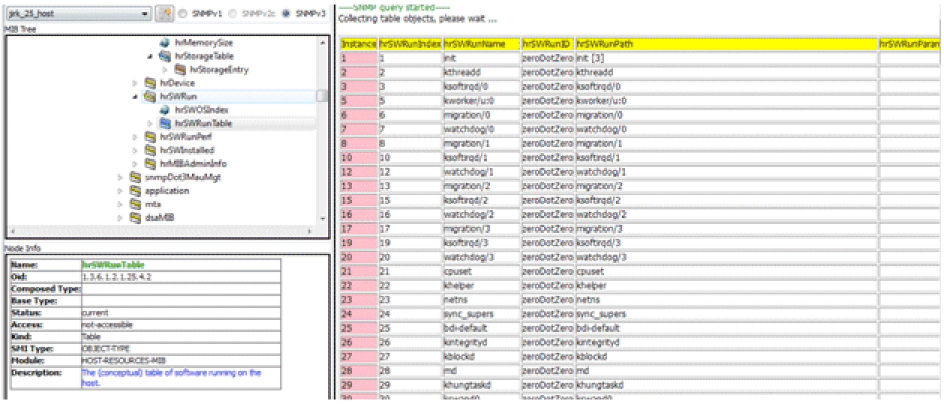
The traffic is available under the OIDs IF-MIB::ifHCOutOctets and IF-MIB::ifHCInOctets. Based on these values taken from two subsequent calls you can determine the interface load.

Software Information

- Information about installed software rpm packages, running processes and their performance statistics (CPU/MEM usage) can be collected from following three OIDs:
- HOST-RESOURCES-MIB::hrSWRun - contains a listing of all running processes
- HOST-RESOURCES-MIB::hrSWRunPerf - contains memory and CPU statistics on the process table from HOST-RESOURCES-MIB::hrSWRun
- HOST-RESOURCES-MIB::hrSWInstalled - contains a listing of the RPM database

Running software

HOST-RESOURCES-MIB::hrSWRun - contains a listing of all running processes on a OpenScape 4000 host system:



Name:	hrSWRunTable
Oid:	1.3.6.1.2.1.25.4.2
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Table
SMI Type:	OBJECT-TYPE
Module:	HOST-RESOURCES-MIB
Description:	The (conceptual) table of software running on the host.

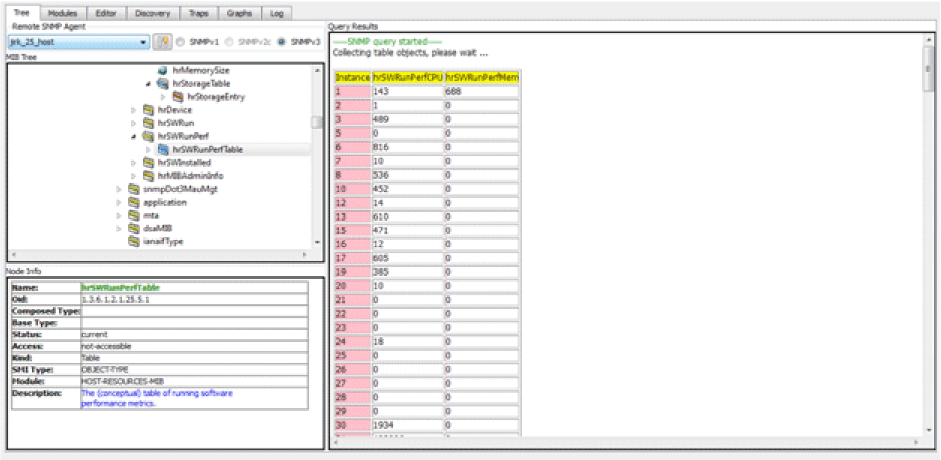
-----SNMP query started-----
Collecting table objects, please wait ...

Instance	hrSWRunIndex	hrSWRunName	hrSWRunID	hrSWRunPath	hrSWRunParam
1	1	init	zeroDotZero	init [3]	
2	2	kthreadd	zeroDotZero	kthreadd	
3	3	ksoftirqd/0	zeroDotZero	ksoftirqd/0	
5	5	kworker/u:0	zeroDotZero	kworker/u:0	
6	6	migration/0	zeroDotZero	migration/0	
7	7	watchdog/0	zeroDotZero	watchdog/0	
8	8	migration/1	zeroDotZero	migration/1	
10	10	ksoftirqd/1	zeroDotZero	ksoftirqd/1	
12	12	watchdog/1	zeroDotZero	watchdog/1	
13	13	migration/2	zeroDotZero	migration/2	
15	15	ksoftirqd/2	zeroDotZero	ksoftirqd/2	
16	16	watchdog/2	zeroDotZero	watchdog/2	
17	17	migration/3	zeroDotZero	migration/3	
19	19	ksoftirqd/3	zeroDotZero	ksoftirqd/3	
20	20	watchdog/3	zeroDotZero	watchdog/3	
21	21	cpuset	zeroDotZero	cpuset	
22	22	khelper	zeroDotZero	khelper	
23	23	netns	zeroDotZero	netns	
24	24	sync_supers	zeroDotZero	sync_supers	
25	25	bdi-default	zeroDotZero	bdi-default	
26	26	kintegrityd	zeroDotZero	kintegrityd	
27	27	kblockd	zeroDotZero	kblockd	
28	28	md	zeroDotZero	md	
29	29	khungtaskd	zeroDotZero	khungtaskd	
30	30	kswapd0	zeroDotZero	kswapd0	

Figure 132: hrSWRun

Installed software performance

HOST-RESOURCES-MIB::hrSWRunPerf - contains memory and CPU statistics on the process table from HOST-RESOURCES-MIB::hrSWRun:



Name:	hrSWRunPerfTable
Oid:	1.3.6.1.2.1.25.5.1
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Table
SMI Type:	OBJECT-TYPE
Module:	HOST-RESOURCES-MIB
Description:	The (conceptual) table of running software performance metrics.

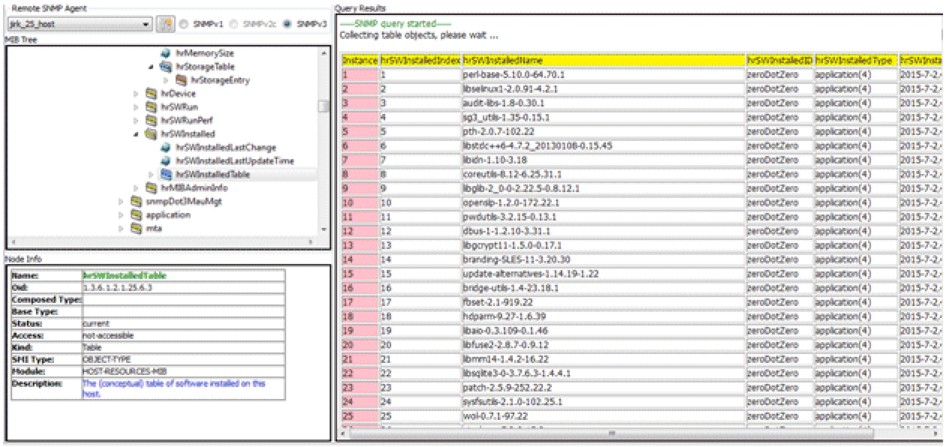
---SNMP query started---
Collecting table objects, please wait ...

Instance	hrSWRunPerfCPU	hrSWRunPerfMem
1	143	688
2	1	0
3	489	0
5	0	0
6	816	0
7	10	0
8	536	0
10	452	0
12	14	0
13	610	0
15	471	0
16	12	0
17	605	0
19	385	0
20	10	0
21	0	0
22	0	0
23	0	0
24	18	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0
30	1934	0

Figure 133: hrSWRunPerf

Installed software packages

The table hrSWInstalledTable from HOST-RESOURCES-MIB::hrSWInstalled part of mib can be used to collect information about the installed rpm packages on the OpenScape4000 host system:



Name:	hrSWInstalledTable
Oid:	1.3.6.1.2.1.25.6.3
Composed Type:	
Base Type:	
Status:	current
Access:	not-accessible
Kind:	Table
SMI Type:	OBJECT-TYPE
Module:	HOST-RESOURCES-MIB
Description:	The (conceptual) table of software installed on this host.

---SNMP query started---
Collecting table objects, please wait ...

Instance	hrSWInstalledIndex	hrSWInstalledName	hrSWInstalledID	hrSWInstalledType	hrSWInsta
1	1	perl-base-5.10.0-64.70.1	zeroDotZero	application(4)	2015-7-2,
2	2	libselinux1-2.0.91-4.2.1	zeroDotZero	application(4)	2015-7-2,
3	3	audit-libs-1.8-0.30.1	zeroDotZero	application(4)	2015-7-2,
4	4	sg3_utils-1.35-0.15.1	zeroDotZero	application(4)	2015-7-2,
5	5	pth-2.0.7-102.22	zeroDotZero	application(4)	2015-7-2,
6	6	libstdc++6-4.7.2_20130108-0.15.45	zeroDotZero	application(4)	2015-7-2,
7	7	libidn-1.10-3.18	zeroDotZero	application(4)	2015-7-2,
8	8	coreutils-8.12-6.25.31.1	zeroDotZero	application(4)	2015-7-2,
9	9	libglib-2_0-0-2.22.5-0.8.12.1	zeroDotZero	application(4)	2015-7-2,
10	10	openslp-1.2.0-172.22.1	zeroDotZero	application(4)	2015-7-2,
11	11	pwdutils-3.2.15-0.13.1	zeroDotZero	application(4)	2015-7-2,
12	12	dbus-1-1.2.10-3.31.1	zeroDotZero	application(4)	2015-7-2,
13	13	libgcrypt11-1.5.0-0.17.1	zeroDotZero	application(4)	2015-7-2,
14	14	branding-SLES-11-3.20.30	zeroDotZero	application(4)	2015-7-2,
15	15	update-alternatives-1.14.19-1.22	zeroDotZero	application(4)	2015-7-2,
16	16	bridge-utils-1.4-23.18.1	zeroDotZero	application(4)	2015-7-2,
17	17	fbset-2.1-919.22	zeroDotZero	application(4)	2015-7-2,
18	18	hdparm-9.27-1.6.39	zeroDotZero	application(4)	2015-7-2,
19	19	libaio-0.3.109-0.1.46	zeroDotZero	application(4)	2015-7-2,
20	20	libfuse2-2.8.7-0.9.12	zeroDotZero	application(4)	2015-7-2,
21	21	libmm14-1.4.2-16.22	zeroDotZero	application(4)	2015-7-2,
22	22	libsqlite3-0-3.7.6.3-1.4.4.1	zeroDotZero	application(4)	2015-7-2,
23	23	patch-2.5.9-252.22.2	zeroDotZero	application(4)	2015-7-2,
24	24	sysfsutils-2.1.0-102.25.1	zeroDotZero	application(4)	2015-7-2,
25	25	wol-0.7.1-97.22	zeroDotZero	application(4)	2015-7-2,

Figure 134: hrSWInstalled

8.1.5 Backup and Restore

The SNMP setting is part of the iso recovery image.

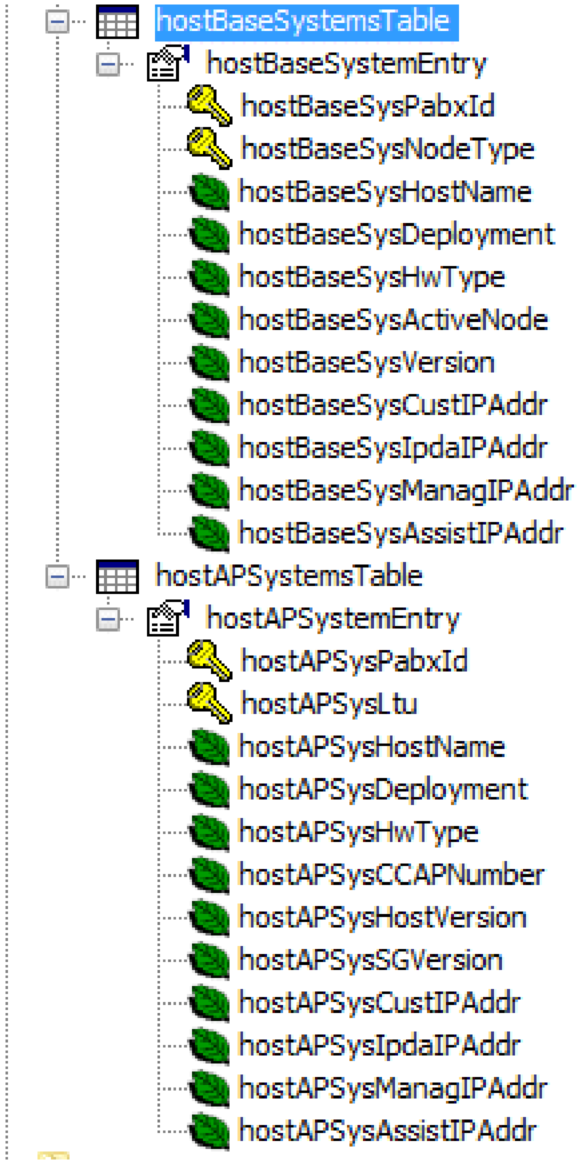
On the Assistant the SNMP setting is part of the cdb backup.

