A MITEL
PRODUCT
GUIDE

Unify OpenScape Xpert

OpenScape Xpert V8R0

Service Manual
08/2024

P31003-X2075-S100-02-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 History of changes

Changes mentioned in the following list are cumulative.

Changes in V8R0

Impacted chapters	Change description
How to Install OpenScape Xpert Client SW via Network under Windows 10 on page 158	Add information about the possibility to configure a proxy server.
How to create a bootable USB stick on page 162	Add information about the possibility to enable LLDP-MED during the installation,
How to Install the OpenScape Xpert Client Application on page 192	Add information about the possibility to configure a HTTP/HTTPS proxy for System Manager.
LLDP-MED on page 196	Mention that the LLDP-MED server is disabled by default.
Upgrade of an OpenScape Xpert Standalone Server from V7 to V8 on page 82	Update versions.
How to change the webuser password	Fix the command for changing the webuser password in the database.
OpenScape Xpert V7 Licensing on page 40	Update information about licensing modes and grace period.
How to Install MLC.deb on page 107	Update instruction for installing MLC.deb
Setting Up in MLC on page 152	New chapter about setting Unify Office lines in MLC.
Local DNS caching for MLC on page 155 Configuration on page 156 Usage on page 156	New chapters about configuring MLC for DNS caching.
Change Password on page 44 How to activate the Active Directory authentication of ConfigServer user	Updated chapters about using named pipe authentication for csuser.
OpenScape Xpert Management Portal Web GUI on page 37 How to Use https in Browser on page 58 How to use your own certificate for HTTPS on page 61	Updated chapters with information about browsers.
The credentialStore.bcfks file on page 56 The secretKey.store file on page 57 How to change the credential store password on page 59	Updated chapters about using Encrypted password for Credential Store.

Impacted chapters	Change description
The credentialStore.bcfks file on page 56 How to change the credential store password on page 59 Upgrade of an OpenScape Xpert Standalone Server from V7 to V8 on page 82	Updated chapters about Webuser with GSSAPI.
Upgrade of an OpenScape Xpert Standalone Server from V7 to V8 on page 82	Updated chapter about updating from V7 to V8.
Password complexity check for the Administrator and API User password on page 44	New chapter about password complexity check.
How to configure static IPv4 address on page 164 How to configure static IPv6 address on page 167	Updated chapters about the Turret component

2 Introduction and Important Notes

OpenScape Xpert is an industry first, best-in-class, pure IP multi-line communications solution addressing both Trading floors and Dispatching Centers of energy, railway or transport networks, airports and their movement areas.

This document describes the installation of OpenScape Xpert V7 from the initial installation of the System Manager Server (Windows Server 2012 R2 and Windows Server 2016), MLC and OpenScape Xpert clients based on a sample configuration.

NOTICE:

The setup commands of the STMI2/STMI4 in HiPath 4000 / OpenScape 4000 are described in the document "OpenScape 4000 V7, Volume 4: IP Solutions, Service Documentation" available in E-Doku. Please refer to this document for german and english AMOs in key-oriented and position-oriented OpenScape 4000 commands for the STMI2/STMI4 (SIP subscriber).

2.1 Target Group and Requirements

Intended Audience

What You Need to Know

The OpenScape Xpert V7 - Service Manual is intended for qualified service personnel responsible for installing and configuring the OpenScape Xpert system.

A working knowledge of computers and client-server network architectures is necessary for executing the tasks. In addition, you should be familiar with telecommunications equipment functionality and have obtained proper login permissions.

NOTICE:

Depending on version and licenses, the features described in this manual may not be available or only available to a limited extent.

2.2 Manual Structure

This manual is structured to show step by step all the required tasks to install and configure all the necessary components (System Manager, MLC, OSX end-points, etc.)

2.3 Notational Conventions Used

This manual uses the following notational conventions:

Purpose	Style	Example
Special emphasis	Bold	Name must not be deleted.
User interface elements	Bold	Click OK.
Menu sequence	>	File > Close
Textual cross-references	Italic	For more information, see Network.
Output	Font with a fixed width such as Courier	Command not found.
Input	Font with a fixed width such as Courier	Enter LOCAL as the file name.
Key combinations	Font with a fixed width such as Courier	<CTRL>+<ALT>+<ESC>
Steps and subordinate steps in instructions	Numbered lists (using numbers and letters)	Set up the DSL telephony subscriber with the corresponding extension number.Click Add.In DSL Telephony Subscriber, enter the name of the DSL telephony subscriber.
Options in instructions	Bulleted list	If you want to output amounts, select the Output Amounts, Not Units checkbox.If you want to output units, deselect the Output Amounts, Not Units checkbox.

IMPORTANT:

Identifies useful information.

2.4 Safety Information and Warnings

Work on communication systems and devices may only be carried out by qualified persons.

For the purposes of safety information and warnings, qualified persons are persons who are authorized to place into operation, ground, and label systems, devices, and lines in accordance with applicable safety procedures and standards.

It is absolutely essential that you read and understand the following safety information and warnings before starting installation and implementation work on the communication system or device.

You should also carefully read and observe all safety information and warnings on the communication systems and devices themselves.

Familiarize yourself with emergency numbers.

Always consult your manager before starting work in conditions where the necessary safety precautions do not appear to be in place.

Types of safety information and warnings

DANGER

Indicates an immediate danger that could result in death or serious injury.

WARNING

Indicates a general danger that could result in death or serious injury.

CAUTION

Indicates a danger that could result in injury.

NOTICE:

Indicates situations that could result in damage to property and/or loss of data.

Symbols for specifying the source of danger more exactly

The following symbols are not usually used in the manual. They explain symbols that may be depicted on the communication systems and equipment.

* electrostatically sensitive devices

2.4.1 Warning Sign: Danger

DANGER

Risk of electric shock through contact with live wires!

- Note: Voltages above 30 Vac (alternating current) or 60 Vdc (direct current) are dangerous.
- Only personnel with proper qualifications or qualified electricians should perform work on the low-voltage network (1000 Vac).

2.4.2 Warning Sign: Warning

WARNING

Risk of electric shock through contact with live wires!

An electric shock can be life-threatening or lead to serious injuries such as burns.

There are additional dangers even when working with low voltage and large cable cross-sections. Cables with a large cross-section generally have lower voltages, although the amperages are higher.

- Before starting any work, check that the circuits involved are de-energized. Never take it for granted that turning off a main switch or circuit breaker will reliably interrupt all circuits.
- Only use systems, tools, and equipment which are in perfect condition. Do not use equipment with visible damage.
- Replace any damaged safety equipment (covers, labels and ground wires) immediately.
- Replace the power cable immediately if you notice any damage.
- Only place systems or devices in protection class I into operation using a ground contact socket.
- Connect the communication system and, if necessary, the main distribution frame to the ground wire before starting up the system and connecting telephones and lines. Never operate the communication system without the required ground wire.
- Never touch live wires without ensuring adequate insulation.
- Do not carry out any hardware installation work on telecommunication systems and devices during a storm.
- Expect leakage current from the telecommunications network. Disconnect all telecommunication lines from the system before disconnecting the prescribed ground wire from the system.

WARNING

Disconnection from power circuit(s)!

A disconnect device can be a disconnecting switch (main switch), circuit breaker (fuse/cutout), or power plug that completely disconnects the telecommunication system and device from the power circuit.

- Before carrying out any work on the communication system or on the device, find out whether there is a disconnect device and locate it.
- When you need to disconnect the power supply to the communication system or device, you do so using the disconnect device..
- Secure the disconnect device mechanically so that it cannot be used by other persons and attach a sign reading DO NOT OPERATE to the disconnect device.
- Ensure that the communication system or device is not powered from an additional power source (for example, an uninterruptible power supply), or that it is protected by an additional fuse or an additional main switch.
- If you are performing work on circuits with hazardous voltages, always work together with a partner who is familiar with the location of the disconnect devices for the power supplies.
- Always disconnect the power supply when you are working directly next to a power supply unit or direct current converter, unless the work instructions expressly permit you to work without disconnecting the power supply.
- As long as the power supply is switched on, always observe the greatest caution when performing measurements on powered components and maintenance work on plug-in cards, PC boards and covers.
- Metallic surfaces such as mirrors are conductive. If you touch them, there is a risk of electric shocks or short circuits.

2.4.3 Warning Sign: Caution

CAUTION

Danger of injury:

An electric shock can be life-threatening or lead to serious injuries such as burns.

- When working on an open communication system or device, make sure that it is never left unattended.
- Risk of injury resulting from heavy items or loads. Lifting heavy objects/loads can cause injury. Use appropriate aids to carry out such tasks.
- Risk of injury resulting from laser radiation. If there are any optical interfaces: In case of laser radiation, do not look directly into the beam. You could damage your eyes.

CAUTION

Risk of explosion if accumulators and batteries are not changed properly:

- Only use the approved battery pack and batteries.
- The lithium battery must be replaced only by an identical battery or one recommended by the manufacturer.

CAUTION

Risk of fire:

- Only telecommunications cables with a cable diameter of at least 0.4 mm (AWG 26) or larger may be used..
- The system cabinets must not be fitted with any third-party devices that have not been approved.
- Do not store any documents or similar flammable items in the system.

CAUTION

General risk of injury/accidents in the workplace:

- When maintenance work has been completed, always re-install all safety equipment in the right place. Also close all doors, covers, or the housing after completing test and maintenance work.
- Install cables in such a way that they do not pose a risk of accident (tripping), and cannot be damaged.
- Make sure that the work area is well lit and tidy.
- When working on the systems, never wear loose clothing and always tie back long hair.
- Do not wear jewelry, metal watchbands or clothes with metal ornaments or rivets. There is a risk of injury and short circuits.
- Always wear the necessary eye protection whenever appropriate.
- Always wear a hard hat where there is a risk of injury from falling objects.
- Check your tools regularly. Only use intact tools.

2.4.4 Important Information

Note the following information in order to avoid damage to property:

- Before placing the system into operation, check whether the nominal voltage of the power supply network corresponds to the nominal voltage of the communication system or device (type plate). If necessary, adjust the nominal voltage of the communication system or device appropriately.

- To protect electrostatically sensitive devices (ESD):
  - Always wear the wristband in the prescribed manner before performing any work on PC boards and modules.
  - Transport PC boards and modules only in suitable protective packaging.
  - Always place PC boards and modules on a grounded conductive base, and do not work on the PC boards anywhere else.
  - Only use grounded soldering irons.
- Use only original accessories. Failure to comply with this safety information may damage the equipment or violate safety and EMC regulations.
- Before starting wall assembly, check that the load-bearing capacity of the wall is adequate, Always use suitable installation and fixing material to make sure that the communication system is mounted safely.
- Condensation damage:

  If the temperature changes rapidly, air humidity can precipitate. If the communication system or device is moved from a colder to a warmer environment, moisture can precipitate. Wait until the temperature has adjusted to the ambient temperature and the communication system or device is completely dry before starting it up.

2.5 Emergencies

What to Do in an Emergency?

- In the event of an accident, remain calm and controlled.
- Always switch off the power supply before you touch an accident victim.
- If you are not able to immediately switch off the power supply, only touch the victim with non-conductive materials (such as a wooden broom handle), and first of all try to isolate the victim from the power supply.

First Aid

- Be familiar with basic first aid procedures for electrical shock. A fundamental knowledge of the various resuscitation methods if the victim has stopped breathing or if the victim’s heart is no longer beating, as well as first aid for treating burns, is absolutely necessary in such emergencies.
- If the victim is not breathing, immediately perform mouth-to-mouth or mouth-to-nose resuscitation.
- If you have appropriate training, immediately perform heart massage if the victim’s heart is not beating.

Calling for Help

Immediately call an ambulance or an emergency physician. Provide the following information in the following sequence:

- Where did the accident happen?
- What happened?
- How many people were injured?
- What type of injuries?
- Wait for questions.

2.6 Reporting Accidents

- Immediately report all accidents, near accidents and potential sources of danger to your manager.
- Report all electrical shocks, no matter how small.

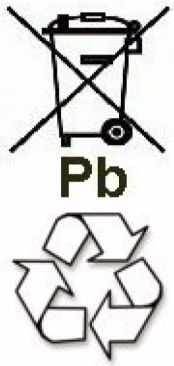
2.7 Proper Disposal and Recycling

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service, the shop where you purchased the product or your sales representative.

The statements quoted above are only fully valid for equipment which is installed and sold in the countries of the European Union and is covered by the Directive 2002/96/EC. Countries outside the European Union may have other regulations regarding the disposal of electrical and electronic equipment.



Used accumulators and batteries with this sign are valuable economic goods and must be recycled. Used accumulators and batteries that are not recycled must be disposed of as hazardous waste with full observance of all regulations.

2.8 Standards and Guidelines on Installation

2.8.1 Connection to the Power Supply

OpenScape communication systems are approved for connection to TN-S power supply systems. They can also be connected to a TN-C-S power supply

system in which the PEN conductor is divided into a ground wire and a neutral wire. TN-S and TN-C-S systems are defined in the IEC 364-3 standard.

If work on the low-voltage network is required, it must be carried out by a qualified electrician. The installation work required to connect OpenScape communication systems must be carried out with full observance of IEC 60364 and IEC 60364-4-41 or the equivalent legal norms and national regulations (in the US and Canada, for example).

2.8.2 Fire Safety Regulations

Fire safety regulations are specified in country-specific building codes. Adhere to the relevant regulations.

To conform with the legal fire protection and EMC requirements, operate the OpenScape systems only when closed. You may open the system only briefly for assembly and maintenance work.

As regards their burning behavior, OpenScape system cables conform to the international standard IEC 60332-1. The following standards include equivalent requirements regarding the burning behavior of cables.

IEC 60332-1 --- **Note**: IEC 60332-1 corresponds to UL VW-1	EN 50265-1 with EN 50265-2-1 --- **Note**: EN 50265-1 and -2-1 replace HD 405.1	VDE 0482 parts 265-1 with VDE 0842 parts 265-2-1 --- **Note**: VDE 0482 parts 265-1 and -2-1 replace VDE 0472, part 804, test type B

The responsible project management and service departments must verify whether this standard satisfies the applicable building regulations and any other additional regulations.