During an Assistant restore process, the data will not be distributed to the connected hosts. If required, you have to do this manually after the restore process is finished.

8.1.6 hicomMIB Enhancements

The actual hicomMIB is extended by two tables which are filled during the system discovery.

- hostBaseSystems – table with IP addresses of the 4K host systems (nodeA, nodeB, quorum nodes) that belong to the particular Assistant
- hostAPsystems – table with IP addresses and LTUs of Softgate/ SurvivableSoftgate/AP-E host systems that belong to the particular Assistant



```
hostBaseSystemsTable
  hostBaseSystemEntry
    hostBaseSysPabxId
    hostBaseSysNodeType
    hostBaseSysHostName
    hostBaseSysDeployment
    hostBaseSysHwType
    hostBaseSysActiveNode
    hostBaseSysVersion
    hostBaseSysCustIPAddr
    hostBaseSysIpdaIPAddr
    hostBaseSysManagIPAddr
    hostBaseSysAssistIPAddr
hostAPSystemsTable
  hostAPSystemEntry
    hostAPSysPabxId
    hostAPSysLtu
    hostAPSysHostName
    hostAPSysDeployment
    hostAPSysHwType
    hostAPSysCCAPNumber
    hostAPSysHostVersion
    hostAPSysSGVersion
    hostAPSysCustIPAddr
    hostAPSysIpdaIPAddr
    hostAPSysManagIPAddr
    hostAPSysAssistIPAddr
```

Figure 135: hostBaseSystemsTable / hostAPSystemsTable

8.1.6.1 hostBaseSystemsTable

The table of host systems includes the following fields:

- hostBaseSysPabxId - Unique intentifier of the 4K system usable on the 4K Manager. On the Assistant this is always 1

- hostBaseSysNodeType - Type of the 4K host node. For simplex only nodeA is used. In case of duplex on the host, the node can be nodeA,nodeB or quorum node(nodeQ)
- hostBaseSysHostName - HostName of the node
- hostBaseSysDeployment - Identification of the deployment type as text, e.g. DuplexNode, SimplexNode ...
- hostBaseSysHWType - Identification of the hardware type, e.g. VM, DSCXLv2, OSA500i, ...
- hostBaseSysActiveNode - Usable in duplex mode for the identification of the activeNode and standby nodes in time.
- hostBaseSysVersion - Version of the 4K host system.
- hostBaseSysCustIPAddr - Customer Lan IP address of the appliance.
- hostBaseSysIpdaIPAddr - IPDA LAN IP address of the appliance.
- hostBaseSysManagIPAddr - Management Lan IP address of the appliance.
- hostBaseSysAssistIPAddr - The appliances associated with the assistant IP address.

8.1.6.2 hostAPSystemsTable

The table of sofware based APs includes the following fields:

- hostAPSysPabxId - Unique intentifier of the 4K system usable on the 4K Manager. On the Assistant this is always 1
- hostAPSysLtu - LTU (Line Trunk Unit) number of the access point.
- hostAPSysHostName - HostName of the node.
- hostAPSysDeployment - Identification of the deployment type as text, .e.g StandaloneSG, SurvivableSG, ...
- hostAPSysHwType - Identification of the hardware type as text. e.g. DSCXLv2, OSA500i, VM ...
- hostAPSysCCAPNumber - APE/SurvivableSG access point number.
- hostAPSysHostVersion - Platform release version.
- hostAPSysSGVersion - SoftGate release version.
- hostAPSysCustIPAddr - Customer Lan IP address of the appliance.
- hostAPSysIpdaIPAddr - IPDA LAN IP address of the appliance.
- hostAPSysManagIPAddr - Management Lan IP address of the appliance.
- hostAPSysAssistIPAddr - The appliances associated with the assistant IP address.

8.1.7 OpenScapeFM enhancements

The OpenScape Fault Management is extended for a better understanding of the snmp trap messages generated by the host (defined in host4000 mib).

The changes in hicomMIB together with the sysDescr values from MIB2 are used by the OpenScape Fault Management autodiscovery feature; thus, by passing on the IP address of the Assistant to the OpenScape Fault Management, all connected nodes can be detected.

The Fault Management can then display all nodes in the IP view and 4000 plugin view, where the APs and their hosts will be joined.

Due to the sysDesc provided by the MIB2 agent, on each host the OpenScapeFM will also be aware of the hardware type of the AP which is required by the HPA500 Board Recognition feature.

The new app4K MIB is integrated in OSFM so that the alarms are displayed accordingly. Host-related alarms will be mapped to the corresponding IP nodes in OSFM. If the IP nodes do not exist in the OSFM database (e.g. if they could not be created automatically because of a missing IP network), the alarm will be mapped to the IP node representing the assistant. For this purpose, the IP address of the assistant will be taken from the trap variable binding.

If neither the assistant nor the host system IP node exist in the OSFM, the alarm will be displayed without being mapped to any object.

8.1.7.1 OS4K

The IP addresses of the hosts belonging to a 4K are queried, and the IP nodes are created for all host systems (only possible if the IP network already exists or the network mask can be determined via SNMP). The 4K is displayed in the OSFM topology as a container object. This container object contains the 4K (Assistant) object (which already exists in the current OSFM version) plus all related IP nodes for the host systems.

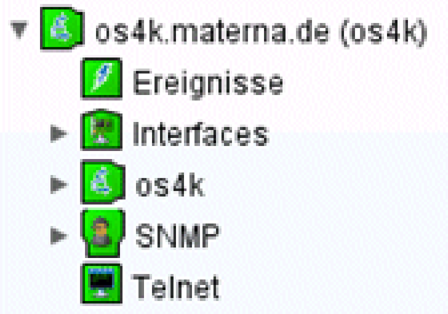


Figure 136: Display of an OS4K - Old Version

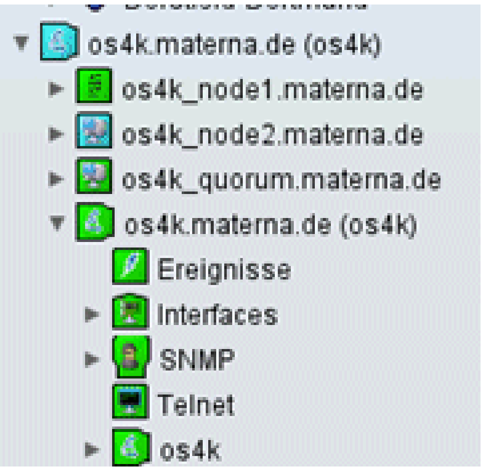


Figure 137: Display of an OS4K including Host Systems - New Version

The OS4K (os4k.materna.de) is placed into a container object with the same name which - in addition - contains the IP nodes representing the host systems (node1, node2, quorum).

There is a new menu item "Host Systems" on an OS4K object, displaying the content of the host system table textually as list.

8.1.7.2 AP/APE

The IP addresses of the AP/APEs are queried via SNMP, and an IP node is created for each address (only possible if the IP network already exists or the network mask can be determined via SNMP). The AP/APE objects are placed below their related IP nodes.

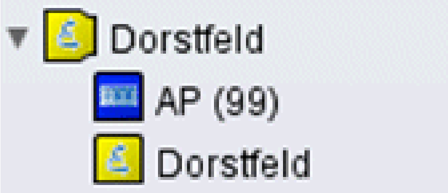


Figure 138: Representation of an AP- Old Version

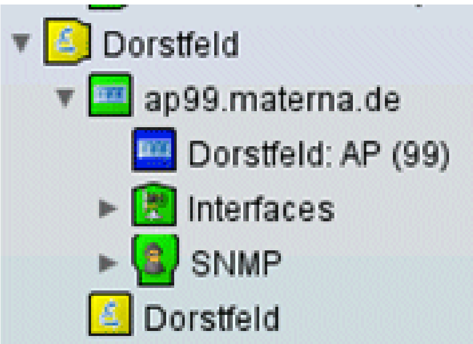


Figure 139: Representation of an AP (merged with IP Node) - New Version

8.1.7.3 Evaluation of sysDescription

The SNMP variable "sysDescription" (MIB2) of the host systems contains a string describing the hardware type of the host system. This string is appended to the symbol label in OSFM.

8.2 HPA500 Board Recognition

With this feature you can detect the HW type of an Access Point over SNMP. You can do this via hicomMIB (SNMP get request to Assistant) or via MIB2 supported by each host (SNMP get request to AP host system)

8.2.1 hicomMIB

Existing version (in V7R1):

If an hicomErrorTrap with the Fault message is generated based on an error on some AP, it includes the PEN identification.

Similarly, if an Alarm is generated and is it based on some AP problem, it includes the LTU numbers of the affected APs.

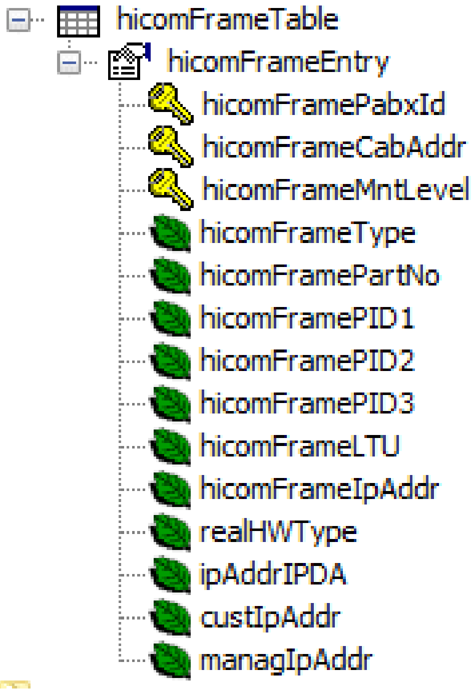
Thus, Fault Management is able to identify the affected AP.

New for V7R2:

With this feature Fault Management also knows the hardware type of the AP. Fault Management retrieves this information from the hardware agent running on the Assistant/Manager. This information is gathered by the hardware agent during the hardware discovery.

The IP addresses of the host system for the frame are also detected.

The frametable is extended with "realHardwareType" and 3 IP addresses of the frame - ipAddrIPDA, custIpAddr, managIPAddr. The new values are appended at the end of the table/OIDs.



```
hicomFrameTable
  hicomFrameEntry
    hicomFramePabxId
    hicomFrameCabAddr
    hicomFrameMntLevel
    hicomFrameType
    hicomFramePartNo
    hicomFramePID1
    hicomFramePID2
    hicomFramePID3
    hicomFrameLTU
    hicomFrameIpAddr
    realHWType
    ipAddrIPDA
    custIpAddr
    managIpAddr
```

Figure 140: hicomFrameTable

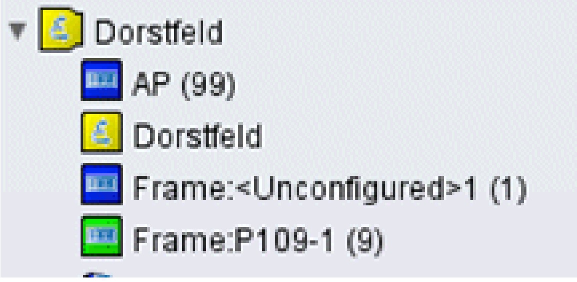
- ipAddrIPDA - the IP address from the AP host system used from the IPDA interface.
- custIPAddr - The IP Address of the Portal of the Standalone SG (this is an optional configuration parameter).
- managIPAddr - The management IP address of the SG configured via AMO STMIB plus SG WBM for the LAN Interface to be used (this is an optional configuration parameter).

8.2.2 MIB2

The NMS which is unaware of how to use hicomMIB and its discovery processes can gather the HW information from the sysDescr of the mib2agent running on each host.

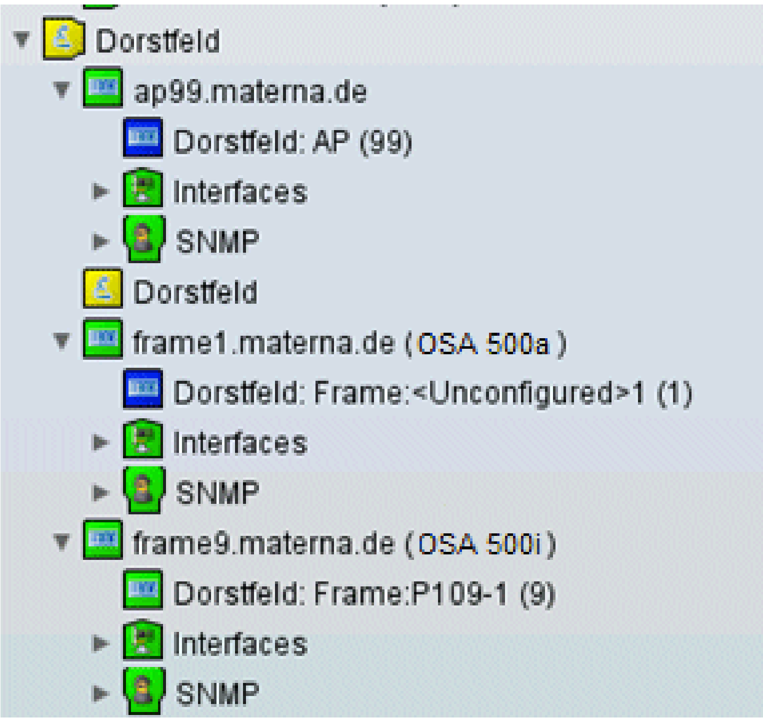
8.2.3 OSFM Enhancement

OSFM displays the "realHardwareType" of a frame as a label extension for the related IP node of the frame. In addition, an IP node is created for the IP address of the frame (only possible if the IP network already exists or the network mask can be determined via SNMP). The frame object is merged with the related IP node object (the frame object will be located below the IP node object).



```
▼ Dorstfeld
    AP (99)
    Dorstfeld
    Frame:<Unconfigured>1 (1)
    Frame:P109-1 (9)
```

Figure 141: Representation of Frames in OSFM- Old Version



```
▼ Dorstfeld
    ▼ ap99.materna.de
          Dorstfeld: AP (99)
        ▶ Interfaces
        ▶ SNMP
      Dorstfeld
    ▼ frame1.materna.de (OSA 500a )
          Dorstfeld: Frame:<Unconfigured>1 (1)
        ▶ Interfaces
        ▶ SNMP
    ▼ frame9.materna.de (OSA 500i )
          Dorstfeld: Frame:P109-1 (9)
        ▶ Interfaces
        ▶ SNMP
```

Figure 142: Representation of ames in OSFM (Frame Object merged with IP Node) - New Version

8.3 Representation of Frames in OSFM

With this feature you can:

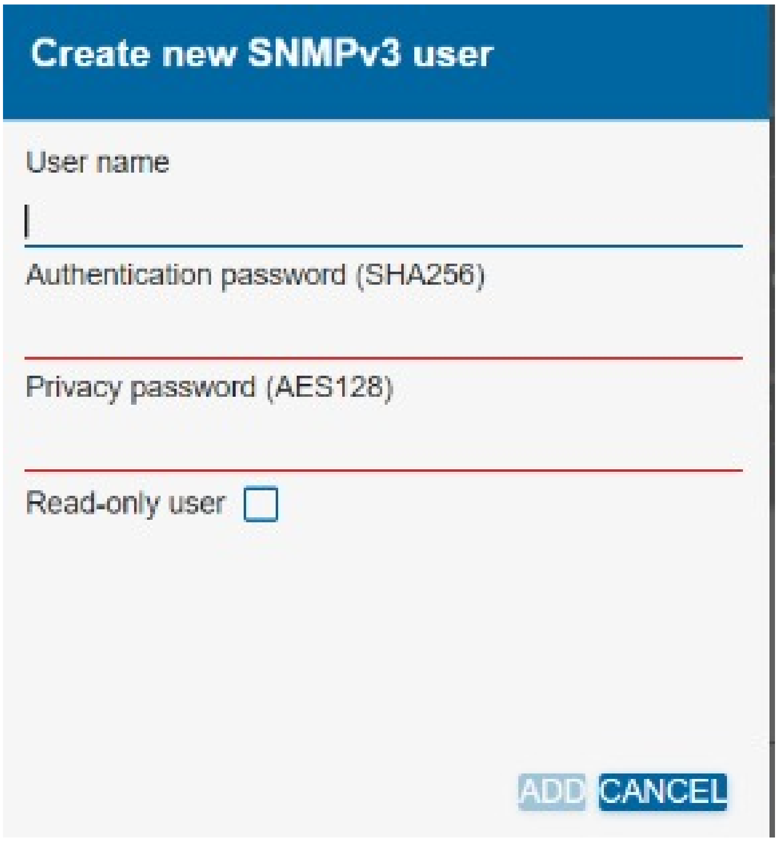
- Save and distribute the SNMPv3 configuration (including filter and keep-alive setup) to all hosts of all machines in the OpenScape4000 area from the Assistant (IPDA based AP-Es are not covered, you have to use the Assistant on an IPDA-based AP-E to configure SNMP on the host).

- Save and distribute the SNMPv3 configuration (including filter and keep-alive setup) to all hosts of all machines in the OpenScape4000 area from the Manager (IPDA-based AP-Es are covered, you have to use the Assistant on an IPDA-based AP-E to configure SNMP on the host).
- Reset the alarms on all/selected systems (including Assistant/Manager alarms from alarm group 7)
- Use the Gateway Dashboard on the Assistant to see and save the SNMPv1 configuration parameters on the list of the IP gateways.
- Use the Gateway Dashboard on the Assistant to change the QoS data collection (QDC) settings on the list of IP gateways.

8.3.1 SNMPv3 Configuration on the Assistant

8.3.1.1 Define the SNMPv3 User for the Hosts

You can use the Assistant SNMP Configurator to define whether a particular SNMPv3 user definition with its trap destination shall be configured on all hosts.



Create new SNMPv3 user

User name

Authentication password (SHA256)

Privacy password (AES128)

Read-only user ☐

Figure 143: SNMP Configurator - Configure on all Hosts

Such a user (including the trap destinations assigned into this user) will be configured as a read-only user on all host systems during the distribution of the configuration.

8.3.1.2 Define the SNMP Control Parameters for all Hosts

see SNMP Control Parameters

8.3.1.3 Define the SNMP Filter for all Hosts

see Trap Filters

8.3.1.4 Distribute the SNMPv3 Users Setup to Hosts

see Distribution to Hosts

8.3.1.5 Reset all Alarms

see Reset All Alarms Raised on RMX or Assistant

8.3.2 SNMPv3 Configuration on the Manager

Using the SNMP Configurator on the Manager, you can create SNMP Profiles (domains). Each SNMP profile has it's own own SNMP setting like SNMPV3 Users, SNMPV1 Communities, Trap Destinations, Trap Filters (including host trap filtering and filtering Fxxxx messages from RMX) and SNMP Control parameters.

Each SNMP profile has a list of OpenScape 4000 V7R2 systems (Adding an OpenScape 4000 into a Profile - it can be also the OpenScape4000 of an IPDA-based AP-E) where this SNMP setup shall be applied. (Therefore, everything that can be defined in the Assistant SNMP Configurator can be defined in the profile on the Manager.)

If you have created a profile on the Manager, you can start the distribution of this profile to the Assistants listed in the given profile.

In the Distribute Configuration dialog you can select the profiles you want to distribute. You can also select the behavior of the distribution for each profile – i.e. whether the Assistant shall also distribute the data to all hosts and - if so - select the distribution arguments like in the Assistant Distribute Configuration window.

You can monitor the progress of the distribution in the Distribute Configuration dialog y.

You can also Reset all Alarms for all connected systems via one click from the Manager.

8.3.2.1 SNMP Profiles

Using the SNMP Configurator, you can create/select/edit/delete SNMP configuration profiles.

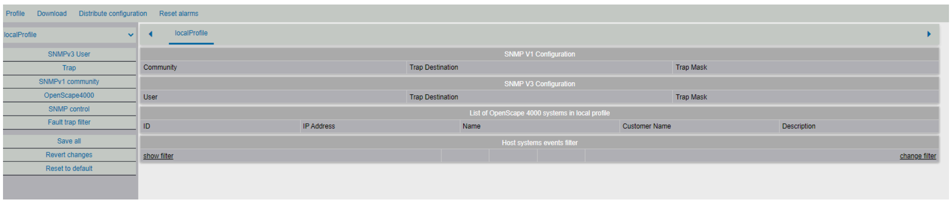


Figure 144: SNMP Configuration Manager

By default there is a local profile on the Manager which can be edited by the user; this profile will be used as the SNMP configuration on the Manager. The local profile cannot be deleted.

Each profile includes:

- A set of the defined SNMPv1/v3 configuration (SNMPV1 Communities, SNMPV3 Users, Trap Destinations)
- The SNMP Control settings
- The Fault Trap Filter (also including the filter for app4Kmib used by the 4K hosts)
- A List of Assistants (Adding an OpenScape 4000 into a Profile) to which the profile is to be distributed

You can select a profile by choosing from a combo box or directly by clicking on the profile name and delete a profile by selecting Profile -> Delete.

SNMPV3 Users

Using the menu on the left side (SNMPv3 User->Add/Change/Remove) you can add/change/remove SNMPv3 users to/from the profile.

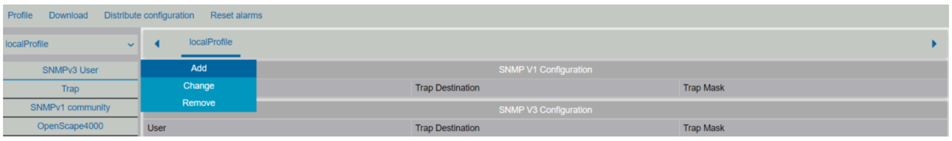
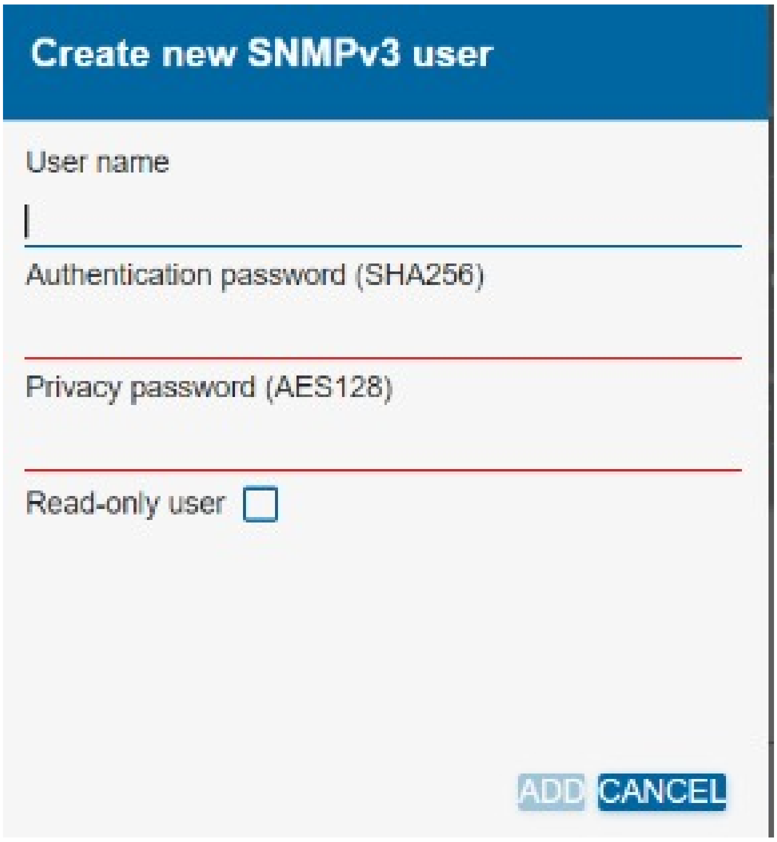


Figure 145: Add/Change/Remove SNMP3 User

One profile can contain several users. An SNMPv3 user is represented by its name and contains two passwords (authentication and privacy password). By default, the SNMPv3 user is created for read/write access. This can be changed by check the option 'Read-only user'.