2.8.3 Screened Lines for LAN, WAN, and DMZ Connections

The following prerequisites must be met in order to comply with CE requirements relating to the electromagnetic compatibility of the communication system and its LAN, WAN, and DMZ connections:

- The communication system may only be operated with screened connection cables. This means that a screened CAT.5 cable with a length of at least 3m must be used between the screened LAN, WAN, and DMZ connection sockets of the communication system and the connection to the building utilities or the connection to active external components. The cable screen on the cable end that connects to the building utilities or active external components must be grounded (building potential equalization connection).
- In the case of shorter connections with an active external component (LAN switch or similar), a screened CAT.5 cable must also be used. However, the

active component must have a corresponding screened LAN connection with a grounded screened connector (building potential equalization connection).

- The screen properties of the cabling components must comply with the requirements of the European EN 50173-1 standard on generic cabling systems and with any requirements referenced therein. The European EN 50173-1 standard is derived from the global ISO/IEC 11801 standard.
- Building utilities that have integrated and screened symmetrical copper cabling in accordance with the requirements of class D of EN 50173-1 fulfill the condition above. Class D is also attained if components (cables, connection boxes, connection cables, etc.) of category 5 (CAT.5) are installed.
- In North America, UTP cabling is normally installed (US EIA/TIA 568A standard), and the following conditions apply to the LAN connections of communication systems there: The communication system may only be operated with screened connection cables. This means that a screened CAT.5 cable with a length of at least 3m must be used between the screened LAN, WAN, and DMZ connection sockets of the communication system and the connection to the building utilities or the connection to active external components. The cable screen on the cable end that connects to the building utilities or active external components must be grounded (building potential equalization connection).
- Note the information pertaining to the screened connection on the LTU frame exit point for the LAN connection to PC boards in LTUs.

2.8.4 Labeling

The compliance of the equipment according to EU directives is confirmed by the CE mark. This Declaration of Conformity and, where applicable, other existing declarations of conformity as well as further information on regulations that restrict the usage of substances or affect the declaration of substances used in products can be found in the Unify Expert WIKI at

ttp://wiki.unify.com under the section “Declarations of Conformity”.

2.9 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 Unify GmbH & Co. KG 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.
- Make the most of password restrictions: Do not allow unauthorized persons to find out passwords that you have noted down on paper, for example.
- 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.

2.10 Documentation Feedback

If you have questions that are not answered by this document:

- Internal employees should contact their National Support Center.
- Customers should contact their retailer or the Unify Customer Support Center.

When you call, state the title, ID number, and issue of the document.

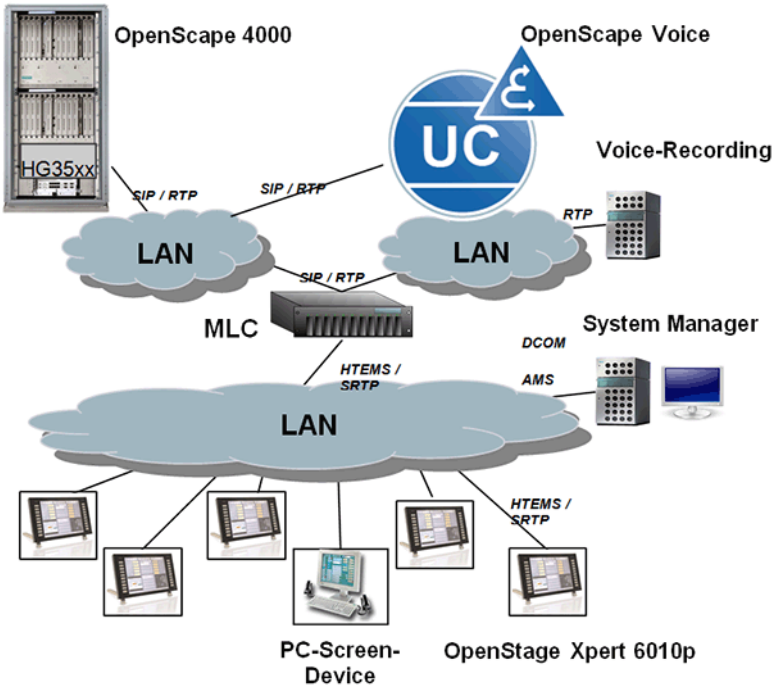
Example

- Title: OpenScape 4000 V7, Service Documentation
- ID number: P31003H3170S104010020
- Issue: 1

3 Overview of the OpenScape Xpert System

3.1 Example Scenario

Following simple installation is based with 1 Ethernet interface per MLC and explains all necessary hardware components for OpenScape Xpert. Different scenarios with different network environments and so forth are not part of this installation manual. This document describes the installation of OpenScape Xpert.



IMPORTANT:

If OSV or OS4k for Xpert RX are in different subnets, please take the "Network Planning" chapter of the “Planning Guide” document available via E-Doku into consideration.

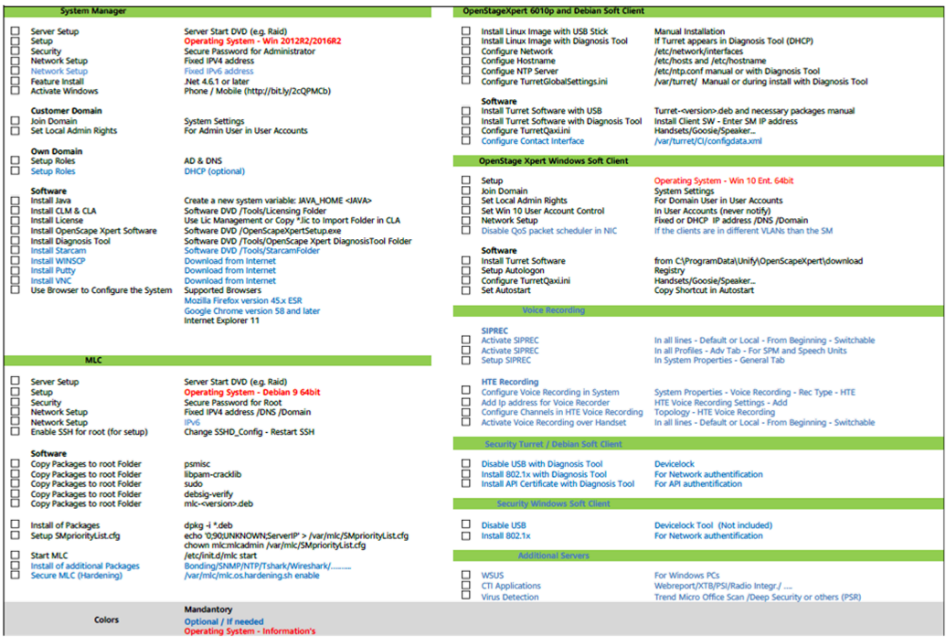
http://apps.g-dms.com:8081/techdoc/en/P31003X2050P1000176A9/index.htm

3.2 Recommendation

The OpenScape Voice (8000) provides the SIP protocol and SIP subscribers.

With OpenScape Xpert from Version V4 on, the maximum number of lines per MLC is 240.

3.3 OpenScape Xpert Installation Checklist



System Manager

☐ Server Setup	Server Start DVD (e.g. Raid)
☐ Setup	Operating System - Win 2012R2/2016R2
☐ Security	Secure Password for Administrator
☐ Network Setup	Fixed IPV4 address
☐ Network Setup	Fixed IPv6 address
☐ Feature Install	.Net 4.6.1 or later
☐ Activate Windows	Phone / Mobile (http://bit.ly/2cQPMCb)
Customer Domain	
☐ Join Domain	System Settings
☐ Set Local Admin Rights	For Admin User in User Accounts
Own Domain	
☐ Setup Roles	AD & DNS
☐ Setup Roles	DHCP (optional)
Software	
☐ Install Java	Create a new system variable: JAVA_HOME <JAVA>
☐ Install CLM & CLA	Software DVD /Tools/Licensing Folder
☐ Install License	Use Lic Management or Copy *.lic to Import Folder in CLA
☐ Install OpenScape Xpert Software	Software DVD /OpenScapeXpertSetup.exe
☐ Install Diagnosis Tool	Software DVD /Tools/OpenScape Xpert DiagnosisTool Folder
☐ Install Starcam	Software DVD /Tools/StarcamFolder
☐ Install WINSCP	Download from Internet
☐ Install Putty	Download from Internet
☐ Install VNC	Download from Internet
☐ Use Browser to Configure the System	Supported Browsers
	Mozilla Firefox version 45.x ESR
	Google Chrome version 58 and later
	Internet Explorer 11

MLC

☐ Server Setup	Server Start DVD (e.g. Raid)
☐ Setup	Operating System - Debian 9 64bit
☐ Security	Secure Password for Root
☐ Network Setup	Fixed IPV4 address /DNS /Domain
☐ Network Setup	IPv6
☐ Enable SSH for root (for setup)	Change SSHD_Config - Restart SSH
Software	
☐ Copy Packages to root Folder	psmisc
☐ Copy Packages to root Folder	libpam-cracklib
☐ Copy Packages to root Folder	sudo
☐ Copy Packages to root Folder	debsig-verify
☐ Copy Packages to root Folder	mlc-<version>.deb
☐ Install of Packages	dpkg -i *.deb
☐ Setup SMpriorityList.cfg	echo '0;90;UNKNOWN;ServerIP' > /var/mlc/SMpriorityList.cfg
	chown mlc:mlcadmin /var/mlc/SMpriorityList.cfg
☐ Start MLC	/etc/init.d/mlc start
☐ Install of additional Packages	Bonding/SNMP/NTP/Tshark/Wireshark/.....
☐ Secure MLC (Hardening)	/var/mlc/mlc.os.hardening.sh enable

Colors	**Mandantory**
	Optional / If needed
	Operating System - Information's

OpenStageXpert 6010p and Debian Soft Client

☐ Install Linux Image with USB Stick	Manual Installation
☐ Install Linux Image with Diagnosis Tool	If Turret appears in Diagnosis Tool (DHCP)
☐ Configure Network	/etc/network/interfaces
☐ Configue Hostname	/etc/hosts and /etc/hostname
☐ Configue NTP Server	/etc/ntp.conf manual or with Diagnosis Tool
☐ Configure TurretGlobalSettings.ini	/var/turret/ Manual or during install with Diagnosis Tool
Software	
☐ Install Turret Software with USB	Turret-<version>.deb and necessary packages manual
☐ Install Turret Software with Diagnosis Tool	Install Client SW - Enter SM IP address
☐ Configure TurretQaxi.ini	Handsets/Goosie/Speaker...
☐ Configure Contact Interface	/var/turret/CI/configdata.xml

OpenStage Xpert Windows Soft Client

☐ Setup	Operating System - Win 10 Ent. 64bit
☐ Join Domain	System Settings
☐ Set Local Admin Rights	For Domain User in User Accounts
☐ Set Win 10 User Account Control	In User Accounts (never notify)
☐ Network Setup	Fixed or DHCP IP address /DNS /Domain
☐ Disable QoS packet scheduler in NIC	If the clients are in different VLANs than the SM
Software	
☐ Install Turret Software	from C:\ProgramData\Unify\OpenScapeXpert\download
☐ Setup Autologon	Registry
☐ Configure TurretQaxi.ini	Handsets/Goosie/Speaker...
☐ Set Autostart	Copy Shortcut in Autostart

Voice Recording

SIPREC	
☐ Activate SIPREC	In all lines - Default or Local - From Beginning - Switchable
☐ Activate SIPREC	In all Profiles - Adv Tab - For SPM and Speech Units
☐ Setup SIPREC	In System Properties - General Tab
HTE Recording	
☐ Configure Voice Recording in System	System Properties - Voice Recording - Rec Type - HTE
☐ Add Ip address for Voice Recorder	HTE Voice Recording Settings - Add
☐ Configure Channels in HTE Voice Recording	Topology - HTE Voice Recording
☐ Activate Voice Recording over Handset	In all lines - Default or Local - From Beginning - Switchable

Security Turret / Debian Soft Client

☐ Disable USB with Diagnosis Tool	Devicelock
☐ Install 802.1x with Diagnosis Tool	For Network authentification
☐ Install API Certificate with Diagnosis Tool	For API authentification

Security Windows Soft Client

☐ Disable USB	Devicelock Tool (Not included)
☐ Install 802.1x	For Network authentification

Additional Servers

☐ WSUS	For Windows PCs
☐ CTI Applications	Webreport/XTB/PSI/Radio Integr./ ....
☐ Virus Detection	Trend Micro Office Scan /Deep Security or others (PSR)

4 System Manager

4.1 Setting Up the Server for the OSX System Manager

4.1.1 General Information

This chapter describes the installation of the System Manager server with operating system, domain controller / Active Directory, DNS (Domain Name Server) and DHCP (Dynamic Host Configuration Protocol).

Hardware

Windows Server 2016 Standard and Windows Server 2019 Standard are approved for the OpenScape Xpert system manager server. The hardware requirements of the system manager server are described in the “Project Guidelines”. This manual describes the setup of a Windows Server **All in One**.

Options

There are two different options for configuring system manager:

- The system manager server is an **All in One** server, i.e. Active Directory server, DHCP server, DNS server and system manager components.

  List of the software components:

  – Operating system Windows Server 2016 Standard or Windows Server 2019 Standard.
  – Active Directory server (AD): The AD is for the login accounts of the Windows domain.
  – DNS server: The DNS is for the correct name resolution (IP to names and vice versa).
  – DHCP server (optional): The DHCP is optional and for dynamic IP support of the Xpert turrets.
  – OpenScape Xpert V7 Server
- The system manager server is a member server -> i.e. system manager only. (The Active Directory, DHCP and DNS server functions are stored on a separate server).

Hints

- Unless approved by GVS, the server should not contain any other applications except for the OpenScape Xpert software apart from diagnosis software.
- A functionally network interfaces card (NIC) is mandatory necessary and plugged in the system manager server.
- A switch has to be connected in advance to the NIC for setting up the Microsoft services.

4.1.2 Windows Server 2016/2019 Operating System

This section describes the setup of a Windows Server Operating System.

4.1.2.1 How to Install the Operating System

Prerequisites

For more information see: https://docs.microsoft.com/hu-hu/windows-server/identity/ad-ds/active-directory-domain-services

Step by Step

1) If existing: setup the servers with Startup Server DVD provided by the server hardware manufacturer and configure the RAID conditions first.