Create new SNMPv3 user

User name

Authentication password (SHA256)

Privacy password (AES128)

Read-only user □

Figure 146: Create new SNMPv3 User

SNMPV1 Communities

You can add/remove a community into the profile using the left side menu: SNMPv1 community->Add/Remove.

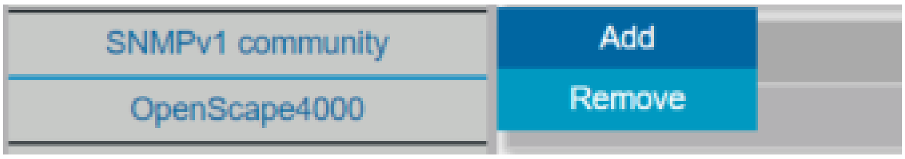
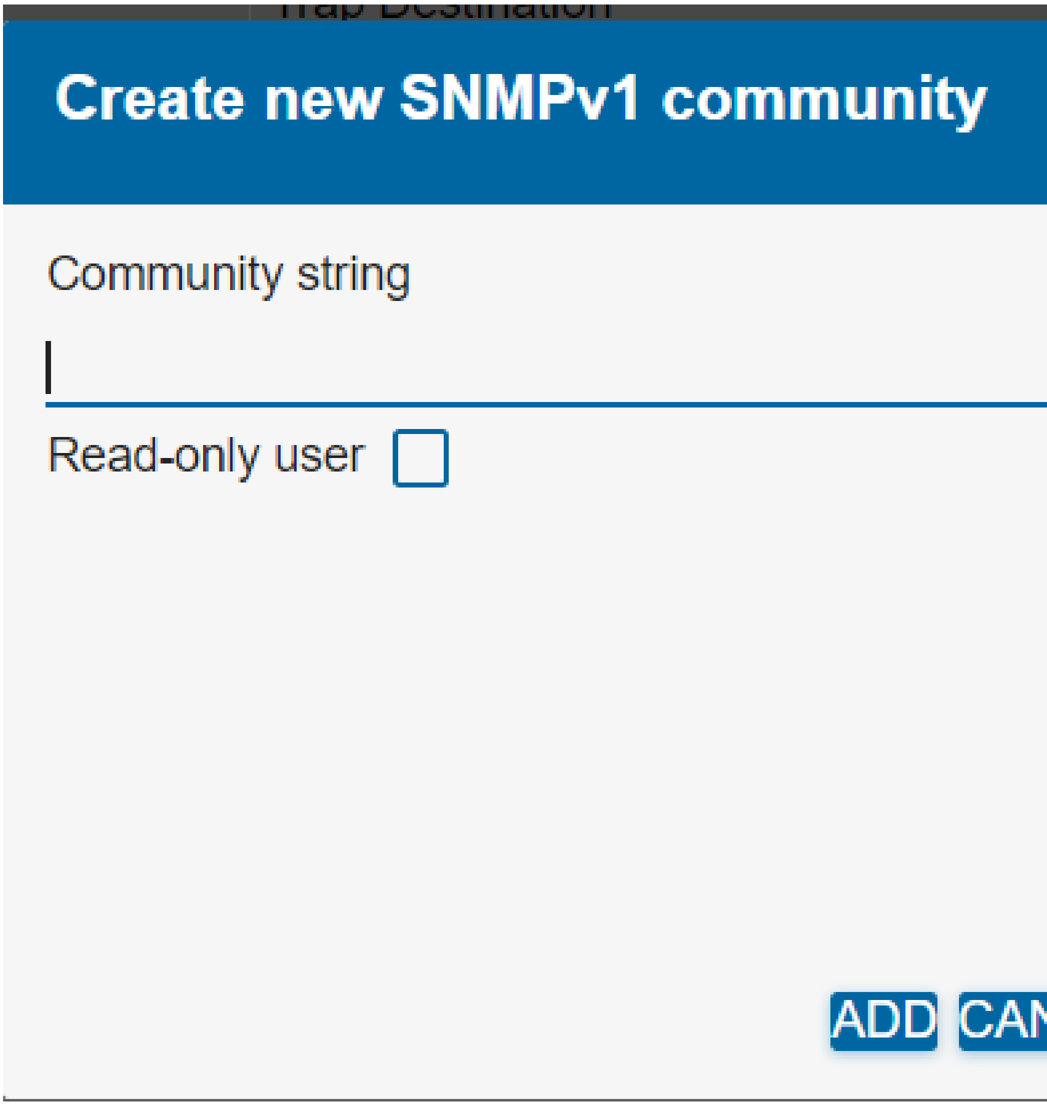


Figure 147: Add/Remove SNMPv1 Community

One profile can contain several communities. Ab SNMPv1 community is represented by its name and can also be read-only.



Trap Destination

Create new SNMPv1 community

Community string

Read-only user □

Figure 148: Create new SNMPv1 Community

Trap Destinations

Using the left side menu (Trap->Add), you can add a new trap destination. You can also use Trap->Remove from the left side menu to remove a defined trap destination.

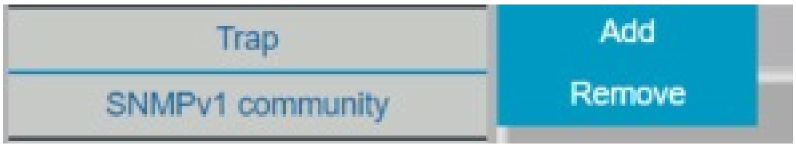


Figure 149: Add/Remove Trap

The IP address for a trap destionation has to be associated with a user/community which is used during the sending of SNMP trap to the defined destination. One user/community can be used to send traps to several trap destinations.

8.3.2.2 Create new Trap - Adding an OpenScape 4000 into a Profile

By adding an OpenScape 4000 into a profile you can specify that you want to use the SNMP configuration defined in the profile on this OpenScape 4000 system.

You can add an OpenScape 4000 into a profile as follows:

1) Select the profile (using the combo box or from the tabsheet).

2) Use the left side menu OpenScape 4000 -> Move to profile.

3) Select the system that is to be moved into the selected profile and click the MOVE button.

One OpenScape 4000 system can only be included in one profile at any given time. If an OpenScape 4000 is moved to a profile, it is automatically removed from its last profile.

8.3.2.3 SNMP Control

Using the 'SNMP control' option from the left side menu you can define the behavior of the SNMP error agent running on the OpenScape 4000 Assistant/ Manager.

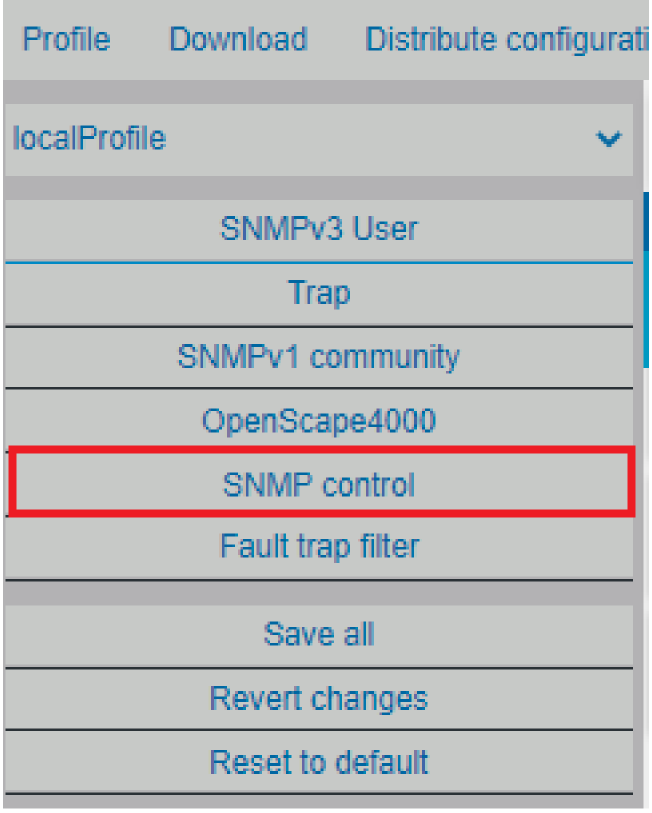
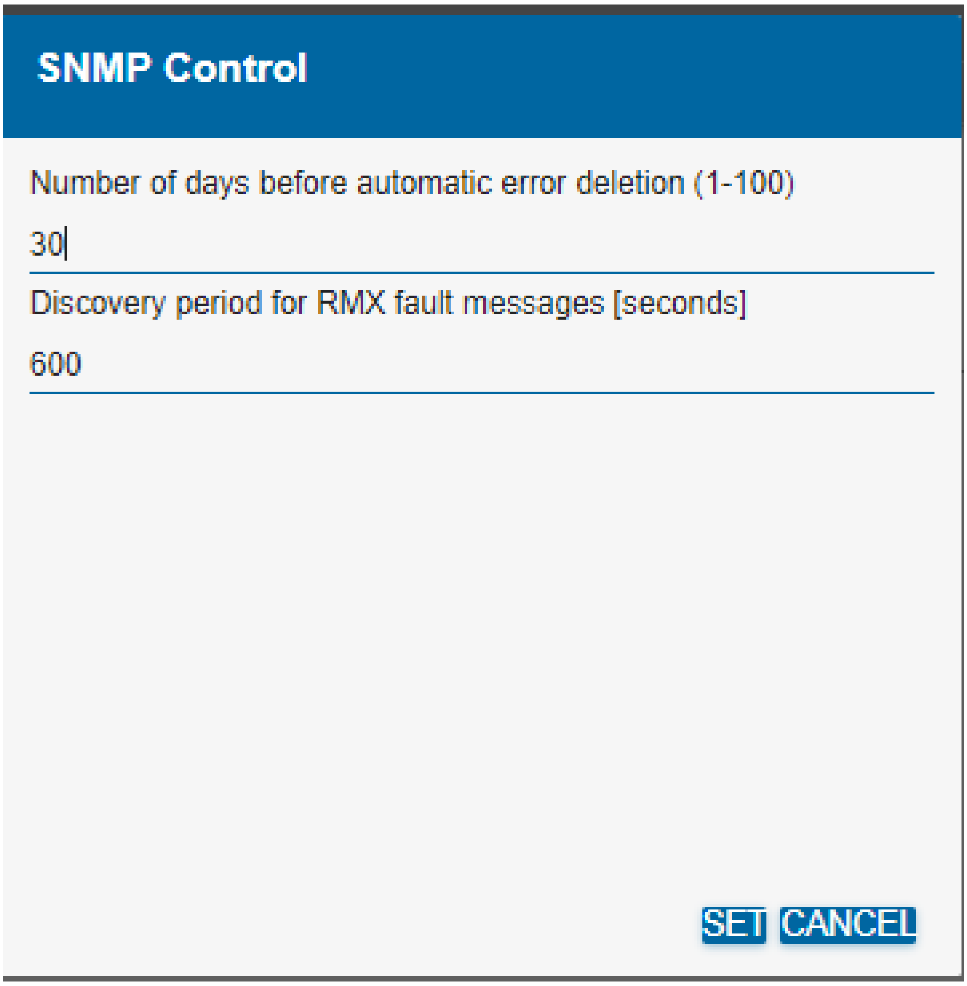


Figure 150: SNMP Control Menu Item

The following values can be set:

Number of days before automatic error deletion - Any RMX Fxxxx messages older than the specified number of days will be automatically deleted from the database (lerror table).

Discovery period for RMX - The RMX error faults are polled by default each 10 minutes, and error traps are geneated if new faults are discovered. You should change this value if the delay of received traps on your NMS or on your trap receiver is too long for your requirements. The minimum poll value is 30 seconds.



SNMP Control

Number of days before automatic error deletion (1-100)

30

Discovery period for RMX fault messages [seconds]

600

Figure 151: SNMP Control Dialog

8.3.2.4 RMX Faults Trap Filter & Host System Events Filter

In each profile you can define filtering for:

- Fxxxx messages send by RMX via the Assistant/Manager SNMP engine as hicomErrorMsg traps (from hipath4000.mib)
- Host system events (from app4K.mib) send by each host system in the 4K area

Fault Trap Filter

Using the 'Fault trap filter' option from the left side menu you can select which Fxxxx message should be filtered.

Figure 152: Fault Trap Filter Menu Item

By default all Fxxxx messages are enabled.

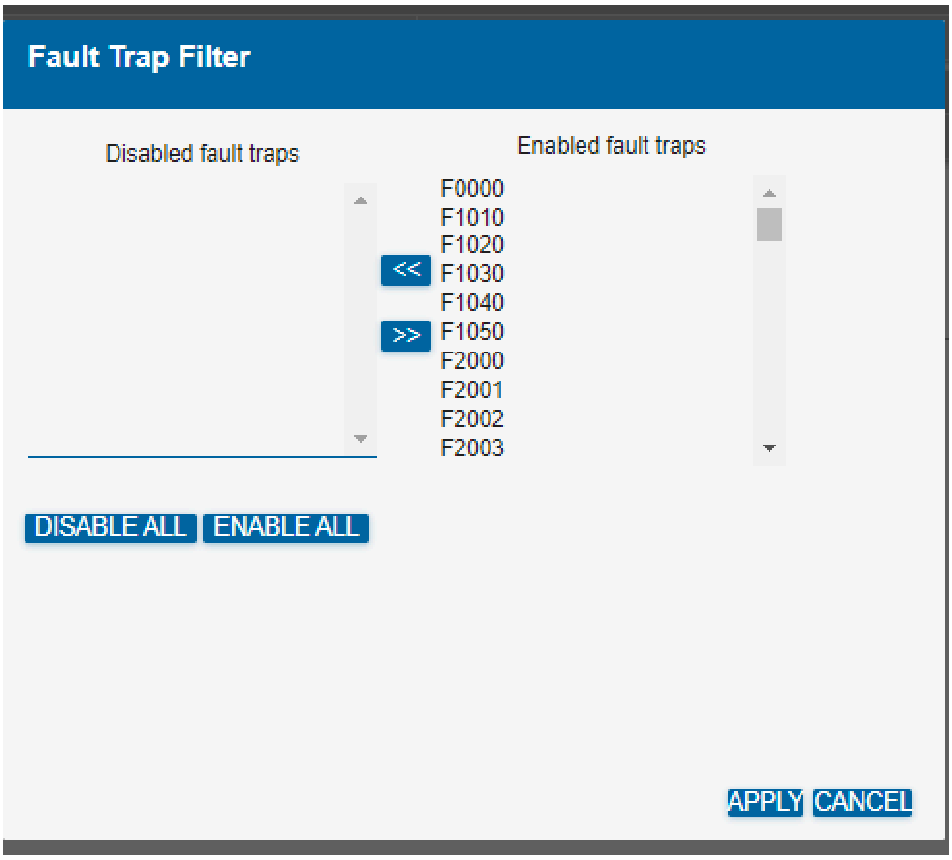


Figure 153: Fault Trap Filter Dialog

Host System Events Filter

You can show/hide the filter defined for the profile in the Host Systems Events Filter part by clicking on 'show filter':

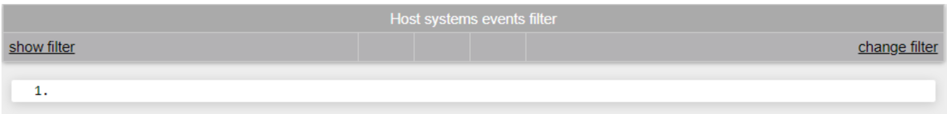
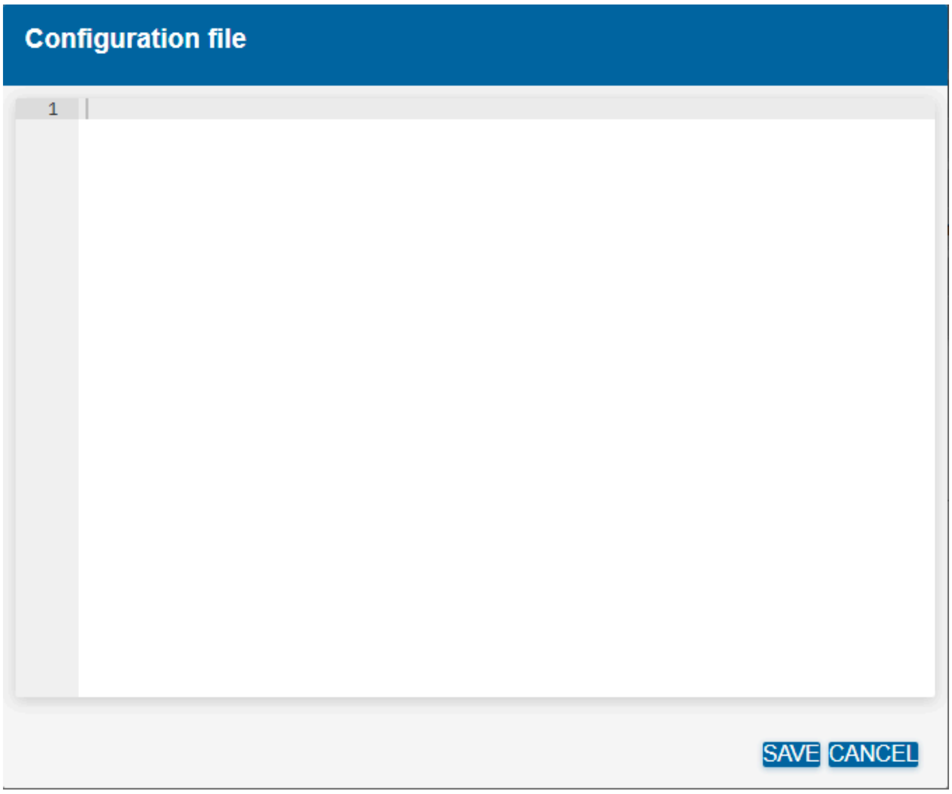


Figure 154: Host System Events Filter

You can change the filter by clicking on 'change filter'.



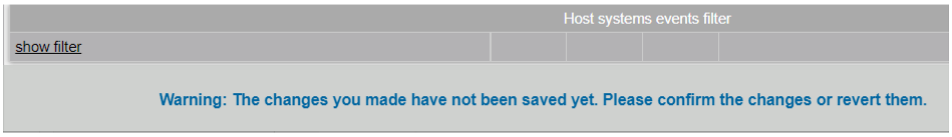
Configuration file

```
1
```

Figure 155: Host System Events Filter Dialog

8.3.2.5 Saving/Reverting Changes

As soon as changes have been made, you are informed by a yellow warning text at the bottom of the page:



Warning: The changes you made have not been saved yet. Please confirm the changes or revert them.

Figure 156: Warning Text

As long as the changes have not been saved, they are only kept in the browser; if you close the browser window without saving your changes, all the changes are lost.

You can choose to:

- Save All Changes
- Revert All Changes
- Reset to Default

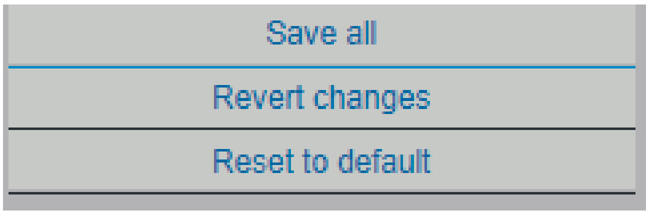


Figure 157: Save/Revert/Reset Menu

Save All Changes

If you click on the 'Save all' option from the left side menu, all the changes made in the SNMP Configuration Manager are saved to the Manager's database.

The changes made in the local profile are also saved into the Manager's SNMP engine.

Revert All Changes

If you click on the 'Revert changes' option from the left side menu, all the changes made since the last save operation are deleted - it is same action like closing the browser window.

Reset to Default

If you click on the 'Reset to default' option from the left side menu and then select 'RESET SELECTED', you can reset selected (or all) profiles into a clean (default) state; all data defined in the profile are deleted from the Manager database.

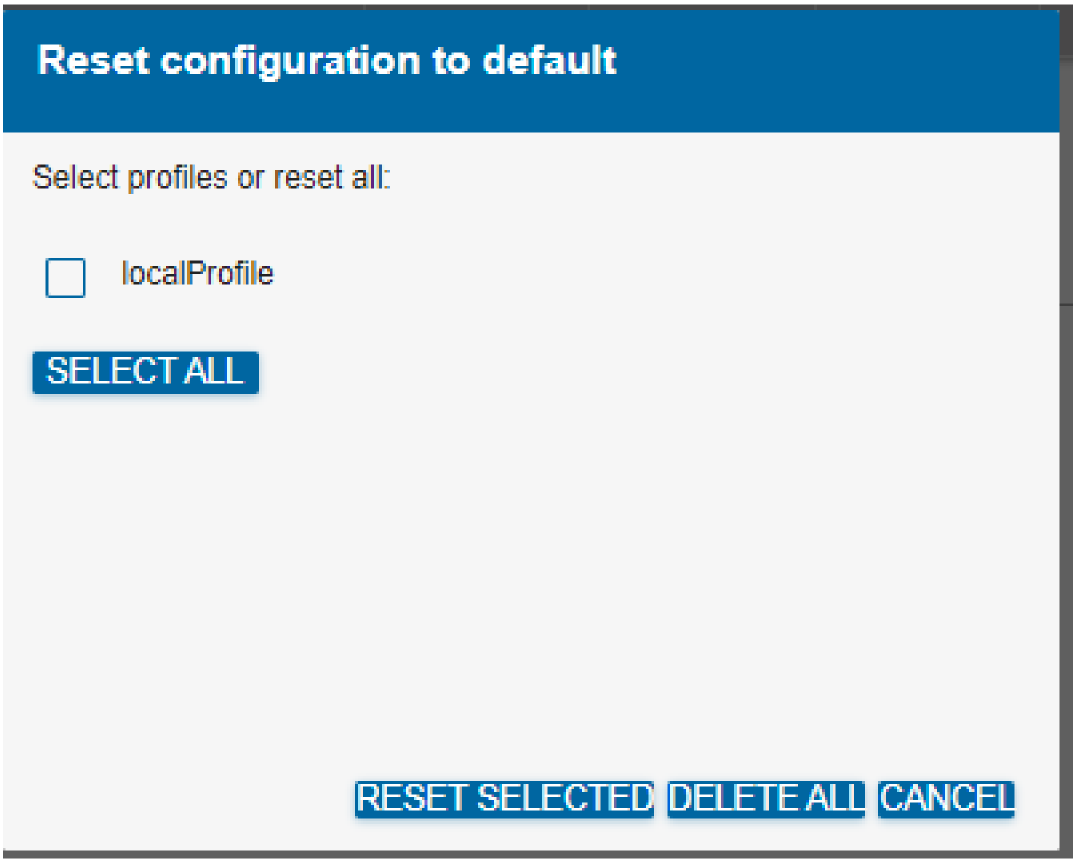


Figure 158: Restore Configuration to Default Dialog

The 'DELETE ALL' button also deletes all profile and all settings from the local profile; if you use this option, you go back to the state right after a fresh system installation.