2) Insert the Windows Server 2016/2019 DVD, restart the PC and boot from CD/DVD.

Setup will be started automatically.

3) Enter your regional options (Language, time and currency format, keyboard layout). Click **Next**.

4) On the next confirmation window click **Install now**.

5) Enter the product key.

6) Select the setup option **Server with a GUI**.

7) Read and accept the License terms.

8) If you get the question **Which type of installation do you want?**, select **Custom: Install Windows only (advanced)**

9) Partitioning the hard disc (C:\System (min. 100 GB), D:\Data).

10) .Setup will run for some minutes and the PC restarts automatically (two times).

NOTICE:

Do not remove the W2016/2019 install DVD from the DVD drive, it will be needed for features setup.

---

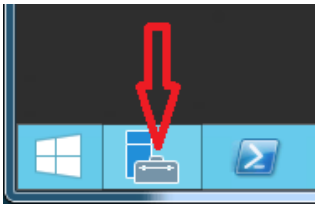
11) Define the Administrator password. Please pay attention to the complexity requirement.

12) After finalizing the setup, press CTRL + ALT + DEL to sign in.

a) For the question "Do you want to find PCs.." click **No**

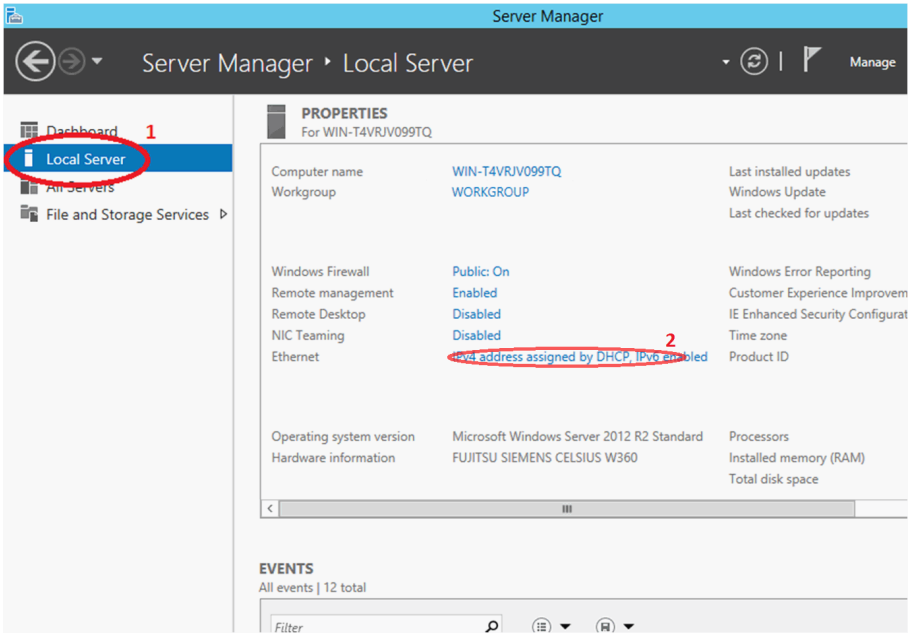
The Server Manager appears.

13) If the Server Manager is closed, you can start Server Manager here:



14) Setup as custom setting the networking components **static IP address**, **Subnet mask**, **Default gateway** and **preferred DNS server** using the following steps:.

15) Go to: **Server Manager** / **Local Server**



a) Click on the **Ethernet** entry.

The window **Network Connections** appears.

b) Click the right mouse button on **Ethernet**, choose **Properties**, select **Internet Protocol Version 4** and press **Properties**.

16) TCP/IPv6 protocol is necessary only if V7 is installed with IPv6.

17) Change the Computer Name to an appropriate name:

a) Go to **Server Manager** / **Local Server** / **Computer name**

b) Click on the Computer name entry (It's better to do it now, later in the Domain Controller needs more effort.).

18) Activate Windows. Press the right mouse button on **Start** and select **System**.

The **System** window appears.

19) Click on **Activate Windows** and type in the product key.

20) According to the customer requirements, install the latest Microsoft Windows updates and hotfixes.

21) ".Net 4.6.1" or later is necessary for the operation of the Diagnosis Tool. After the installation .Net is installed and its version can be checked in Server Manager. To check the ".Net" version on Windows Server 2016 proceed as follows:

a) Click on **Local Server** and go to **Roles and Features**.

b) Type `.net` in the text box

The following entries must be listed:

.Net Framework 4.6 Features

.Net Framework 4.6

4.1.2.2 The Installation of Required Roles and Features

This section describes the installation of the system manager as All in One server.

This following components have to be installed:

- Active Directory Domain Services (AD DS)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Quality Windows Audio Video Experience

For more information see: https://docs.microsoft.com/hu-hu/windows-server/identity/ad-ds/active-directory-domain-services

4.1.2.3 How to Setup AD DS

Step by Step

1) Start the Server Manager.

2) On Dashboard click on „**Add roles and features**”.

The wizard appears.

3) Click on **Server Selection** (on the left).

4) Click on **Server Roles** (on the left).

5) Select **Active Directory Domain Service**.

A dialog appears.

6) Select **DNS Server**.

A dialog appears.

7) On the **Add features...** dialog click on **Add Features**.

8) Click on **Features** (on the left).

9) Click on Confirmation (on the left).

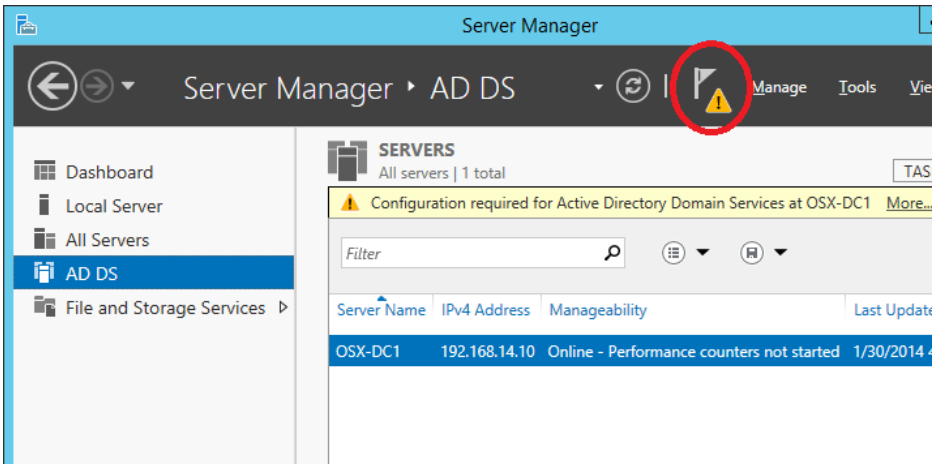
10) Click on **Specify an alternate source path**: E:\sources\sxs ; E:\ depends on the CD drive, where the Win2016/2019 install DVD is located.

11) Click on Install.

12) Installation progress.

13) Click **Close** to close the wizard.

14) In the **Server Manager** click the **alert** in the upper right.



15) In the **Task Details** window click on „**Promote this server to a domain controller**".

The **Active Directory Domain Services Configuration** Wizard appears.

16) In the **Deployment Configuration** dialog select **"Add a new forest"** and add the Root domain name: "`yourdomain.xxx`", e.g. "`OSXDomain.local`", and click **Next**.

17) In the **Domain Controller Options** dialog set the **Forest and Domain functional level** to „Windows Server 2016" (It depends on the other servers. It can be raised later, but not rolled back.)

18) Enter and confirm the **Directory Services Restore Mode (DSRM) Administrator Password** (suggestion: same as administrator password), and click **Next**.

19) The delegation warning message can be ignored, click **Next**.

20) In **Additional Options** dialog „The NetBIOS domain name" is already assigned. Click **Next**.

21) In the **Paths** dialog specify the location of the AD DS database, log files, and SYSVOL. The folders are set to `C:\...` by default.

IMPORTANT:

For a better system performance it is recommended to change the database and log folders to `D:\...`. The partition `D:\` must be configured and already formatted with NTFS.

---

a) Change the path of the database folder to `D:\WINDOWS\NTDS` using the **Browse** button.

b) Change the path of the log folder to `D:\WINDOWS\NTDS` using the **Browse** button.

22) Click **Next** to continue.

23) In the **Review Options** dialog click **Next**.

24) In the **Prerequisites Check** dialog (if the check is ok) click **Install**.

25) After a reboot you can login with the domain credential: `domain\Administrator`.

4.1.2.4 How to Setup DNS (Domain Name Server)

Step by Step

1) Logon to the system in the OpenScape Xpert domain using the administrator ID and the correct password.

The **Managing Your Server Role** dialog appears.

2) By installing Active Directory the DNS has been installed automatically. Click **Start-Programs-Administrative Tools-DNS (Windows Server 2016 Start – Windows Administrative Tools - DNS)** to open the DNS Manager.

3) Check the Forward Lookup Zone "yourdomain.xxx".

Your server host should appear in the list.

4) Add Reverse Lookup Zone by right clicking at **Reverse Lookup Zone New Zone…**. In the Welcome to the New Zone Wizard click **Next**.

5) In the **Zone Type** dialog, select the **Primary zone** option and check the **Store the zone in Active Directory** check box and click **Next**.

6) Select **To all DNS servers running on domain controllers in this domain: "yourdomain.xxx"** and click **Next**. Keep the **Ipv4 Reverse Lookup Zone** setting and click **Next** again.

7) Define the **Network ID**. The last digit is grayed out. Click **Next** to continue.

8) Select the **Allow only secure dynamic updates** option and click **Next**. In the **Completing the New Zone Wizard** window, click **Finish**.

The Reverse Lookup Zone should appear in the list.

9) Add **Pointer** by right clicking the new Reverse Lookup Zone **X.X.X.in-addr.arpa - New Pointer(PTR)** In the **New Resource Record** dialog. Complete the Host IP address: and Browse to the associated Host name (Look in DNS > "yourservername" > Forward Lookup Zones > "yourdomain.xxx" > "yourservername") and click **OK** and **OK** again.

The "yourservername" Pointer with IP address should appear in the list.

10) Open the **Local Area Connection Properties** again. Select the **Internet Protocol (TCP/IP)** entry in the connection list and click the **Properties** button. Add the correct preferred DNS server IP address and click **OK** and **Close**.

11) Check with nslookup in Command prompt if DNS is setup correctly (both directions name and IP address).

IMPORTANT:

Do not continue without DNS working.

---

12) It is recommended to add also the MLC's to the DNS, although it is **not** forcefully needed. In the Forward Lookup Zones right click on **"yourdomain.xxx"** and select **New Host (A or AAAA)**. In the **New Host** dialog insert the name and IP address of the MLC and select **Create associated pointer (PTR) record**, then **Add Host, OK** and **Done**.

IMPORTANT:

With more than one network range it is mandatory to add all the necessary Reverse Lookup Zones into DNS.

4.1.2.5 How to Setup DHCP

Step by Step

1) Start the Server Manager.
2) On **Dashboard** click on „**Add roles and features**”.

   The wizard appears.
3) Click on **Server Selection**.
4) Click on **Server Roles**.
5) Select **DHCP Server**.

   A Dialog appears.
6) Click on **Add Features**.
7) Click on **Confirmation** (left side).
8) Click on **Install**.
9) Close the wizard.
10) Open the **DHCP Manager** (**Administrative Tools** / **DHCP**).
11) Open the <Server Name> and right-click on **IPv4** and select **New Scope...**

    The **New Scope Wizard** appears.
12) ,Click on **Next**.
13) Enter the **Scope Name** and **Description**, click **Next**.
14) Enter the **Start IP address**, **End IP address**, **Length or Subnet mask** and click Next.

    NOTICE:

    The range is important and depends on the number of Xpert turrets. For e.g. 50 Xpert turrets, it is mandatory to define at least a range of 50 IP addresses to avoid a blocking condition.
15) On the **Add Exclusions and Delay** dialog click **Next**.
16) On the **Lease Duration** dialog click **Next**.
17) On the **DHCP Options** dialog select „**Yes, I want to configure these options now**” and click **Next**.
18) Enter the Router (Default Gateway) IP address, click **Add**, click **Next**.
19) In the **Domain Name** and **DNS Servers** dialog (validate the Parent domain name and suffix entry), click **Next**.
20) On the **WINS Servers** dialog click **Next**.
21) On the **Activate Scope** dialog select „**Yes, I want to activate this scope now**” and click **Next**.
22) Click **Finish**.
23) Check the scope’s options in the console.

4.1.2.6 Setting up the IPv6

The IP Addressing Mode of System Manager (and Turrets and MLCs) can be set in 3 ways:

- IPv4/IPv6 Dual Stack Mode (default mode)
- IPv4 Only Mode
- IPv6 Only Mode

IMPORTANT:

The supported configuration requires that each component (SMs, Turrets, MLCs) has the same IP Addressing Mode.

For proper operation, the network components (DNS, DHCP, Routers, Firewalls) must be set up in an appropriate and consistent way.

4.1.2.7 IPv4/IPv6 Dual Stack Mode

The OpenScape Xpert component supports IPv4 and IPv6 addresses. This is the default mode.OSX listeners (e.g. Config Server or Turret IP) listen on both, they accept connection on IPv4 and IPv6 too. However, IPv4 is preferred when starting a connection.

4.1.2.8 IPv4 only Mode

The OpenScape Xpert component has no IPv6 address (on none of the network interfaces). OSX listeners listen on only IPv4 and they accept and start connections on only IPv4. The IPv6 protocol must be disabled for all adapters.

Step by Step

1) Follow this navigation path: **Start** > **Control Panel** > **Network and Internet** > **View network status and tasks** > **Change adapter settings**.
2) Select the network adapter you need to update and Right click and select **Properties**.
3) Click on the **Networking** tab
4) Remove the checkmark from the "**Internet Protocol Version 6 (TCP/IPv6)**".
5) Press **OK**.

Next steps

Repeat the same steps for all adapters that need to disable the IPv6 protocol.

4.1.2.9 IPv6 only Mode

The OpenScape Xpert component has no IPv4 address (on none of the network interfaces). OSX listeners listen on only IPv6 and they accept and start connections on only IPv6. The IPv4 protocol must be disabled for all adapters.