8.3.2.6 Download

Using the 'Download' option from the upper menu, you can download all MIBs supported by the OpenScape 4000 systems:

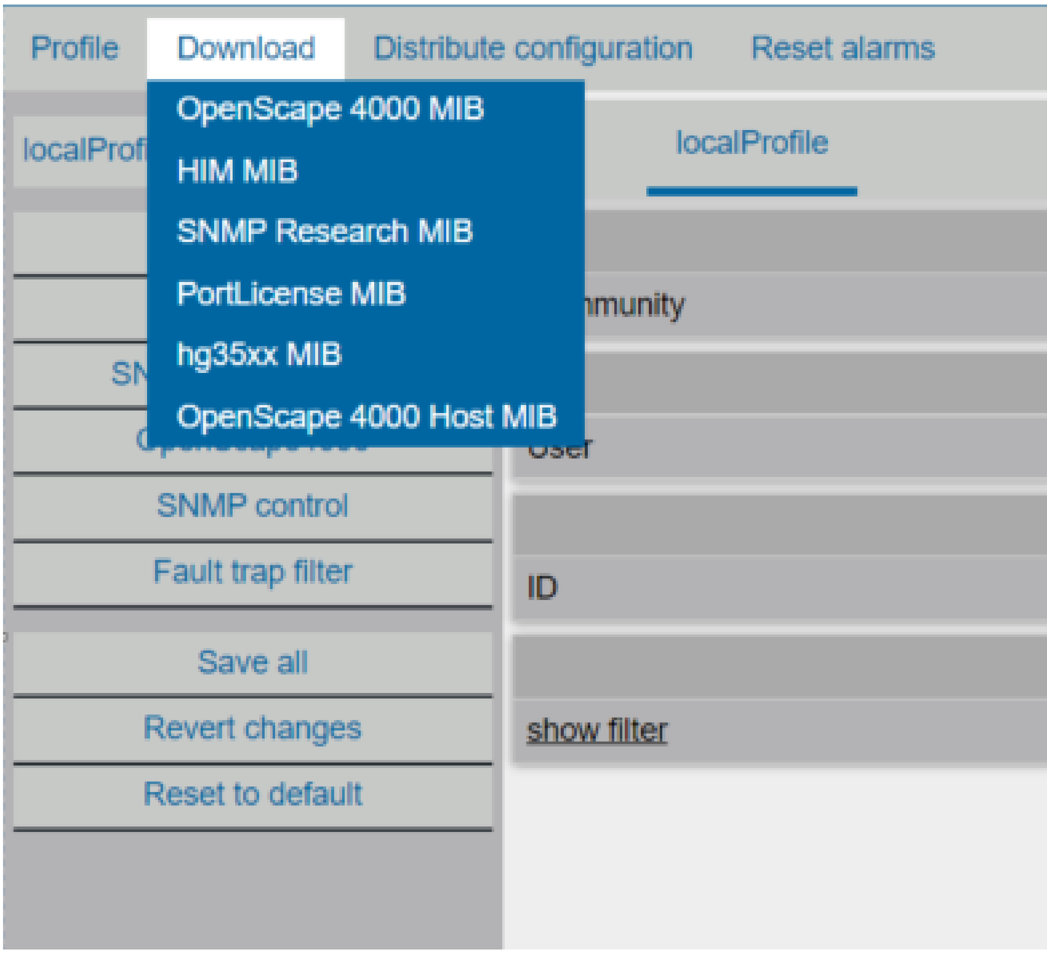


Figure 159: Download Menu

8.3.2.7 Distribute Configuration

Using the 'Distribute configuration' option from the upper menu, you initiate the distribution of the configuration specified in the profile to the OpenScape 4000 Assistants and all hosts (active, standby, quorum, softgates ...) connected to the given OpenScape 4000 system.

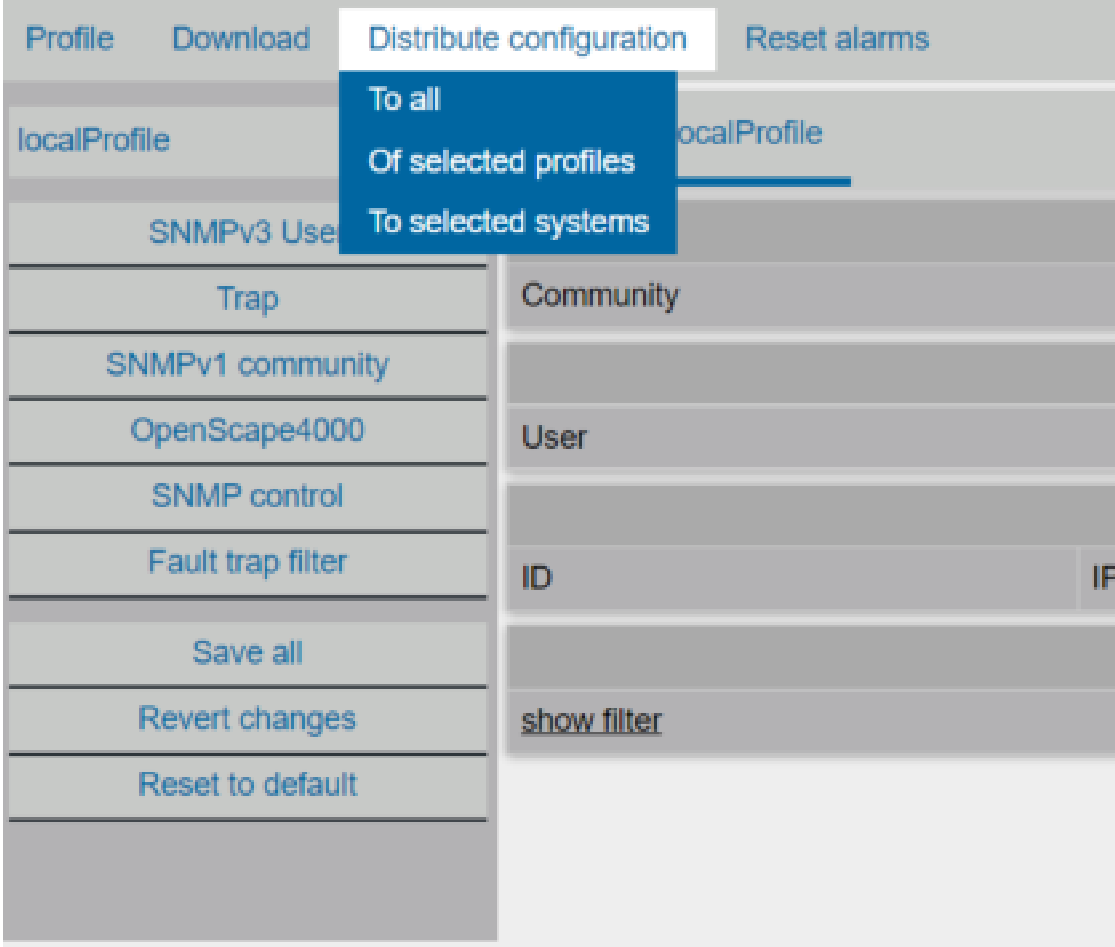


Figure 160: Distribute Configuration Menu

You can distribute the configuration to:

- all systems
- selected systems from the complete set
- all systems of selected profiles

For each system/profile, you can select what to distribute:

- SNMP configuration (users, communities, traps)
- Trap filter configuration (host events filter and RMX Fxxxx filter)
- SNMP control parameters (error deletion interval and error discovery period setting)

The distribution usually takes quite a bit of time so you can display the progress status by opening the Distribution dialog again. The distribution can be in one of these states: not launched yet, running, cancelled, finished OK, finished with error.

You cannot start a distribution again which is in running status.

8.3.2.8 Reset Alarms

You can reset the alarms of the systems. This action has no additional impact as distributing configuration has. You can reset:

- all alarms
- the alarms for the selected system.

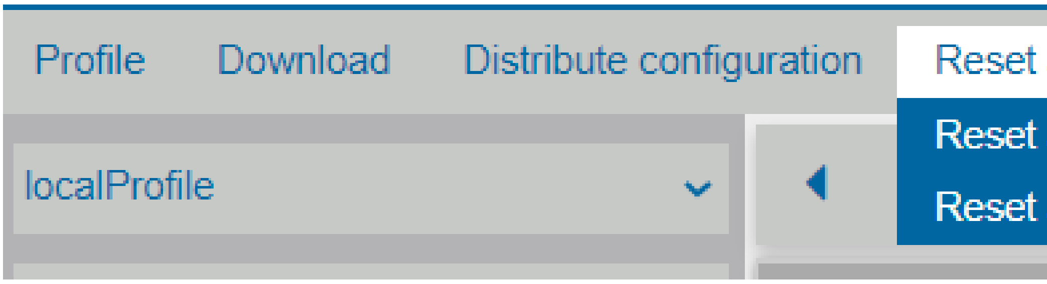


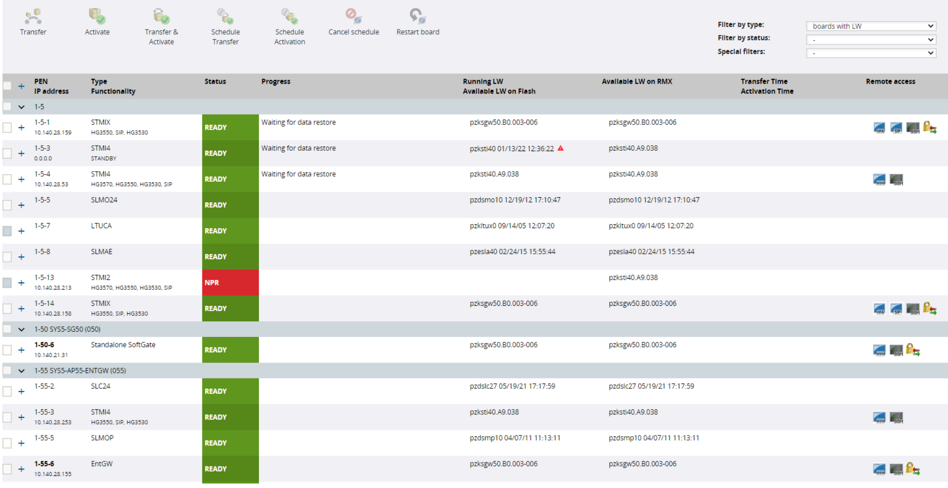
Figure 161: Reset Alarms on Selected Systems

The status of resetting alarms can be seen in the 'Last status' column (not launched yet, running, cancelled, finished OK, finished with error). Resetting an alarm of a given system cannot be executed until the previous status of the alarm reset is in running state.

8.3.3 Configuration for Gateways

Using this feature you can use the Gateway Dashboard to:

- change the SNMPv1 configuration on a list of selected IP gateways
- change the QoS collection data (QDC) setting on a list of selected IP gateways



Filter by type: boards with LW
Filter by status: -
Special filters: -

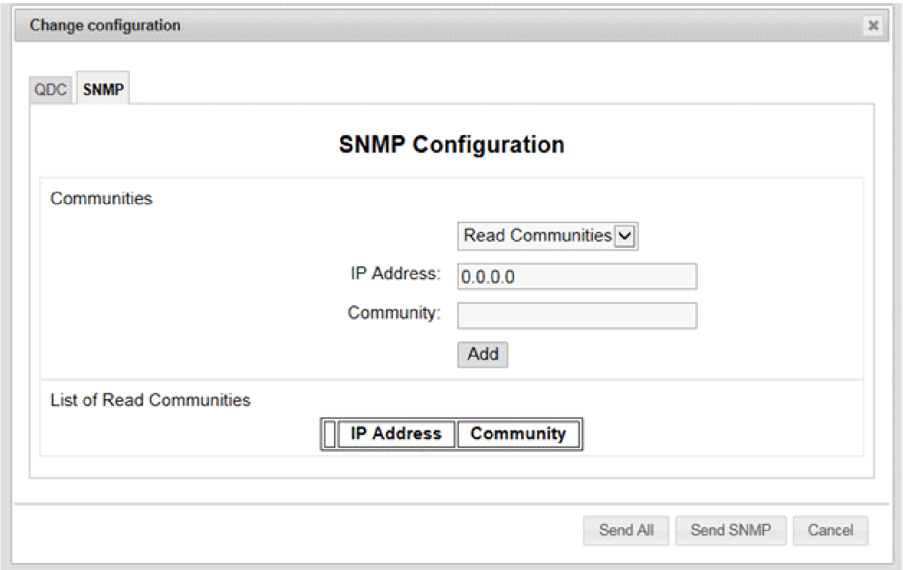
PEN IP address	Type Functionality	Status	Progress	Running LW Available LW on Flash	Available LW on RMX	Transfer Time Activation Time	Remote access
1-5							
1-5-1 10.140.28.159	STMIX HG3550, SIP, HG3530	READY	Waiting for data restore	pzksgw50.B0.003-006	pzksgw50.B0.003-006		HFA SIP SSH 🔒
1-5-3 0.0.0.0	STMI4 STANDBY	READY	Waiting for data restore	pzksti40 01/13/22 12:36:22 ⚠	pzksti40.A9.038		
1-5-4 10.140.28.53	STMI4 HG3570, HG3550, HG3530, SIP	READY	Waiting for data restore	pzksti40.A9.038	pzksti40.A9.038		WBM SSH
1-5-5	SLMO24	READY		pzdsmo10 12/19/12 17:10:47	pzdsmo10 12/19/12 17:10:47		
1-5-7	LTUCA	READY		pzkltux0 09/14/05 12:07:20	pzkltux0 09/14/05 12:07:20		
1-5-8	SLMAE	READY		pzesla40 02/24/15 15:55:44	pzesla40 02/24/15 15:55:44		
1-5-13 10.140.28.213	STMI2 HG3570, HG3550, HG3530, SIP	NPR			pzksti40.A9.038		
1-5-14 10.140.28.158	STMIX HG3550, SIP, HG3530	READY		pzksgw50.B0.003-006	pzksgw50.B0.003-006		HFA SIP SSH 🔒
1-50 SYS5-SG50 (050)							
1-50-6 10.140.21.31	Standalone SoftGate	READY		pzksgw50.B0.003-006	pzksgw50.B0.003-006		WBM SSH 🔒
1-55 SYS5-AP55-ENTGW (055)							
1-55-2	SLC24	READY		pzdslc27 05/19/21 17:17:59	pzdslc27 05/19/21 17:17:59		
1-55-3 10.140.28.253	STMI4 HG3550, SIP, HG3530	READY		pzksti40.A9.038	pzksti40.A9.038		WBM SSH
1-55-5	SLMOP	READY		pzdsmp10 04/07/11 11:13:11	pzdsmp10 04/07/11 11:13:11		
1-55-6 10.140.28.155	EntGW	READY		pzksgw50.B0.003-006	pzksgw50.B0.003-006		WBM SSH 🔒

Figure 162: Gateway Dashboard

8.3.3.1 Changing Configuration

As soon as you have selected some boards, you can use the 'Change configuration' button to get to the configuration widget, where you can:

- Setup the SNMP configuration - in the same way as from the web-based management of hardware-based gateways



SNMP Configuration

Communities

Read Communities

IP Address: 0.0.0.0

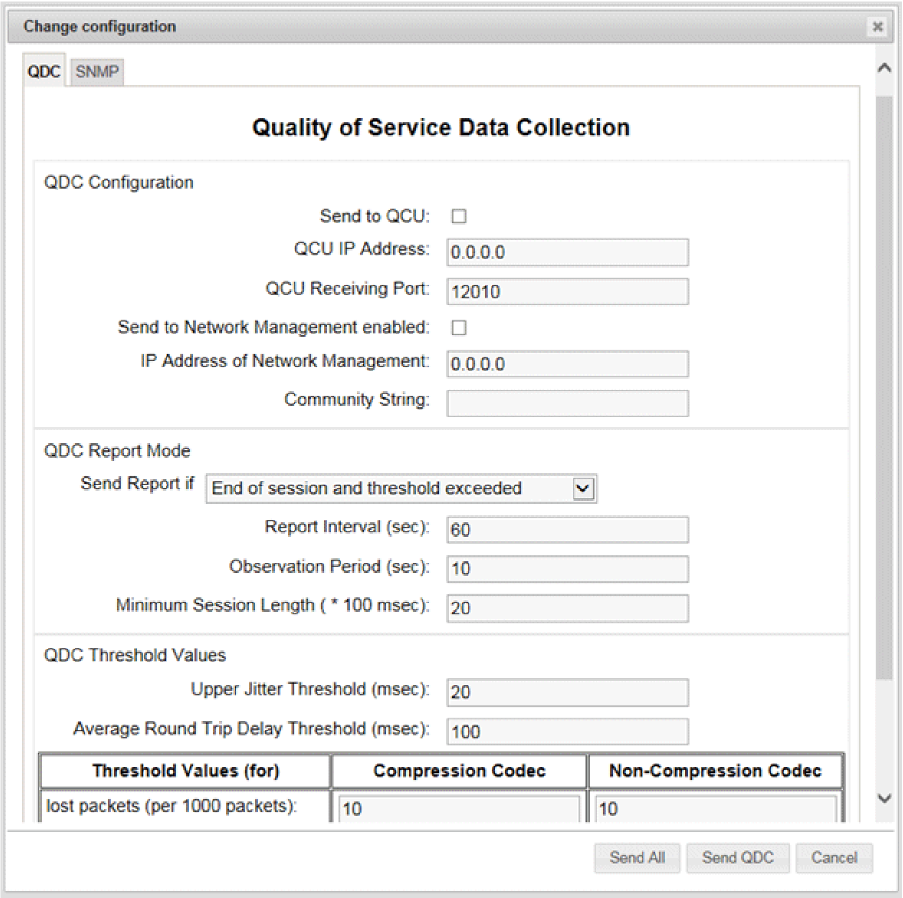
Community:

List of Read Communities

	IP Address	Community

Figure 163: Change Configuration Dialog

- Change the QDC data - in the same way as from the web-based management of the gateway



Quality of Service Data Collection

QDC Configuration

Send to QCU: □

QCU IP Address: 0.0.0.0

QCU Receiving Port: 12010

Send to Network Management enabled: □

IP Address of Network Management: 0.0.0.0

Community String:

QDC Report Mode

Send Report if End of session and threshold exceeded

Report Interval (sec): 60

Observation Period (sec): 10

Minimum Session Length (* 100 msec): 20

QDC Threshold Values

Upper Jitter Threshold (msec): 20

Average Round Trip Delay Threshold (msec): 100

Threshold Values (for)	Compression Codec	Non-Compression Codec
lost packets (per 1000 packets):	10	10

Figure 164: Change Configuration Dialog

Once the changes have been committed, they are saved and sent to all boards selected ('saved' means that the new configuration replaces the current board configuration). If you selected a board that does not support such a configuration, the configuration of this board is simply skipped.

You can commit:

- QDS changes only by clicking on the 'Send QDC' button
- SNMP changes only by clicking on the 'Send SNMP' button
- QDC and SNMP changes by clicking on the 'Send All' button

8.4 Forwarding Manager Alarms from the OpenScape 4000 Assistant to the OpenScape 4000 Manager

The OpenScape 4000 Assistant is able to raise alarms relevant to the OpenScape 4000 Assistant software (local Assistant alarms of class group 7 - so-called Manager Alarms). These alarms are using the general data trap model from the HiPath4000.mib (the same as for alarms raised by the AFR on RMX). However, these alarms are reported by the Assistant SNMP engine only (the AFR on RMX can be configured to report alarms also on the OS4K Manager).

WIth this new feature, available as of Assistant V7R2, the alarms of the Assistant can be sent as SNMP traps and managed from the OpenScape 4000 Manager.

You can now:

- receive alarms raised by the OS4K Assistant as SNMP trap from the OS4K Manager
- upload the OS4K Assistant alarm statuses from the OS4K Assistant cache (database) to the OS4K Manager database (alarm table) via an SNMP set request on the Manager
- reset an alarm on the OS4K Assistant via an SNMP set request on the OS4K Manager

To enable this feature, you have to add (uncommented) the following 2 options to the file /opt/ncc/bin/options on the OS4K Manager:

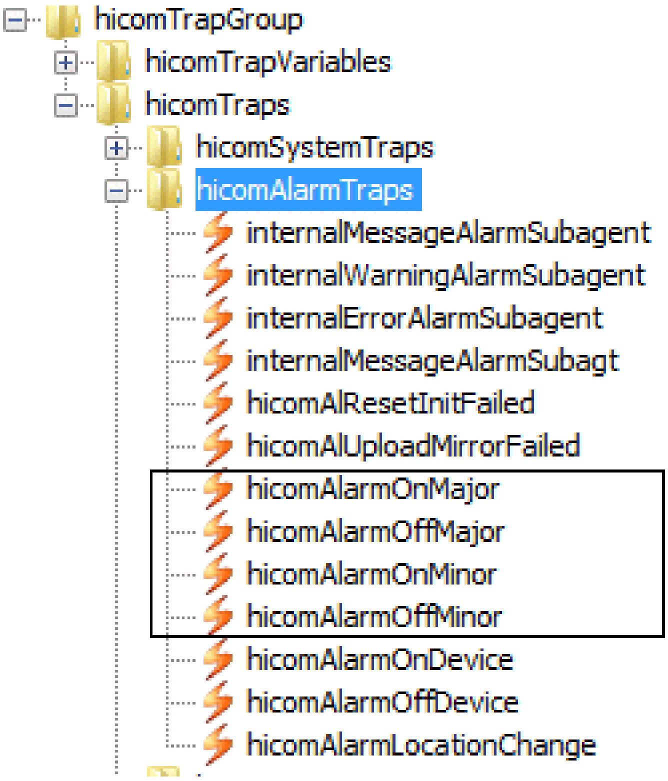
```
STORE_LOG=ON; export STORE_LOG
MANAGER_TRAP=ON; export MANAGER_TRAP
```

and add (uncommented) the following option on the OS4K Assistant to the file /opt/ncc/bin/options:

```
STORE_LOG=ON; export STORE_LOG
```

8.4.1 Receive Alarms Raised by the OS4K Assistant from the OS4K Manager

Based on severity, you can receive the following alarm messages of the HiPath4000.mib from the OS4K Manager:



- hicomTrapGroup
  - hicomTrapVariables
  - hicomTraps
    - hicomSystemTraps
    - hicomAlarmTraps
      - internalMessageAlarmSubagent
      - internalWarningAlarmSubagent
      - internalErrorAlarmSubagent
      - internalMessageAlarmSubagt
      - hicomAlResetInitFailed
      - hicomAlUploadMirrorFailed
      - hicomAlarmOnMajor
      - hicomAlarmOffMajor
      - hicomAlarmOnMinor
      - hicomAlarmOffMinor
      - hicomAlarmOnDevice
      - hicomAlarmOffDevice
      - hicomAlarmLocationChange

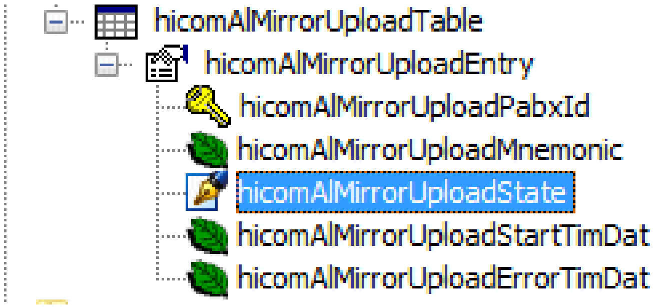
Figure 165: hicomAlarmTraps

Each trap has variable bindings that can be used to identify the source (Assistant) and type of the problem:

- hicomAlTrpSysPabxId ... pabxid from hicomSysTable (available via SNMP .1.3.6.1.4.1.231.7.2.1.1.3) of the OS4K Assistant configured on the OS4K Manager System Management
- hicomAlTrpSysMnemonic ... ID of the system specified in the System Management of OS4K Manager
- hicomAlGroup ... 7 for so-called Manager alarms
- hicomAlSubId ... numeric ID of the alarm (1 - 116)
- hicomAlPriority ... severity of alarm (1 - minor, 2 - major) - redundant value - severity can be gathered from the trap name
- hicomAlAbsMod ... the part of the Assistant raising the alarm
- hicomAlStatus ... the status of the alarm (1 - reset/off, 2 - set/on) - redundant value - severity can be gathered from the trap name
- hicomAlTimDat ... timestamp (unix epoch time)
- hicomAlName ... textual description of the alarm

8.4.2 Upload Assistant Alarms to the Manager

If you want to synchronize the Assistant alarms with the OS4K Manager database, you can achieve this via an SNMP set request executed on the OS4K Manager:



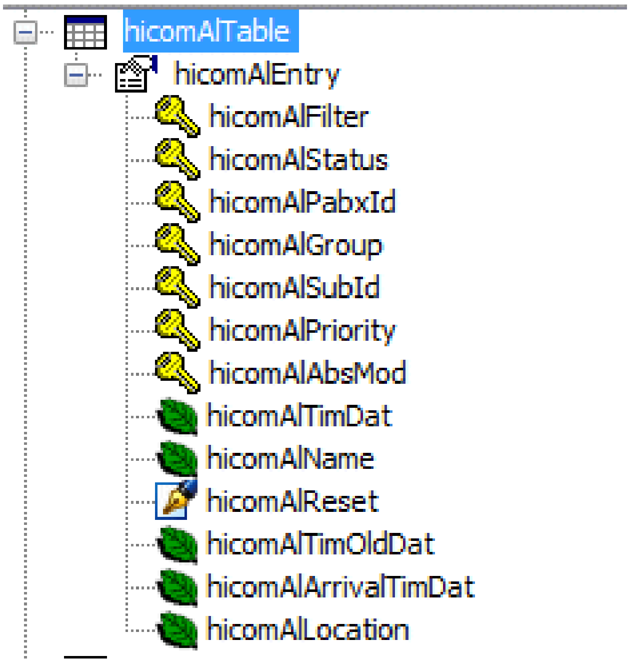
```
hicomAlMirrorUploadTable
    hicomAlMirrorUploadEntry
        hicomAlMirrorUploadPabxId
        hicomAlMirrorUploadMnemonic
        hicomAlMirrorUploadState
        hicomAlMirrorUploadStartTimDat
        hicomAlMirrorUploadErrorTimDat
```

Figure 166: hicomAlMirrorUploadState

Setting the hicomAlMirrorUploadState to 'busy' (3) will upload/ synchronize the alarm statuses raised by the Assistant (specified by hicomAlMirrorUploadPabxID index during set request) with the Manager database.