Step by Step

1) Follow this navigation path: **Start** > **Control Panel** > **Network and Internet** > **View network status and tasks** > **Change adapter settings**.
2) Select the network adapter you need to update, Right click on the mouse and select **Properties**.
3) Click on the **Networking** tab
4) Remove the checkmark from the "**Internet Protocol Version 4 (TCP/IPv4)**".
5) Press **OK**.

Next steps

Repeat the same steps for all adapters that need to disable the IPv4 protocol.

4.1.2.10 How to Setup DNS (Domain Name Server) for IPv6

NOTICE:

The setup of DNS (Domain Name Server) is not supported by using the IPV6 link-local address.

Step by Step

1) Logon to the system in the OpenScape Xpert domain using the administrator ID and the correct password.
2) To open the DNS Manager click on **Start** > **Programs** > **Administrative Tools** > **DNS** or for **Windows Server 2016 Start – Windows Administrative Tools - DNS)**
3) Select the Forward Lookup Zone "yourdomain.xxx".

   Your server host and its IPv6 address should appear in the list also as **IPv6 Host (AAAA)**. If the entry is missing then do the following:

   - -Right click on the mouse
   - -Select the **context menu**
   - -Select the I**Pv6 Host (AAAA)**"
   - -Fill in the **Name** and **IP address** fields
   - -Check both checkboxes
   - -Click on the button **Add Host**
4) Add Reverse Lookup Zone to your IPv6 network by right clicking at **Reverse Lookup Zone** and in the context menu select **New Zone**.
5) In the Welcome to the New Zone Wizard click **Next**
6) In the **Zone Type** dialog, select the **Primary zone** option and check the **Store the zone in Active Directory** check box and click **Next**.
7) Select **To all DNS servers running on domain controllers in this domain: "yourdomain.xxx"** and click **Next**.

8) Select the **IPv6 Reverse Lookup Zone** setting and click **Next** again.
9) Define the same **IPv6 Address Prefix** used by the DHCPv6 server (e.g. "fd01::/64") and click **Next** to continue
10) Define the **Network ID**. The last digit is grayed out. Click **Next** to continue.
11) Select the **Allow only secure dynamic updates** option and click **Next**.
12) In the **Completing the New Zone Wizard** window, click **Finish**.

    The Reverse Lookup Zone to your IPv6 zone should appear in the list.
13) Right click on he new IPv6 Reverse Lookup Zone and select in the context menu the **New Pointer(PTR)**
14) In the **New Resource Record** dialog complete the Host IP address: and Browse to the associated Host name (Look in DNS > "yourservername" > Forward Lookup Zones > "yourdomain.xxx" > "yourservername") and click **OK** and **OK** again.

    The "yourservername" Pointer with IP address should appear in the list.

4.1.2.11 How to Setup DHCP for IPv6

Step by Step

1) Open the **DHCP Manager** (**Administrative Tools** / **DHCP**).
2) Open the <Server Name> and right-click on **IPv6** and select **New Scope...**

   The **New Scope Wizard** appears.
3) Click on **Next**.
4) Enter the **Scope Name** and **Description**, click **Next**.
5) Enter the **Prefix** (e.g."fd01"), click **Next**
6) Enter the **Start IPv6 Address**, **End IPv6 Address** and click **Next**.
7) Set the **Preferred LifeTime**, **Valid LifeTime** and click **Next**
8) On the **Activate Scope Now** radio button select **Yes**.
9) Click **Finish**.
10) The new scope appears under the IPv6.

4.1.2.12 Default Address Selection for Internet Protocol version 6 (IPv6)-RFC 3484

RFC 3484 describes algorithms, for source and destination address selection for a new connection. The algorithms specify default behavior for all Internet Protocol version 6 (IPv6) implementations. The algorithms are specified as a set of rules that define a partial ordering on the set of addresses that are available for use.

This RFC is implemented within the operating systems (Windows, Linux) and are used by OSX components to select addresses for a new connection.

In dual-stack implementations , the destination address selection algorithm can consider both IPv4 and IPv6 addresses depending on the available source addresses. The default rules prefer IPv6 addresses over IPv4 addresses but OSX applications, in contrast, prefer IPv4 protocols.

4.1.2.13 Useful Commands in IPv6 Context

Show IP Adresses

```
>ipconfig
```

Show DNS Name Resolution for a Host

```
>nslookup {host name}
```

Show Reverse DNS Lookup for an Address

```
>nslookup {host address}
```

Show RFC 3484 Rules

```
>netsh interface ipv6 show prefixpolicies
```

```
>netsh int ipv6 show pref
```

Show Network Connections and Listeners

```
>netstat /nba
```

4.2 Setting Up OpenScape Xpert on the Server

This chapter describes the installation of the OpenScape Xpert V6 system software at the System Manager server.

Prerequisites

Please, read carefully the corresponding software release note before setting up the OpenScape Xpert v6.

4.2.1 How to Initially Install the OpenScape Xpert System Manager

Prerequisites

There’s no OpenScape Xpert installed on the system.

The OpenScape Xpert V7 installation DVD should be in the DVD drive, or the installation files have to be unzipped in a temporary folder on a hard disk drive.

Step by Step

1) Run the `OpenScapeXpertSetup.exe`.
2) Click **Next** on the welcome page.

   The installer checks if there’s no previous version and that the MariaDb is not installed.
3) You can change the default install location, which is `C:\Program Files (x86)\Unify\OpenScapeXpert (hereunder <SM_install_dir>)`. Click **Next**.

4) Select “New standalone server or new cluster” at server type. (Please see chapter “Building the Cluster on page 48” if you want to add the server to a cluster). Click **Next**.
5) Enter the IP address of the License server to be used. Click **Next**.
6) Verify the list of components to be installed. Click **Next**.

NOTICE:

Clicking on **Cancel** at any point during the installation, quits Setup and aborts the installation of the software.

The installer now installs and prepares the required components, starts the services, creates shortcuts to the Windows Desktop and in the Start Menu, updates the Registry and saves the installation log to the <SM_install_dir>, as “Setup Log <date> #<counter>.txt”.

NOTICE:

The System Manager is locked after installation.

Error handling:

If an error occurs during installation, the process will be aborted and the installation has to be started again. In this case please check first the installer logfiles.

The OSX installer and 3rd party installers like the VC Redistributable or MariaDb create logs in the temp folder of the user. Check the TEMP environment variable of the actual path of the folder. It is typically `C:\Users\<username>\AppData\Local\Temp`*. For MariaDB logfiles check for* `MSI*.txt` *files. For VC redistributable log files* `dd_vcredist*.txt` *files. In case an issue with the installer is reported to the support, please attach all *.txt and *.log file from this folder created during the time frame of the installation.*

4.2.2 How to Install License Management

Prerequisites

You need a license key for the System Manager server (MAC address of the active network card).

Step by Step

1) Start the **setup.exe** in the **Tools\Licensing\CLM** folder on the software CD and click **Next**.
2) Keep all settings and click **Next**, again **Next** and **Install**.
3) Start the **setup.exe** in the **Tools\Licensing\CLA** folder on the software CD and click **Next**.
4) Keep all settings and click **Next** and **Install**.
5) Copy the License file and paste it into `C:\Program Files (x86)\Licensing\License Agent\import`.

   The file disappears after a few seconds and the license is active.

4.2.3 Uninstall OpenScape Xpert System Manager

Prerequisite: OpenScape Xpert is installed.

4.2.3.1 How to Uninstall System Manager Using the Installer

Step by Step

1) Run OpenScapeXpertSetup.exe

The installer finds the software that can be removed or upgraded, it asks for your decision about upgrade or remove.

2) Select **Remove the current installation** and click **Next**.

The installer asks you if you are sure.

3) The following choices appear:

The installer asks you if you want to remove the database backup files if the "backups" folder is not empty (See chapter Backup).

- Click **OK** to uninstall, or
- click **No** to exit the installer without uninstalling.

If the installer finds an old version that can’t be removed, an alert is displayed. The alert quits after clicking OK. You have to uninstall the old version using Programs and Features in Control Panel.

4.2.3.2 How to Uninstall System Manager Using Windows Control Panel

Step by Step

1) To remove the System Manager from the system, start the Windows control panel.

2) Select **Programs and Features**.

3) Select **OpenScape Xpert**.

4) Click **Uninstall**.

NOTICE: You have to stop the CLM service during OpenScape Xpert upgrade and uninstall / install processes. You have to enable the service when the OpenScape Xpert software is available again (and the IBM Java is again deployed). If the OpenScape Xpert software is removed but the CLM service runs on the computer then Java should be installed manually.

4.3 Overview of the Installed Components

4.3.1 OpenScape Xpert Management Portal Web GUI

OpenScape Xpert Management Portal (OSXMP) is a web application used for configuring the entire Xpert system. It is the descendant of the Windows application System Manager Admin available in version 5 and before.

Being a web application, one of the supported browsers has to be installed and set as the default browser. The supported browsers are:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Starting the Web GUI

You can start the Web GUI by clicking the shortcuts

- on the Windows Desktop, or
- in the Start Menu / Unify / OpenScape Xpert folder.

When started with shortcuts, the Web GUI opens locally in the default browser. If you would like to use another supported browser, please open it and enter "`https://localhost:8443/osxmp`".

The Web GUI can be opened from another machine in the same network by entering the above URL with the IP address of the server instead of "localhost" in one of the supported browsers.

After installation, login to the OSXMP is possible with a default user.

Default user name: **administrator**

Default password: **Asd123!**.

The default user name cannot be changed, but can be disabled. See section "Use LDAP Authentication".

The default password can be changed with the smdbtool. See section "Change Password".

4.3.2 Java

The OpenScape Xpert Management Portal (OSXMP) on the server side is based on Java EE technology which requires to install the Java on the server. The Java is installed under <SM_install_dir>\Java.

The OSX Installer installs the "IBM Java 11".

The Java is installed under the directory `<SM_install_dir>\Java`.

4.3.2.1 JAVA_HOME variable

A previously installed Java (e.g. Oracle Java) will not cause any problems, but the OSX Installer will overwrite the JAVA_HOME environment variable without any prompt. The OSX components will use the self-installed IBM Java.

NOTICE: Uninstalling the OSX software will not restore the JAVA_HOME variable.

4.3.3 WildFly

WildFly is an open source web application server.

It is the container of the OpenScape Xpert Management Portal (OSXMP). The installer deploys the OSXMP artifact called “osx-mp-ear-1.0-SNAPSHOT.ear”. This .ear file contains the java backend part which is running on the server and the client part which is running in the browser.

It runs under the Windows service „OpenScape Xpert WildFly Service”.

The Wildfly is installed under `<SM_install_dir>\WildFly`. In the directory `<SM_install_dir>\WildFly\standalone` there are the following directories:

- configuration – it contains the „standalone.xml” which is the configuration file of Wildfly
- deployments – it contains the deployed .ear file of OSXMP
- log – it contains the wildfly server log (server.log) and the OSXMP application log (osxmp.log).

Wildfly shares also the files on a http interface used for turret and MLC automatic upgrades. The files can be found under the directory `C:/ProgramData/Unify/`

Wildfly can be configured in two ways (for more details see WildFly documentation at docs.jboss.org).

- Using the administration page : open a browser and enter http://localhost:9990

  http://localhost:9990
- Editing the configuration file "standalone.xml" manually under: `<SM_install_dir>\WildFly\standalone\configuration`

NOTICE:

The service must be stopped before and started after editing the configuration file.

4.3.3.1 How to Create a User to Access the Wildfly Administration Page

Prerequisites

Before being able to use the Wildfly administration page, a management user must be created for Wildfly.

The necessary steps and instructions are shown when accessing the Wildfly administration page before such a user was created. User can be created by launching add-user.bat in `<SM_install_dir>\WildFly\bin>`.

During creating the user follow these steps:

Step by Step

1) Select user type “Management User”,

2) Enter username and password. Select a secure password as suggested.

3) By the question “What groups do you want this user to belong to?” leave the answer empty and press enter.

4) By the confirmation question “About to add user '<username>' for realm 'ManagementRealm'. Is this correct? “ answer “yes”

5) By the question “Is this new user going to be used for one AS process to connect to another AS process?” answer “no”

NOTICE:

When the Wildfly service is started first it deploys the OSXMP “.ear” file. It takes time depending on the server. During this deployment time the Management Portal is not reachable.

4.3.4 Config Server

Config Server communicates with clients (Turrets and MLCs) over TCP using proprietary HTEMS protocol and therefore open a listening port on 9004. It provides configuration data for clients and the clients can save configuration data into the DB via Config Server.

The Config Server provides also the assignment information (association between Turret IP and Node Address). Config Server provides the information for Turrets and MLCs which version of files has to be used for automatic upgrade.

The Config Server also has connection to the Database and to the java backend which is running in the Wildfly service.

If the cluster is built up the Config Server establishes network connection to other Config Server over TCP using own HTEMS protocol.

It runs under the Windows service „OpenScape Xpert Config Server”.

Its files are installed under `<SM_install_dir>`.

4.3.5 Database

OpenScape Xpert stores all configuration data in a MariaDB database management system, which provides also the data replication platform used by the System Manager Cluster.

MariaDB is an open-source relational database management system (RDBMS). For more details see the MariaDB documentation at

https://mariadb.com/kb/en/mariadb/documentation/

It runs as a Windows service called „OpenScape Xpert Database Server”. Its files are installed under <SM_install_dir>\Database.

Data files e.g. logfiles are under C:\ProgramData\Unify\OpenScapeXpert \Database.

The “osx” schema of the database contains the data of the OpenScape Xpert application.

IMPORTANT:

The consistency of the “osx” schema is important for the OpenScape Xpert system, therefore any changes on this schema is forbidden!

4.3.6 License Server

The license server reserves and releases the licenses in the OpenScape Xpert system. The License server is connected over SSL connection to the License Agent (CLA) Windows service. CLA administrates the licenses and can be queried using License Management (CLM).

The License Server runs as a Windows service called „OpenScape Xpert License Server”.

Its files are installed under `<SM_install_dir>`.

4.3.6.1 OpenScape Xpert V7 Licensing

In V7 R0 new floating license concept is introduced. There are two types of licenses - Basic Client and Full Pages.

When an OSX client is logging in a "Basic Client" license is reserved. If the profile has more than two pages, an additional "Full Pages" license is reserved. When the OSX client logs out, the reserved licenses are released.

If no more Basic User License can be reserved, no more OSX Client can login. In case of cluster configuration, only one Basic User License is reserved per client, no matter what SM it connects to the License Server.

If there are free Basic Client licenses but no more free Full Pages licenses in the CLA, user can login only with profiles with a maximum of two pages.

If the License Server stops, all reserved license are released in CLA. If the License Server starts, the licenses are reserved again.

In case the license server is temporarily unavailable the system keeps running. Each Config Server stores a timestamp and maximum number of licenses (based on the last successful response from License Server) and a grace period will be started. The grace period offers time for service to detect and solve the problem in the License Server.

During the grace period:

- The Config Server manages licenses separately from each other.
- The turret displays a dialog after the login: “The license server is currently not available. Login is only allowed temporarily”.
- The following licensing modes are available:
  - **Subscription Based** licensing (7 days of grace period).
  - **Perpetual** licensing (30 days of grace period).
- If the License Server returns, the system will be normalized without any additional action.
- After the grace period a login is no more possible without License Server.

4.4 Database Administration

The database management system (DBMS) installed and used by OpenScape Xpert cannot be used for any other purposes. Changes are only allowed by Unify Software and personnel except what is described in this chapter except what is described in this chapter.

4.4.1 Using the OpenScape Xpert Management Portal (OSXMP)

4.4.1.1 Backup Location

Backups created by the Management Portal are stored either in a local folder (<Program Data>\Unify\OSXMP\backups or on a network share depending on the settings on the Management Portal/System Properties/General Tab Backups.In case of a network share the SM server needs read/write access to it, because NetworkService account presents the computer’s credentials to remote servers. On the sharing window the <domain name>\<sm server name> $ account needs to be added and the “Permission Level” has to be set to read/write for that user. In case of a cluster each SM uses the same share and needs the same access to the share and please sure that files created by one of the accounts can be deleted by the others.

To set up encrypted data transfer over the network the encryption must be enabled in PowerShell for the shared folder:

```
Set-SmbShare –Name <sharename> -EncryptData $true
```

IMPORTANT:

Enabling encryption on the share will result, that only SMB V3 clients can access the share. SMB V3 was introduced in

Windows 8 and Windows Server 2012. Earlier versions of Windows will not be able to access the share.

4.4.1.2 Backup Tasks

You can list, create, delete and download database backup files after selecting Database Backups in the side navigation.

- List: Displays the available database backup files with their creation date and time (UTC).
- Create: Saves the database as an SQL file backup folder. The given file name will be extended with the creation date and time (UTC) and the software version.
- Delete: Deletes the selected database backup file(s) from that folder.
- Download: Copies one selected database backup file into the default download directory of the PC where OpenScape Xpert is running in a browser.

4.4.2 Using SMDBTOOL

For database administration tasks OpenScape Xpert has an own tool called smdbtool with the following features:

- Backup
- Restore
- Attach/Detach a host to/from the cluster
- Check cluster state
- Repair after an unsuccessful cluster attach

4.4.2.1 SMDBTOOL - General Usage

To run Smdbtool you have to open a console window with administrator rights in <SM_install_dir>\databasetools

Usage syntax:

```
smdbtool {command} [options] parameter(s)...
```

When `smdbtool` is started without any parameters, it lists the supported commands.

`smdbtool help` command provides help about the specific command.

4.4.2.2 Backup

The smdbtool command “`backup`” can be used for backup all data stored in the database.

Usage syntax:

```
smdbtool backup backupfile
```

The created backup file contains SQL statements which create and populate the database. Backup can be used for transferring the OSX database to another host.

4.4.2.3 Restore

Smdbtool command “restore” can be used to restore a previously created backup.

Usage syntax:

```
smdbtool restore backupfile
```

Restore has the following steps:

- Stop ConfigServer and Wildfly services
- If this host is part of a cluster, detach from there
- Restore the database from the file
- Upgrade the database schema and data
- Update the data with installation and version specific data
- Start the ConfigServer and Wildfly services

After a restore, the database contains only the local host. Its locked state is set as it was set at creating the backup. If it was part of a System Manager cluster, the cluster has to be built up again. See chapter SystemManager Cluster.

4.4.2.4 Analyze

Smdbtool command “analyze” can be used to check the database health against consistency issues (occurred e.g. during migration process).

Usage syntax:

```
smdbtool analyze
```

Analyze provides detailed logs about inspected database consistency rules and their result and gives a summary about database health.

NOTICE:

This command is used to mitigate the risk of inconsistency issues in database.

4.4.2.5 Other Functions of SMDB Tool

Cluster Related Functions

`Smdbtool` is also used for attaching and detaching a host to the cluster with “attach” and “detach” commands. It is also possible to check the state of the

cluster with “check” command. These are described in chapter System Manager Cluster.

Repair Database Privileges

`Smdbtool` “attach” function changes the database privileges temporary. If the function fails, the privileges may not be restored. `Smdbtool` command “repair” sets the database privileges to their normal state.

Usage syntax:

```
smdbtool repair
```

4.4.2.6 Create API User

Smdbtool command `createapiuser` can be used to create the user for API.

Username is hardcoded: `osxmpapiuser`

For the API usage the API user has to be activated (API calls are working just with the API user). The API user cannot be deleted or deactivated.

Usage syntax:

```
smdbtool createapiuser
```

```
smdbtool createapiuser -p <password>
```

Without -p parameter the password for API user is requested. To change the password of API user you can use the `changepwd` command without `keystoreonly` parameter.

4.4.2.7 Change Password

`Smdbtool` “changepwd” function changes the password for the following users:

- Replicator User
- API User
- Administrator User

The -k parameter can be used to change the password of the Replicator User or the Config Server User only in the keystore.

Usage syntax:

```
smdbtool changepwd -u <user> -p <new password> [-k <true|
false>]
```

Supported users for this command are: `replicator, osxmpapiuser, administrator`

4.4.2.8 Password complexity check for the Administrator and API User password

You can easily enable or disable the password complexity check from **Management Portal** > **System Properties** > **Security Tab**.

When the password complexity check is enabled, and you use the smdbtool createpiuser or changepwd command, the Administrator and Api user passwords must comply with the following password complexity criteria:

- It must be at least 15 characters long.
- It must contain at least 1 lowercase character.
- It must contain at least 1 uppercase character.
- It must contain at least 1 digit.
- It must contain at least 1 special character (!@#&()û[{}]:;',.?/*~$^+=<>).
- It must not match the last 5 passwords.

NOTICE: Do not use language-specific special characters.

You can also configure the password lifetime check.

- To disable the password lifetime check, set the corresponding value to 0.

  When disabled, password lifetime is not checked while the password complexity is checked.
- To enable the password lifetime check, set the corresponding value to the number of days until the password expires.

  When enabled, the password will expire after the number of days you have set. After the password expires, it can no longer be user and you must change it.

To prevent malicious attempts to break a user's password, the portal monitors the number of failed authentication attempts in the last 15 minutes after the current login attempt. If there are three consecutive failed login attempts,the user cannot log even if the correct password is provided. The user will be able to access the portal again after 15 minutes.

4.4.3 Database Access

4.4.3.1 Administrator User

The MariaDB DBMS installed by OpenScape Xpert has an administrator user which is not used by the software after the installation. The user name is ‘OsxMysqlAdmin’ and the password for it is ‘MySqlAdmin1234!’. This user can be used only locally. The password can be changed with the following command:.

```
mysql -u OsxMysqlAdmin -pMySqlAdmin1234! -e "UPDATE
mysql.user SET Password = PASSWORD('NEW_PASSWORD') WHERE
User = 'OsxMysqlAdmin'; FLUSH PRIVILEGES;"
```

4.4.3.2 Read-only User for Queries

It is possible to create a user for direct database access, however the following rules must be kept:

- No change can be made in the osx and osxtemp schemas (read-only access)

- Active host is not used: use either a System Manager in cluster which is not primary in any location or if online data access is not required, a system where a database backup is restored (This is required, because wrongly written queries can lead to unwanted DB locks or performance issues on the local machine.) If access to the osxtemp schema (which stores the Action Key states) is not required, the best is to lock this System Manager on the Management Portal

Create user:

```
mysql -u OsxMysqlAdmin -pMySqlAdmin1234! -e "CREATE USER
'myreadonlyuser' IDENTIFIED BY 'password'; GRANT SELECT ON
`osx%`.* TO 'myreadonlyuser'@'%'; FLUSH PRIVILEGES;
```

Remark: The osx% is surrounded with backticks!

Change user password:

```
mysql -u OsxMysqlAdmin -pMySqlAdmin1234! -e "SET PASSWORD
FOR 'myreadonlyuser' = PASSWORD('NEW_PASSWORD'); FLUSH
PRIVILEGES;"
```

Delete user:

```
mysql -u OsxMysqlAdmin -pMySqlAdmin1234! -e "DROP USER
'myreadonlyuser';"
```

The commands above use username 'myreadonlyuser' and password 'password', but they can be altered.

4.5 System Manager Cluster

4.5.1 Overview

System Manager Cluster allows more System Managers to be used in one OpenScape Xpert system.

- System Managers have different priorities for clients (turrets and MLCs) that belong to a location. There can be only one System Manager with the highest priority (primary server) in a location. The others are backup servers with different or equal priorities.
- This solution can be used for a standby/backup server solution. If the primary server is down or not reachable, one of the backup servers will take over the functionality of the primary server.
- This solution can be used also for a distributed server solution. The turrets are in different locations, connected to different (nearest, primary) servers. In case of a server is down or not reachable the turrets, for this server is the primary, connect to another server (based on the priority list of that location).
- The System Manager servers can be located geographically separated but must be connected with a LAN/WAN connection.
- The System Managers to be connected must have exactly the same version installed.
- Each System Manager must be accessible for the SM, turrets, and MLCs of the remote sites via TCP (HTEMS).

- Each server that has been installed as a System Manager Cluster Node must be synchronized to the same time source.

NOTICE:

System Manager Cluster feature is supported in an IPV6 environment and the IP addresses can be set as IPV6 in the cluster command.

4.5.2 Data Replication

The System Manager Cluster uses the Database built in data replication mechanism. This is a multi-master asynchronous replication.

- It is **multi-master** because data written on any server is replicated to the other servers.
- It is **asynchronous** because the write operation returns successfully if the write operation is done on the local server, replication is done asynchronously after the write operation.
- **Errors** in the replication do not cause errors in the application using the database.

Multi-master replication is achieved by creating two replication routes between all two servers of the cluster; one for each direction. Data changed on any servers is pulled by all the other servers.

During attaching an SM to the cluster, the initial data set is moved to the newly attached SM. In a working replication, only changed data is moved from one SM to the other.

4.5.3 Failover and Failback

Failover

- If the primary SM becomes unavailable, the connected turrets and MLCs start connecting to the next highest priority backup SM of that location.
- If there are more than one backup SMs with this priority, the clients select randomly where to connect.
- Until the connection to the backup is built up, turret users can’t save any changes in their profile. This temporary state can take up to 90 seconds and the users are visually informed about it.

Failback

- If a turret or MLC is connected to a backup SM, and the primary SM becomes available again, the turret/MLC will switch back to the primary SM.
- Turrets and MLCs have all the features while connected to a backup SM too. Data can be read and written, all messages are routed to the right place. As soon as the primary SM is up again, the data written on the other SMs is immediately replicated to it.

4.5.4 Building the Cluster

There are two options to attach a backup server to the cluster:

- Attach backup server during System Manager installation.
- Attach backup server after System Manager installation.

4.5.4.1 How to Attach a System Manager to the Cluster During System Manager Installation

Prerequisites

At least one running OSX System Manager server is needed.

IMPORTANT:

Never run attach on multiple System Managers at the same time. This can cause that the original system stays in a not working state and has to be repaired.

Step by Step

1) Run `OpenScapeXpertSetup.exe`

2) Click **Next** on the welcome page.

The installer checks if there's no previous version and the MariaDB is not installed.

3) You can change the default install location. Click **Next**.

4) Select " Add this server to an existing Cluster" at **server type** and click **Next**.

5) Enter the IP address of any server already in the cluster (or the other server's IP address if there's no cluster yet) and click **Next**.

6) Enter the IP address of the server that will act as license server.

7) Verify the list of components to be installed and click **Next**, then **Finish** at the end.

The installer now installs the required components, builds the cluster, starts the services, creates shortcuts to the Windows Desktop and in the Start Menu, updates the Registry and saves the installation log to the `<SM_install_dir>, as "Setup Log <date> #<counter>.txt"`.

The log of smdbtool is saved as `<SM_install_dir>\databasetools \smdbtool_cluster_log.txt`.

NOTICE:

Clicking on Cancel at any point during the installation, quits Setup and aborts the installation of the software.

IMPORTANT:

In both cases, if the servers have more IP addresses use an IP address visible from the other server.

IMPORTANT:

Attaching a node to a cluster is only possible if the cluster is working fine. It is automatically checked before the attach.

IMPORTANT:

If the process fails at some point, the cluster (or only the other server) might stay in a non working state.

Command `smdbtool check` can be used to get diagnostic data about the cluster.

Run `smdbtool repair` on any node of the cluster in order to restore DB privileges. No data is modified with this command, only user privileges are modified and services are restarted.

If any replication was built up before the failure, they need to be deleted before an attach is tried again. This can be done with `smdbtool detach` command.

IMPORTANT:

During an attach, OSX system will not work with full functionality.

IMPORTANT:

Attach adds the new SM with priority “Backup Level 5” to each location if it was not part of the cluster previously. Otherwise the priorities are not changed.

NOTICE:

The System Manager is locked after adding it to the cluster either during or after installation.

4.5.4.2 How to Attach a System Manager to the Cluster After System Manager Installation

Prerequisites

At least one running OSX System Manager server is needed.

Step by Step

1) Install the OSX SM on the backup server as a standalone server.
2) On the backup server run the command:

   `smdbtool attach -r <Remote IP address> -l <Local IP address> where:`

   `<Remote IP address>` is the IP address of any server already in the cluster (or the other server’s IP address if there’s no cluster yet),

   `<Local IP address>` is the IP address of the backup server.

3) The log of smdbtool can be checked in the command window.

IMPORTANT:

In both cases, if the servers have more IP addresses use an IP address visible from the other server.

IMPORTANT:

Attaching a node to a cluster is only possible if the cluster is working fine. It is automatically checked before the attach.