8.4.3 Resetting Alarms

You can reset the alarm status raised on with Manager database Assistant by sending an SNMP set request to the OS4K Manager over the hicomAlTable setting hicomAlReset field into busy value (3).



```
hicomAlTable
    hicomAlEntry
        hicomAlFilter
        hicomAlStatus
        hicomAlPabxId
        hicomAlGroup
        hicomAlSubId
        hicomAlPriority
        hicomAlAbsMod
        hicomAlTimDat
        hicomAlName
        hicomAlReset
        hicomAlTimOldDat
        hicomAlArrivalTimDat
        hicomAlLocation
```

Figure 167: hicomAlTable

9 Troubleshooting

9.1 Troubleshooting of SNMP

If subagents do not start correctly or errors occur during operation, information is available that can be used to troubleshoot the problem. The most important source of this information is the directory /opt/hipath_agents/log or /var/hipath_agents/log.

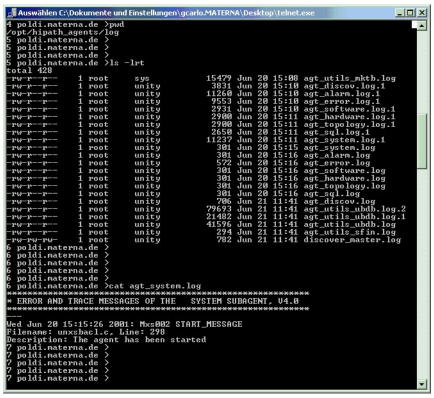
This directory contains, for each subagent, an up-to-date log file that traces the output from the agent since the last time it was started. The naming convention used for these log files is as follows:

"agt_"+<subagent name>+".log"(+"."+SeqNo)

In addition to the current log file, one or two older versions of the file are also stored in this directory for each subagent. The file without the sequence number (SeqNo) is always the most recent version. Each time an attempt is made to start the subagent, a new file is generated and the older versions are deleted or renamed accordingly.

If a subagent does not start, or terminates with an error, the log files will include the corresponding error message, as well as the last ten (10) internal messages from the associated subagent.

If these messages are not sufficient to determine the cause of the problem, be sure to save these log files so that they can be made available to Technical Support or Service.



Auswählen C:\Dokumente und Einstellungen\gcarlo.MATERNA\Desktop\telnet.exe

```
4 poldi.materna.de >pwd
/opt/hipath_agents/log
5 poldi.materna.de >
5 poldi.materna.de >
5 poldi.materna.de >
5 poldi.materna.de >ls -lrt
total 428
-rw-r--r--    1 root     sys          15479 Jun 20 15:08 agt_utils_mktb.log
-rw-r--r--    1 root     unity         3831 Jun 20 15:10 agt_discov.log.1
-rw-r--r--    1 root     unity        11260 Jun 20 15:10 agt_alarm.log.1
-rw-r--r--    1 root     unity         9553 Jun 20 15:10 agt_error.log.1
-rw-r--r--    1 root     unity         2931 Jun 20 15:10 agt_software.log.1
-rw-r--r--    1 root     unity         2900 Jun 20 15:11 agt_hardware.log.1
-rw-r--r--    1 root     unity         2900 Jun 20 15:11 agt_topology.log.1
-rw-r--r--    1 root     unity         2650 Jun 20 15:11 agt_sql.log.1
-rw-r--r--    1 root     unity        11237 Jun 20 15:11 agt_system.log.1
-rw-r--r--    1 root     unity          301 Jun 20 15:15 agt_system.log
-rw-r--r--    1 root     unity          301 Jun 20 15:16 agt_alarm.log
-rw-r--r--    1 root     unity          572 Jun 20 15:16 agt_error.log
-rw-r--r--    1 root     unity          301 Jun 20 15:16 agt_software.log
-rw-r--r--    1 root     unity          301 Jun 20 15:16 agt_hardware.log
-rw-r--r--    1 root     unity          301 Jun 20 15:16 agt_topology.log
-rw-r--r--    1 root     unity          301 Jun 20 15:16 agt_sql.log
-rw-r--r--    1 root     unity          706 Jun 21 11:41 agt_discov.log
-rw-r--r--    1 root     unity        79693 Jun 21 11:41 agt_utils_ubdb.log.2
-rw-r--r--    1 root     unity        21482 Jun 21 11:41 agt_utils_ubdb.log.1
-rw-r--r--    1 root     unity        41596 Jun 21 11:41 agt_utils_ubdb.log
-rw-r--r--    1 root     unity          294 Jun 21 11:41 agt_utils_sfin.log
-rw-rw-rw-    1 root     unity          782 Jun 21 11:41 discover_master.log
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >cat agt_system.log
***********************************************************
* ERROR AND TRACE MESSAGES OF THE   SYSTEM SUBAGENT, V4.0
***********************************************************
---
Wed Jun 20 15:15:26 2001: Mxs002 START_MESSAGE
Filename: unxsbacl.c, Line: 298
Description: The agent has been started
7 poldi.materna.de >
7 poldi.materna.de >
7 poldi.materna.de >
7 poldi.materna.de >
7 poldi.materna.de >
```

Figure 168: Screenshot of Directory Containing Log Files

10 Abbreviations

This section defines the most important abbreviations used in this manual.

Abbreviation	Definition
AC	alternating current
ACD	automatic call distribution
ACD-G	automatic call distribution global
ACE	adaptive communication environment
ADP	administration data processor; processor card in OpenScape/HiPath switch
AFR	automatic fault report
AM	administration and maintenance
AMO	administration and maintenance order
API	application programming interface
ARC	access right configuration; a UI of SecM to manage user access rights
ASCII	American Standard Code for Information Interchange
BIOS	basic input output system
CC	communications controller
CDB	common database
CE	1. customer engineer (internal) 2. ConformitÃ© EuropÃ©enne (European standards; CE marking)
CHD	customer header data; utility to configure CX communication
CLA	Custormer License Agent
CLI	command line interface
CLS	Central License Server
CM	configuration management
CMS	Communication Management System
CMX	Communications Manager Unixware
ComWin	COMTES for Windows
CPU	central processing unit
CRL	Certificate Revocation List
CS	communications server
CSC	Customer Support Center

cusa	**CU**stomer Security Administrator; predefined user account and security level for customer users
cust	CUSTomer; predefined security level for customer users
DAD	direct AMO dialog
DAT	digital audio tape
DB	database
DC	direct current
DF	differential
DMS	domain management service
DNS	domain name service
DRAM	dynamic random access memory
DSCX	Data Processor and Serial Channel Controller Extended (Pentium)
engr	Engineer: predefined user account and security level for service users
EPNP	enhanced private numbering plan
FAMOS	Fern (= remote) AMO Start
FM	fault management
FSS	Forwarding Support Service: routing component of CMX
FTP	file transfer protocol
GB	gigabyte
GUI	graphical user interface
HD	hard disk
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	identification
IDS	Informix Dynamic Server
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDA	Internet Protocol Distributed Architecture (formerly NBCS)
ISA	Industry Standard Architecture
ISDN	Integrated Services Digital Network
JRE	Java Runtime Environment

LAN	local area network
LCR	least-cost routing
LicM	license management
LTG	line trunk group
LTU	line trunk unit
LVD	1. low voltage differential (SCSI technology) 2. Low Voltage Directive (international standards)
MTBF	mean time between failures
MTTR	mean time to repair
NANP	North American Numbering Plan
NAT	network address translation
NBCS	network based communication system
NIC	1. network interface card 2. Network Information Center
NLS	national language support
NM	network management
NMI	non-maskable interrupt
NS	Netscape
NSL	network security level
NVMEM	nonvolatile memory
NVRAM	nonvolatile random access memory
OCSP	Online Certificate Status Protocol
OD	optical disk
ODBC	open database connectivity
ODF	object description file
OLR	online replacement
OMC	operation and maintenance center
OpenFT	File transfer tool (SNI tool)
OPS	off-premises station
ORB	object request broker
OS	operating system
OSI	Open Systems Interconnection
PBX	private branch exchange

PC	personal computer
PCI	peripheral component interconnect
PCMCIA	Personal Computer Memory Card International Association
PEN	port equipment number
PID	process ID; unique numerical ID of a Unix process
PIN	personal identification number
PL	private line
PLD	programmable logic device
PM	1. performance management 2. project manager
PP	patch package
PPP	point-to-point protocol
PPTP	point-to-point tunneling protocol
PROM	programmable read-only memory
PSTN	public switched telephone network
PSIO	peripheral serial IO
PSM	platform support module
RAID	redundant array of inexpensive disks
RAS	remote access service
RegSvc	registration service
REN	ringer equivalency number
RIP	routing information protocol
RLC	revision level complete
RISC	reduced instruction set computing
RMA	remote administration and maintenance
RMAID	remote administration and maintenance identification
RPS	redundant power system
rsca	remote service customer assistance; predefined user account and security level for service users
rsta	remote service technical assistance; predefined user account and security level for service users
SAF-TE	SCSI accessed fault-tolerant enclosure
SAP	Service Agreement Policy

SASH	stand-alone shell
SCSI	small computer system interface
SCU	server configuration utility
SD	system designer
SDE	single data entry
SDK	software development kit
SDRAM	synchronous DRAM
SE	1. single-ended (SCSI terminator mode) 2. systems engineer
SEA	Strong Encryption and Authentication
SecM	security management
SID	system identification disk
SIP	set installation package
SIS	software information system
SLC	second level cache
SLES	SuSE Linux Enterprise Server
SMP	symmetric multiprocessing
SMR	system maintenance release
SNM	system and network management
SNMP	simple network management protocol
SNS	System and Network Solutions
SP1	Serviceability Pack 1
SP(o)A	single point of access
SPD	service profile definition
SPOC	single point of configuration
SQL	structured query language
SS	single system
SSL	secure socket layer
SSO	Smart Switchover
SSSC	Systems/Service and Support Center
STM	SCSI terminator module
STM-LVD	SCSI terminator module for low voltage differential

STM-SE	SCSI terminator module for single-ended mode
SWA	software activation
SWS	software supply
SWM	software manager
SWU	switching unit
SysM	system management
TA	1. terminal adapter 2. transport address (CMX)
TAO	The ACE ORB
TAP	Techniker Arbeitsplatz (literally, "engineering workstation"; the CE's laptop)
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	telephony diagnostics system
TFT	thin film transistor
TIA	Telecommunications Industries Association
TNS	transport name service
TSP	transport service provider
UBA	Unix Base Administration
UDSC	uniform data security concept
UI	user interface
UL	Underwriters Laboratories
ULCT	UNIX local configuration tool
UNA	user and network administration
URI	1. Unix RMX interface 2. Uniform Resource Identifier
URL	Uniform Resource Locator
USB	universal serial bus
USM	UDSC Session Manager
USV	Unix Supervisor
UTC	Universal Time Coordinated
VGA	variable graphics array
VPN	virtual private network
WAN	wide area network
WOL	wake on LAN

XIE	import/export interface
XML	extensible markup language

Index

mitel.com