IMPORTANT:

If the process fails at some point, the cluster (or the only other server) might stay in a non working state.

Command `smdbtool check` can be used to get diagnostic data about the cluster.

Run `smdbtool repair` on any node of the cluster in order to restore DB privileges. No data is modified with this command, only user privileges are modified and services are restarted.

If any replication was built up before the failure, they need to be deleted before an attach is tried again. This can be done with `smdbtool detach` command.

IMPORTANT:

During an attach, OSX system will not work with full functionality.

IMPORTANT:

Attach adds the new SM with priority “Backup Level 5” to each location if it was not part of the cluster previously. Otherwise the priorities are not changed.

NOTICE:

The System Manager is locked after adding it to the cluster either during or after install.

4.5.4.3 How to Check Database Cluster

Step by Step

Run the `smdbtool check` command.

The following diagnostic information about the cluster is shown:

- Nodes in cluster.

- A replication connection exists between every 2 nodes (in both direction).
- The replications are working.
- A Config Server exitst in the database for every node.
- User privileges are set correctly.

4.5.4.4 Centralized Licensing

In a cluster architecture, the **Centralized Licensing** must be configured for licensing purposes. For this, one SM must be selected as **Central License Server**. On the Central License Server SM host, the **License Agent (CLA)** must be installed together with the **License Manager CLM**. The license file must be activated. On the other SM(s) of the cluster, only the CLA must be installed.

Example configuration with two SMs:

The License Server and License Agent (CLA) on SM1 is the central license server.

The license file is activated in License Manager (CLM) on SM1.

On the SM2, only the CLA is installed.

On the SM2, during the installation the **Add this server to an existing cluster** option must be used.

For adding the local IP address and the IP address of a cluster member, the License Server IP must be set. This is the Central License Server SM IP address.

The local IP address and the IP address of a cluster member must be set in the License Server IP. This represents the IP address of the Central License Server SM.

The Central License serer IP address is saved in the registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unify\Trading E
\Systemmanager LicenseServer]

"LicenseServerHost"="<IP Address of Central License Server
SM>"
```

If it is manually set, then Config Server must restart.

Once the setup is completed, the SM2 will reserve and release licenses from SM1 license Server.

If the **License Server** is not reachable from SM2, then a notification message will be displayed on the dashboard of SM2 and the grace period is started for SM2.

4.5.5 Overview on the System Manager GUI

Cluster List

Click on **System Managers** in the side menu to see the list of System Managers in the cluster - including the local SM - with status indication of the Config Server of that System Manager as follows:

Symbol	Description
Green dot	Remote SM, connected correctly.
Red dot	Remote SM Server, not connected.
White circle	Local SM
Question Mark	Remote SM, status unknown (cannot be requested from the local Config Server).

OSX Client/MLC List

In cluster the clients (OSX Client / MLC) have the following states.

Symbol	Description
White circle	The client is unassigned.
Green circle	The client is connected to its primary server.
Yellow circle	The client is connected to one of its backup servers.
Red circle	The client is disconnected from the cluster.
Question Mark	Status unknown when the local Config Server is stopped.

4.5.6 How to Detach a System Manager from the Cluster

- Any System Manager can be detached from the cluster using smdbtool.
- The command can be issued on the SM that's to be detached or on any other.
- The System Manager can be removed from the cluster by simply uninstalling the OSX software from the SM.

Step by Step

1) The following command has to be executed: `smdbtool detach -h <IP address to be detached> [ -ch <cluster IP address> ]`

The optional `-ch` parameter has to be given if the node to be detached is not available from the cluster (e. g. the computer is damaged). The node specified here is used to get the list of cluster nodes.

IMPORTANT:

Ater this command all turrets that were connected to the detached SM (e.g. due to a network issue) will stay there permanently, so make sure that they are connected to another SM before executing this step.

---

2) The log of smdbtool can be checked in the command window.

IMPORTANT:

If a detached node was not available at the time of detach (e.g. network was not available or the computer was damaged) a detach (or uninstall) has to be run on the node when it becomes available again.

4.5.7 Restore Database in Cluster

If the SM is in cluster, smdbtool restore automatically detaches the cluster. It has to be rebuilt using smdbtool on the backup servers.

IMPORTANT:

If the SM is not in the restored DB (i.e. it was not part of the cluster previously where the backup was created), the SM is added to the priority list of each location with priority “Backup Level 5”.

4.5.8 How to change replicator user password

Using smdbtool command `changepwd` the password of replication DB user can be changed:

```
smdbtool changepwd -u replicator -p <new password>
```

NOTICE:

Before changing the password on SM, the administrator has to prevent all DB changes. So the SM(s) has to be locked. After changing the password it has to be unlocked.

If the replicator user password is changed it is recommended to change it before the SMs is attached.

4.5.8.1 How to change the password before creating a cluster

Step by Step

1) Lock SMs

2) Change password on all standalone SMs to the same password

3) Unlock SMs

4) Attach SMs together with the attached command

4.5.8.2 How to change the password in an existing cluster

Step by Step

1) Lock SMs
2) Change password on SM1
3) The replication status of SM2 has a temporary error.
4) Change the password on the SM2
5) Check if the replication status on both SMs in the System Manager list is OK.
6) Unlock SMs

4.5.8.3 How to enhance an existing cluster with 1 SM

In the existing cluster the password is already changed. You have to follow the steps below to enhance the existing cluster:

Step by Step

1) Install new SM as standalone
2) Change the password on the new SM to the password as used on other SMs
3) Attach the new SM to the cluster with the attached command

---

NOTICE:

If the replicator user password is already changed on the SM1 the SM2 can not be attached to the SM1 using installer. In this case install first the SM2 as standalone system than change the password on SM2 and then attach SM2 to SM1 using smdbtool.

4.6 Logging

4.6.1 WildFly and OSX Management Portal Server Side

On the server side the WildFly application server logging will be used. It can be configured on the administration page of WildFly (`http:\\localhost:9990`).

Description of how to setup the administration page can be found in the chapter *3.3.2 “Overview of the Installed Componenets - Wildfly*”

- In the upper and left side menus select Configuration / Subsystems / Logging. Press the button “**View**” next to the menu.
- The log level can be set by editing the com.unify.osx.osxmp category’s Level attribute on the LOG CATEGORIES tab.
- The log file size and rotation number can be set by editing the osxmp_sizehandler handler on the HANDLER tab after selecting the “**Size**” menu.
  - Edit “**Max backup index**” for the number of log files kept.
  - Edit “**Rotation size**” for the size of one log file.

- The WildFly creates the log files in a separate log directory:

  `<SM_install_dir>\WildFly\standalone\log`

  In this directory there is the server.log file which is the WildFly own log file and the osxmp.log which is the server side log file of the OSXMP application.

4.6.2 Config Server

Logging can be enabled and configured in the `SmConfigServer_logger.lcp` file which can be found in the `<SM_install_dir>`.

- Logs are written to the file(s) `SmConfigServer_log.txt` in the `%ProgramData%\Unify\OpenScapeXpert\Logs`.
- The **log level** can be changed by changing the value of the `log4cplus.rootLogger key`.
- The **size** of the log file can be changed by changing the value of the `log4cplus.appender.File.MaxFileSize key`.
- The **number** of the log files can be changed by changing the value of the `log4cplus.appender.File.MaxBackupIndex key`.

NOTICE:

Never enable DEBUG level logging for a Config Server in a system with a large number of turrets as this can add a certain level of additional load on the server and can cause system slowdowns and turret and MLC connection issues.

4.6.3 OSX Management Portal Client Side

On the client side (running in browser) there is no way to change the log settings. The portal writes the log in the Browser JavaScript console, the log level is preset to INFO.

The log on the client side will not be saved into a separate log file. It means the user cannot see the history of the user actions in a log file on browser side. If there is an error on the client side the user has to reproduce the use case to see the logs entries in the JavaScript console.

To open the JavaScript console press **F12** in the browser and select the **Console** tab.

4.6.4 License Server

Logging can be configured the same way as for the ConfigServer.

The log configuration file is `SmLicenseServer_logger.lcp` and the log output file is `SmLicenseServer_log.txt` at the same location (`%ProgramData%\Unify\OpenScapeXpert\Logs`).

4.6.5 SmDbTool

Log settings for the SmDbTool cannot be changed. The log is written to the `<SM_install_dir>\ databasetools\smdbtool.log` file.

4.6.6 Installer

Log level of the installer cannot be set.

After a successful install the logs can be found in the `<SM_install_dir>\Intall_Log.txt`.

During install and if the installer fails the log files can be found in the folder `C:\Users\<Username>\AppData\Local\<TempName>\*.log;*.txt`

where:

- `<Username>` is the name of the user running the installer.
- `<TempName>` is a temporary folder name. Can be found by looking for the latest created folder.

The folder can be different if Windows temp folder is configured to a different place.

NOTICE:

On failure collect the logs before closing the error window, because exiting the installer can delete log files.

4.7 Security

The OpenScape Xpert V7 System Manager is not completely secured by default after installation. Several steps need to be done to have a secure system.

4.7.1 How Secrets Are Stored in Wildfly

4.7.1.1 The credentialStore.bcfks file

The **credentialStore.bcfks** file contains the `https.keystore` password.

The secret key used for encrypting the passwords in the credential store, is kept in the `keystore.bcfks` file.

The keystore.bcfks file

keystore: keystore.bcfks

key type: AES

key alias: key

Contains the secret key for encrypting the passwords in the credential store.

The keystore.bcfks file is installed by default in the <INSTALL_DIR>\Wildfly\credentialStores directory.

The default credential store master password is “Asd123!.” and it is stored as an encrypted expression in the secretKey.store file.

Other secrets (e.g. passwords) can be stored in the credentialStore.bcfks file using <INSTALL_DIR>\WildFly\bin\elytron-tool.bat.

The credentialStore.bcfks file is installed by default in the <INSTALL_DIR>\Wildfly\credentialStores directory.

4.7.1.2 The secretKey.store file

The **secretKey.store** file is a secret-key-credential-store that provides the credential store master password. The password is stored in AES encrypted format.

This file contains credentialStore.bcfks access and it is installed by default in the <INSTALL_DIR>\Wildfly\credentialStores directory.

4.7.1.3 The https.keystore file

default password of keystore: Asd123!.

default password of key: Asd123!.

keystore type: PKCS12

key alias: osx-sm1

contains: certificate for https connection to OSXMP from Browser

The https.keystore file is installed by default in the <INSTALL_DIR>\Wildfly\credentialStores directory.

At installation, the https.keystore file contains a self-signed certificate which is generated for the name localhost and ip address 127.0.0.1.

4.7.1.4 The osx.truststore file

The osx.truststore file is installed by default in the <INSTALL_DIR> \Wildfly\credentialStores directory and it is empty.

If LDAPS is configured, the file must contain trusted CA certificate(s) for secure LDAP login on OSXMP.

default password of keystore: Asd123!.

password of key: <by default no key; should be same as password of the keystore>

key alias: osx-ca

4.7.1.5 How to Use https in Browser

The new URL is `https://localhost:8443/osxmp` or `https://CN:8443/osxmp` (its depends on the certificate setting, CN is your computer name or IP address).

Step by Step

1) If your certificate needs to be accepted by **Microsoft Edge** or **Chrome**, go to **Settings**.
   a) In **Chrome**, go to **Privacy and security** > **Security** > **Manage device certificates**.

      In **Microsoft Edge**, go to **Privacy, search, and services**, scroll down to the **Security** area and select **Manage certificates**.
   b) On the **Trusted Root Certification Authorities** click **Import** and then **Next**.
   c) Browse for the root CA certificate (e.g. ca.crt), click **Next** and then **Finish**.

2) In Firefox:
   a) When activating the SSL with a self-signed certificate, choose the option: **I Understand the Risks -> Add Exception -> Confirm Security Exception**.
   b) If the certificate was signed with a CA, go to **Options -> Advanced -> Certificates -> View Certificates -> Authorities -> Import**.
   c) For the question “Do you want to trust CA for the following purposes?” check **Trust this CA to identify websites**.
   d) Confirm with **OK**.

4.7.2 Keystore and Elytron tool commands

The following commands can be executed using the Windows Command Prompt. In case the commands contain the password of the keystore or the credential store in clear text, it is strongly recommend to close the Command Prompt window after the execution of the commands in order to delete the history.

Several commands contain a path in the options, such as keystore or providerpath. In these examples, the `<INSTALL_DIR>` is used and it must be changedproperly.

IMPORTANT: Using the WildFly Elytron tool to modify a credential store that is in use by a running JBoss EAP server can result in losing the changes in the store. To prevent this, stop the Wildfly service before using the Elytron tool commands.

4.7.2.1 How to list the content of the keystore.bcfks and the credentialStore.bcfks file

The content of the keystore.bcfks file can be displayed using the following command, where the keystore file is a parameter:

```
"%JAVA_HOME%\bin\keytool" -list -keystore "<INSTALL_DIR>
\WildFly\credentialstores\keystore.bcfks" -
```

```
storetype BCFKS -storepass Asd123!. -providerClass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
-providerPath "<INSTALL_DIR>\WildFly\modules\org
\bouncycastle\fips\main\bc-fips-1.0.2.3.jar" -v
```

The content of the credentialStore.bcfks file can be displayed using the following command in the directory where elytron-tool.bat is instaled (`<INSTALL_DIR>\WildFly\bin`):

```
elytron-tool.bat credential-store --location ".. 
\credentialStores\keystore.bcfks" --password Asd123!. -u
"keyStoreType=BCFKS;external=true;keyAlias=key;externalPath=..
\credentialStores\credentialStore.bcfks" --aliases
```

4.7.2.2 How to list the content of the https.keystore file

The content of https.keystore can be displayed with the following command, where the keystore file is a parameter:

```
"%JAVA_HOME%\bin\keytool" -list -keystore "<INSTALL_DIR>
\WildFly\credentialstores\https.keystore" -storetype PKCS12
-v
```

At prompt the keystore password of https.keystore has to be entered.

4.7.2.3 How to change the credential store password

The credential store password can not be changed. In case a change of password is needed, the credential store (credentialStore.bcfks) and keystore (keystore.bcfks) must be deleted and new ones must be created. The credential store and keystore password and the key in the keystore must be the same.

The Wildfly service must be stopped.

To create the keystore with a new secret key (keystore.bcfks), use the following command:

```
"%JAVA_HOME%\bin\keytool" -genseckey -alias key -
keyalg AES -keysize 256 -keystore "<INSTALL_DIR>
\WildFly\credentialstores\keystore.bcfks" -
storetype BCFKS -storepass <NEW PASSWORD>
-keypass <NEW PASSWORD> -providerClass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
-ProviderPath "<INSTALL_DIR>\WildFly\modules\org
\bouncycastle\fips\main\bc-fips-1.0.2.3.jar"
```

To create the credential store with `https.keystore` password, run the following command in the `<INSTALL_DIR>\WildFly\bin` directory:

```
elytron-tool.bat credential-store -c -a
https_keystore_password -x "nsms(7mjr5kY" -p <NEW
PASSWORD> -l "../credentialStores/keystore.bcfks" -u
"keyStoreType=BCFKS;external=true;keyAlias=key;externalPath=../
credentialStores/credentialStore.bcfks"
```

NOTICE: The same name (credentialStore.bcfks) must be used.

NOTICE: An alias must be defined when creating the credential store (e.g. the https_keystore_password).

Next, change the old password to the new one in the the `standalone.xml`:

1) Generate the new encrypted expression:
```
"../credentialStores/secretKey.store" --type
 PropertiesCredentialStore --encrypt key
```
Enter `<NEW PASSWORD>` when prompted to enter a “Clear text value”, then confirm it.

2) Change `standalone.xml`.

Copy the token resulted from the previous command and paste it into the `standalone.xml` file:
```
<credential-reference clear-
text="${ENC::osxmp_resolver:<ENCRYPTED_EXPRESSION_TOKEN>}"/
>
```

Finally, add further passwords with the alias defined in the old credential store.

Once all the steps are completed, start the Wildfly service.

4.7.2.4 How to change certificates in https.keystore

If the default self-signed certificate has to be replaced in the https.keystore to a RootCa signed certificate do the following steps:

- Delete certificate from the http.keystore with the following command:

```
" %JAVA_HOME%\bin\keytool" -delete -keystore "
%<INSTALL_DIR>\WildFly\credentialStores\https.keystore" -
storetype PKCS12 -alias osx-sml -v
```

At prompt the keystore password of https.keystore has to be entered.

- Generate self-sign certificate into the https.keystore:

```
"%JAVA_HOME%\bin\keytool" -genkeypair -
keystore "<INSTALL_DIR>\WildFly\credentialStores
\https.keystore" -storetype PKCS12 -alias osx-
sm1 -keyalg RSA -keysize 2048 -dname "CN=<Server
FQDN>,OU=<OrgUnit>,O=<Company>,L=<location>,ST=<location>,C=<country>"
-validity 10950 -ext SAN=IP:<Server IP Address> -v
```

For alias name it is recommended to use the server name. The validity parameter in the example is set to 10950 day (about 30 years). The most important setting is the CN which is requested with "What is your first and last name?" which has to be set to the FQDN of the server. With -ext option it can be set additional extensions in the certificate. In the above example the SAN (Subject Alternative Name) IP address is set with Server IP address.

- Create CSR - Certificate Signing Request file:

```
"%JAVA_HOME%\bin\keytool" -certreq -keystore "<INSTALL_DIR>
\WildFly\credentialStores\https.keystore" -storetype PKCS12
-alias osx-sm1 -keyalg RSA -file "<INSTALL_DIR>\WildFly
\credentialStores\osx-sm1.csr" -v#
```

With the above mand a .csr file will be generated to the path what is set in -file option.

The .csr file has to be signed on RootCa. Then the RootCa certificate and the certificate chain file (p7b) have to be downloaded from the RootCa.

- Import RootCa certificate file on alias ca:

```
"%JAVA_HOME%\bin\keytool" -import -keystore "<INSTALL_DIR>
\WildFly\credentialStores\https.keystore" -storetype PKCS12
-alias ca -file "<INSTALL_DIR>\WildFly\credentialStores
\<rootca.crt>" -noprompt -v#
```

- Import certificate chain file (.p7b) on alias osx-sm1:

```
"%JAVA_HOME%\bin\keytool" -import -keystore "<INSTALL_DIR>
\WildFly\credentialStores\https.keystore" -storetype
PKCS12 -alias osx-sm1 -file "<INSTALL_DIR>\WildFly
\credentialStores\certnew.p7b" -v##
```

In this example the p7b file is called certenew. It has to be imported into the same alias where the generated self-signed certificate resides (osx-sm1). The downloaded certnew.p7b file in this example is on **<INSTALL_DIR>\WildFly \credentialStores path.**

4.7.3 How to use your own certificate for HTTPS

This chapter describes how to use the already issued certificate for https of OSXMP in https.keystore.

The following parameters have to be set for generated certificate / keystore file:.

- It has to be issued for webserver:
- It has to contain private key also
- Its format is PKCS12 (e.g. .pfx file)
- The password has to be the default of https.keystore (Asd123!.) or the changed password of https.keystore

The already existing https.keystore has to be deleted. The exported PKCS12 file has to be copied into `<INSTALL_DIR>\WildFly\credentialStores` and renamed to https.keystore.

Because the generated alias is sufficient, it has to be changed to osx-sm1. First list the https.keystore as described above and copy the generated alias.

- Change the alias in the https.keystore with following command:

  ```
  "%JAVA_HOME%\bin\keytool" -changealias -keystore
  "<INSTALL_DIR>\WildFly\credentialStores\https.keystore"
  -storetype PKCS12 -alias <generated alias> -destalias
  osx-sm1 -v#
  ```

- Import the rootCA certificate into the https.keystore:

  ```
  "%JAVA_HOME%\bin\keytool" -import -keystore
  "<INSTALL_DIR>\WildFly\credentialStores\https.keystore"
  -storetype PKCS12 -alias ca -file <rootca.crt> -noprompt
  -v##
  ```

After these steps the OpenScape Xpert Wildfly Service has to be restarted.

NOTICE:

The Windows system must trust the CA certificate used. If the CA certificate is imported on Windows server, the Chrome and Microsoft Edge browsers will display OSXMP as secure site.

The Firefox browser uses own certificate store and CA certificate must be imported as Authority to display as secure site.

4.7.4 How to configure Passwords in Wildfly

For several special settings, a password must be included in the Wildfly standalone.xml configuration file (e.g. password for LDAP connection or HTTPS keystore). It is recommended to hide them with Wildfly's Credential Store feature.

A credential store contains sensitive encrypted data. The encryption key is stored in a keystore file. The key is AES encrypted.

4.7.4.1 How to add a password to the credential store

To add a password with alias to the credential store, the `<INSTALL_DIR>\WildFly\bin\elytron-tool.bat` must be used. It initializes the connection with the credential store. Therefore, the credential store password must be added.

To add a new password with alias use the following command:

```
elytron-tool.bat credential-store --location
"..\credentialStores\keystore.bcfks" --
password <CREDENTIAL_STORE_PASSWORD> -u
"keyStoreType=BCFKS;external=true;keyAlias=key;externalPath=..
\credentialStores\credentialStore.bcfks" --add <NEW_ALIAS>
--secret <ALIAS_PASSWORD>
```

NOTICE: You can omit the secret argument from the command. In this case, you will be prompted to enter the secret manually, using standard input.

If the credential store initialization is successful and the new alias has been created, it is possible to change the clear text password in the standalone.xml as follows:

```
<credential-reference store="osxmp_credentialstore"
alias="< NEW_ALIAS >"/>
```

4.7.5 Secure Connection Between License Server and Config Server

Since Thrift is a clear-text protocol, the communication is encrypted with Mutual TLS (M-TLS).

The implementation of OpenSSL is used for both client and server authentication that is shipped together with the thrift library. The System Manager currently uses default certificates from this path:

```
<SM_install_dir>/certificates/licenseserver/
```

4.7.5.1 How to Turn On Host Name Verification

When the System Manager installed, then host name verification is inactive. If you want turn on the host name verification follow these steps:

Step by Step

1) Set HKEY_LOCAL_MACHINE\SOFTWARE\Wow64\Node\Unify\Trading E\Systemmanager LicenseServer\AllowAccessAllHost to “0” (turn on host verification).
2) Set HKEY_LOCAL_MACHINE\SOFTWARE\Wow64\Node\Unify\Trading E\Systemmanager LicenseServer\LicenseServerHost to the hostname/ address of the License server, as it appears in the certificate of the license server (i.e. if you use the default certificates generated by Unify, set it to “localhost”. If the License Server and the ConfigServer are not on the same machine, you must replace the default certifications, see the next section "How to Create an Own Certificate").
3) Restart the ConfigServer.

4.7.5.2 How to Create an Own Certificate

If you want to use your certificates, follow these steps:

Step by Step

1) Generate the private/public keys and a certificate file for License Server.
2) Stop the ConfigServer and the LicenseServer from Service Manager.
3) Copy your CA certificate file in PEM format to:

   ```
   <SM_install_dir>/certificates/licenseserver/ca-cert.pem
   ```
4) Copy your server’s certificate file in PEM format to:

   ```
   <SM_install_dir>/certificates/licenseserver/server-cert.pem
   ```
5) Copy your server’s key file in PEM format to:

   ```
   <SM_install_dir>/certificates/licenseserver/server-key.pem
   ```
6) Copy your client’s certificate file in PEM format to:

   ```
   <SM_install_dir>/certificates/licenseserver/client-cert.pem
   ```
7) Copy your client’s key file in PEM format to:

   ```
   <SM_install_dir>/certificates/licenseserver/client-key.pem
   ```
8) Start the Config Server and the License Server from Service Manager.

When everything is set, „ThriftCommunicationServer() Secured Thrift Communication Server is created!” message is written into the License Server’s log file.

Make sure of the following otherwise the HTEMS connection will not be successful :

- for the Server certificates the Key Usage extension must have the Digital Signature and Key Encipherment attributes set,
- for the Client certificates the Key Usage extension must have the Digital Signature set.

4.7.6 Use TLS Encryption in DB Replication

In case of cluster configuration the DB replications between cluster nodes are encrypted with TLS.

The MariaDB uses the yaSSL (Yet Another SSL) library from wolfSSL () on platform windows.

`https://www.wolfssl.com/wolfSSL/Products-yassl.html`

yaSSL is a lightweight implementation of OpenSSL API. Its capabilities are limited. Please check on the www.wolfssl.com site (e.g. up to TLS 1.1 supported).

The TLS encryption needs a server certificate issued by a CA. The necessary certificate files are configured in my.ini file located in `C:\Program Files (x86)\Unify\OpenScapeXpert\certificates\Dat abase` folder.

After the installation of OpenScapeXpert System Manager test certificates issued by Unify are installed and used to secure DB replication. If you want to use own self signed or trusted certificates, simple replace the certificate files.

- ca-cert.pem is the CA certificate
- server-key.pem is the private key of the System Manager
- server-cert.pem is the certificate of the System Manager

4.7.6.1 How to Create an Own Certificate

If you want to use your certificates, follow these steps:

Step by Step

1) Generate the private/public keys and a certificate file for License Server.

2) Stop the ConfigServer and the LicenseServer from Service Manager.

3) Copy your CA certificate file in PEM format to:

`<SM_install_dir>/certificates/licenseserver/ca-cert.pem`

4) Copy your server’s certificate file in PEM format to:

`<SM_install_dir>/certificates/licenseserver/server-cert.pem`

5) Copy your server’s key file in PEM format to:

`<SM_install_dir>/certificates/licenseserver/server-key.pem`

6) Copy your client's certificate file in PEM format to:

   `<SM_install_dir>/certificates/licenseserver/client-cert.pem`

7) Copy your client's key file in PEM format to:

   `<SM_install_dir>/certificates/licenseserver/client-key.pem`

8) Start the Config Server and the License Server from Service Manager.

When everything is set, „ThriftCommunicationServer() Secured Thrift Communication Server is created!" message is written into the License Server's log file.

Make sure of the following otherwise the HTEMS connection will not be successful :

- for the Server certificates the Key Usage extension must have the Digital Signature and Key Encipherment attributes set,
- for the Client certificates the Key Usage extension must have the Digital Signature set.

4.7.6.2 Example to Generate Certificates

The next script is a working example to generate self signed certificates with OpenSSL to MariaDB replication:

- MariaDB-SSL.bat

```
SET OPENSSL_CONF=%~dp0openssl.cnf
SET OpenSSLWithPath=%~dp0openssl.exe

REM Create a root CA, self-signed X.509 certificate valid for twenty years
CALL %OpenSSLWithPath% req -x509 -newkey rsa:2048 -keyout ca-key.pem -out ca-cert.pem -days 7300 -nodes -subj "/CN=ca-cert/C=HU/ST=Budapest/L=Budapest/O=Unify" -text

REM Create server certificate signing request and private key
CALL %OpenSSLWithPath% req -newkey rsa:1024 -keyout server-key.pem -out server-req.pem -days 7300 -nodes -subj "/CN=localhost/C=HU/ST=Budapest/L=Budapest/O=Unify"

REM Convert the key to yassl compatible format
CALL %OpenSSLWithPath% rsa -in server-key.pem -out server-key.pem

REM sign the server certificate with CA certificate
ECHO 01>serial
ECHO. 2>index.txt
CALL %OpenSSLWithPath% ca -days 7300 -batch -cert ca-cert.pem -keyfile ca-key.pem -policy policy_anything -outdir %~dp0 -out server-cert.pem -infiles server-req.pem
```

NOTICE:

To execute the above script change the `dir` parameter to "`dir = .`" in the `openssl.cnf` file.

4.7.7 Use LDAP Authentication

It is possible to log in to OSXMP not only with the default username and password stored in the database, but also with domain account using LDAP protocol. These two methods can be used in parallel.

Starting with V7 R5.0, the upgraded Wildfly version is used with the Elytron security subsystem. Using Elytron, the old security subsystem is no longer available. Therefore, the login-modules have been replaced by security-realms (see the standalone.xml file). The Security-realms work the same as the old login-modules in Wildfly.

The configuration of ldap-realm used for LDAP login must follow the structure of the active directory. This can be different for each customer.

The next chapters provide an example with a safe modification of the active directory and the matching configuration of the ldap-realm in the standalone.xml file. For other implementations, please contact your active directory administrator.

4.7.7.1 Adjustments in Standalone.xml

It is recommended to always make a backup before modifying the standalone.xml file (even though WildFly automatically creates backups by itself as well).

Changes in the standalone.xml file will be applied only after restarting the OpenScape Xpert WildFly Service.

Security-realms can be found in the Elytron subsystem and they have the following structure:

```
<security-realms>
<custom-realm name="elytron_osxmp_customdbrealm" ...>
   ...
</custom-realm>
<ldap-realm name="elytron_osxmp_ldaprealm" ...>
   ...
</ldap-realm>
<distributed-realm name="elytron_osxmp_distributedrealm"
 realms="elytron_osxmp_customdbrealm" />
   ...
</security-realms>
```

4.7.7.2 Authentication with Default User

The administrator creates a default user during the installation in the database. The default security-realm is located in the standalone.xml file:

```
<custom-realm name="elytron_osxmp_customdbrealm"
 module="com.unify.osx.mp.customsecurity" class-
name="com.unify.osx.mp.customsecurity.CustomDbRealm">
<configuration>
<property name="data-source" value="java:jboss/datasources/
mySqlDS"/>
</configuration>
</custom-realm>
```

4.7.7.3 How to Setup the Domain Controller

IMPORTANT:

The **OSXMP_Admin** string on Domain Controller is no more used for OSXMP login (from V7.0.3).

The Administrator must use a Group where the users used to login into OSXMP. In the example below the group is configured to the following level:

- cn = Users, dc = company, dc = com

  If only existing users are to be allowed to login to OSXMP, go to step 3, otherwise proceed from step 1.

Step by Step

1) Create a new Organizational Unit in the active directory root for the new OSXMP administrator users (e.g. ou=OSX-Admin-Users).
2) Create new users in this organizational unit.

   IMPORTANT:

   Already existing users can be put here only by moving. So please consider creating new OSXMP administrators in the group of the other users if you want to allow old users too.

3) Create a new Organizational Unit in the active directory root for the OSXMP administrator roles (e.g. ou=OSX-Admin-Roles).
4) Create a new group in this organizational unit with the following parameters:
   - **Group name**: OSXMP_Admin
   - **Group scope**: Global
   - **Group type**: Security
5) Add to this group all the users that should be allowed to login to OSXMP.
6) Create a new user with password that will be used exclusively by the Wildfly Service itself when it goes to the active directory to authenticate and authorize users (e.g. wildflysrv).
7) Clear the checkbox **User must change password at next logon**.
8) Set the check box **Password never expires**.

4.7.7.4 How to configure Wildfly LDAP login

The LDAP realm for LDAP login is already added to the installed default standalone.xml file with comments:

```
<ldap-realm name="elytron_osxmp_ldaprealm" dir-
context="elytron_osxmp_ldapconnection" direct-
verification="true">
<identity-mapping rdn-identifier="sAMAccountName"
 search-base-dn="E.g.: cn=Users,dc=trading,dc=isec,dc=hu
 Change to your organization!" filter-
name="(&amp;(sAMAccountName={0})(E.g.:
 memberOf=cn=OSXMP_Admin,cn=Users,dc=trading,dc=isec,dc=hu
 Change to your organization!))">
```

The search base and filter name must be configured. If there is an older version of the standalone.xml file with the LDAP login module, then the base context and filter can be copied from it.

Additionally, the dir context must be modified with the LDAP server address and port and the LDAP user and password:

```
<dir-contexts>
<dir-context name="elytron_osxmp_ldapconnection" url="E.g.
 ldap://192.168.0.1:389 Change to your LDAP server
 address!" principal="E.g. test@trading.isec.hu Change to
 your LDAP user name!">
<credential-reference clear-text="Password of LDAP user"/>
```

To activate ldap realm for OSXMP login, the ldap-realm name must be included in the distributed realm parameter:

```
<distributed-realm name="elytron_osxmp_distributedrealm"
 realms="elytron_osxmp_customdbrealm
 elytron_osxmp_ldaprealm" />
```

Restart the Wildfly server to activate this configuration.

4.7.7.5 How to Prepare for using Secure LDAP Connection

Domain Controllers do not allow secure LDAP connection by default. This configuration is outside of the scope of this document. We only provide help to configure the Wildfly side of such a connection.

Step by Step

1) `Standalone.xml` must be edited. The protocol part of the URL must be replaced with ldaps and port number must be changed to 636:

```
<dir-context name="elytron_osxmp_ldapconnection"
url="ldaps:// <ldap_host_name>:636"
principal="<ldap_user>" ssl-
context="osxmp_ldap_ssl_context">
```

2) The LDAP server certificate must be downloaded in .pem format (Base-64).

   Use the following command to import the certificate to the osx.truststore file in the credentialstores directory:

   ```
   "%JAVA_HOME%\bin\keytool" -importcert -trustcacerts
   -keystore "<INSTALL_DIR>\WildFly\credentialstores
   \osx.truststore" -storetype PKCS12 -storepass
   Asd123!. -alias osx-ca -file "<INSTALL_DIR>\WildFly
   \credentialstores\<certificate filename>.pem" -noprompt
   -v
   ```

3) You can set any password for this trust store, but it must be saved in the credential store as described in chapter How to add a password to the credential store on page 62 with `osx_truststore_password` as alias.

4.7.7.6 LDAP Authentication of the Client Profile

It is also possible to authenticate the client profiles using LDAP. Because LDAP is a clear-text protocol, it is highly recommended to use LDAP over SSL, that can be configured in the MP.

When you use LDAP over SSL, the Config Server receives and verifies the server certificate of the LDAP server in order to make sure it is communicating with the correct party. The server-certificate must be signed by a certificate authority (CA), and the Config server checks this. For this purpose, the certificate of the CA must be copied to the following location:

```
<Install dir>\certificates\ldap\cacert.pem
```

typical example:

```
C:\Program Files(x86)\Unify\OpenScapeXpert\certificates
\ldap\cacert.pem
```

NOTICE:

The certificate must be in PEM format. If you have it in a different format, you have to convert it (i.e. openssl can do it), or reexport it. (Microsoft Certificate Export Wizard calls this format Base-64 encoded X.509 (.CER)).

After (re)placing the `cacert.pem` file into the above directory, the Config Server must be restarted.

4.7.8 File system protection of private keys

Step by Step

1) **Create new users for three OpenScape Xpert services:**

   OpenScape Xpert Config Server: <osxCSServiceUser

   OpenScape Xpert License Server: <osxLSServiceUser>

   OpenScape Xpert Database Server: <osxDBServiceUser>

   A. Log in on the Active Directory

   B. Open Active Directory Users and Computers

   C. Right click on Users in your domain folder, click **New** and then click on **User**

   D. Enter the First name, Last name and User logon name and then click on **Next**

   E. Enter and confirm a password.Set the checkboxes according to your needs and click on **Next**

   F. Click on **Finish**

   G. Log out from the Active Directory

2) **Grant access to Program Data/Unify/OpenScape Xpert:**

   A. Open the properties of the OpenScape Xpert folder

   B. Click **Edit...** on the Security tab

   Add < osxCSServiceUser> with Full Control

   Add <osxLSServiceUser> with Full Control

   Add <osxDBServiceUser> with Full Control

3) **Set the Log on User for all three services:**

   Open Services

   Open the properties of the OpenScape Xpert Config Server

   A. Select Log On tab

   B. Select **'This account:**''

   Click **Browse**

   Select **Entire Directory** at Locations...

   Enter the osxCSServiceUser, check Names and then click **OK.**

   Enter and confirm the password and click **OK.**
   Open the properties of the OpenScape Xpert License Server

   A. Select Log on tab.

   B. Select **'This account:**''

   Click **Browse**

   Select Entire Directory at Locations...

   Enter the osxLSServiceUser user, check Names and then click **OK**

   Enter and confirm the password and then click on **OK.**
   Open the properties of the OpenScape Xpert Database Server

   A. Select Log On tab.

   B. Select **'This account:**''

   Click **Browse**

   Select Entire Directory at Locations...

   Enter the osxDBServiceUser user, check Names and then click **OK**

   Enter and confirm the password and then click on **OK.**

4) **Get LDAP cert:**

   Download the certificate of the LDAP server in PEM format and save it as cacert.pem under <INSTALL_DIR>\certificates\ldap directory.

5) Set access permissions of private keys::

In the <INSTALL_DIR>\certificates\directories set the followings:

A. Full Control permission for ’Administrators’

B. Read permission for the new users as described below:

C, In htems folder:

- client-key.pem: ,osxCSServiceUser

- server-key.pem: ,osxLSServiceUser>

In licenseserver folder:

- client-key.pem: <osxCSServiceUser>

- server-key.pem: <osxLSServiceUser>

In Database folder:

- server-key.pem: ,osxDBServiceUser>

Open the properties of the -key.pem file

Click the Security tab

Click **Advanced**

Click **Change Permissions...**

Uncheck ’Include inheritable permissions...’, on Windows Security warning and then click **Add.**

Remove all users except Administrators and then click twice **OK.**

Click **Edit...**

Click **Add...**

Enter the user with read permission and then click on **OK.**

Uncheck everything except Allow-Read and then click twice **OK.**

6) **Set access permissions of certificates:**

   In the <INSTALL_DIR>\certificates\directories set the followings:

   A. Full Control permission for ’Administrators’

   B. Read permission for ’Everyone’

   In all 4 folders:

   Open the properties of the -cert.pem file

   Click the Security tab

   Click **Advanced**

   Click **Change Permissions...**

   Uncheck ’Include inheritable permissions...’, on Windows Security warning and then click **Add.**

   Remove all users except Administrators and then click twice **OK.**

   Click **Edit...**

   Click **Add...**

   Enter Everyone and then click on **OK.**

   Uncheck everything except Allow-Read and then click twice **OK.**

7) **Restart the services:**

   A. OpenScape Xpert Config Server

   B. OpenScape Xpert License Server

   C. OpenScape Xpert Database Server

4.7.9 Securing the DataBase

4.7.9.1 How to activate the Active Directory authentication of DataBase user

To activate the Active Directory authentication of DataBase user (remoteuser) for smdbtool the following configuration steps have to be followed:

Step by Step

1) Open registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \Unify\OpenScapeXpert` and set the `DbAdAuthentication` registry value to 1.

2) Open the command prompt and execute the following command:

NOTICE:

In mysql command before the execute option there are two (2) dashes.

```
mysql -u OsxMysqlAdmin -p<OsxMysqlAdminPassword> --
execute="GRANT ALL ON `osx`.* TO 'remoteuser'@'%'
IDENTIFIED WITH gssapi AS '<adusername>@example.com';"
```

NOTICE:

`OsxMysqlAdminPassword` is the password of the `OsxMysqlAdmin` user that can be the default or can be changed.

NOTICE:

The aduser@example.com has to be changed to the Active Directory user principal which will be used for the administration of OSXMP.

4.7.9.2 How to deactivate the Active Directory authentication of DataBase user

If Active Directory authentication is activated, the Cluster feature is also working.

IMPORTANT:

`GSSAPI` configuration has to be correct and same (set in Registry and in DB) for all hosts.

Active Directory user for remote user has to be the same for all hosts.

To deactivate the Active Directory authentication of DataBase user (remoteuser) for smdbtool the following configuration steps have to be followed:

Step by Step

1) Open registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \Unify\OpenScapeXpert` and set the `DbAdAuthentication` registry value to 0.

2) Open the command prompt and execute the following commands:

NOTICE:

In mysql command before the execute option there are two (2) dashes.

a) `mysql -u OsxMysqlAdmin -p< OsxMysqlAdminPassword > --execute="GRANT ALL ON *.* TO 'remoteuser'@'%' IDENTIFIED BY PASSWORD '*43B7B9B74C7932870AA10825185C3A1B3FABFCC1' REQUIRE SSL;"`

b) `mysql -u OsxMysqlAdmin -p< OsxMysqlAdminPassword > --execute="GRANT SUPER ON *.* TO 'remoteuser'@'%';"`

c) `mysql -u OsxMysqlAdmin -p< OsxMysqlAdminPassword > --execute="GRANT GRANT OPTION ON *.* TO 'remoteuser'@'%';"`

NOTICE:

`OsxMysqlAdminPassword` is the password of the `OsxMysqlAdmin` user that can be the default or can be changed.

NOTICE:

The aduser@example.com has to be changed to the Active Directory user principal and will be used for the administration of OSXMP

4.7.9.3 How to Encrypt the Database Folder

Step by Step

1) Stop the OpenScape Xpert MariaDB.

2) Open the administrator command prompt and execute the following commands:

a) `"cd C:\ProgramData\Unify\OpenScapeXpert\"`

b) `"cipher /e/a/s:MariaDb"`

c) `"cipher /adduser/certhash:"[Thumbprint value]" /b/h/a/s:MariaDB *.*"`

NOTICE:

The thumbprint value noted in chapter "Service Users" must be one space before.

d) `"cipher MariaDB\*"`

NOTICE:

The ’E’ included in filename shows its encryption.

3) Start OpenScape Xpert MariaDB.

4.7.10 HTEMS certificate/key change

4.7.10.1 Certificate Requests

Step by Step

1) Generate certificate requests per involved computer.
2) Send the certificate requests to CA of the organization.
3) Save the private keys for certificate requests..

Example

An example using openssl appears below:

- IP address(es) and/or DNS name(s) of the subject computer.

  NOTICE:

  You have to use the suitable one for CN and list the others in SAN.

- Country Name for C
- State or Province Name for ST
- Organization Name for L
- Organization Unit Name for O

  NOTICE:

  In case OCSP is used, please ask OCSP responder URI.

1) Edit openssl.cnf according to the collected data (e.g. complete SAN as subjectAltName = [], OCSP USRI as authorityInfoAccess = OCSP;URI:[] etc. in [usr_cert] section)

   NOTICE:

   Contents of openssl.cnf depend on the used openssl distribution.

```
openssl req -newkey rsa:2048 -days 7300 -keyout
[file_name_of_private_key.pem] -out [file_name_of.csr] -
nodes -subj "/CN=[]/C=[]/ST=[]/L=[]/0=[]"
```

```
openssl rsa -in [file_name_of_private_key.pem] -out
[file_name_of_private_key.pem]
```

4.7.10.2 How to sign a certificate (Signing request)

Step by Step

1) Generate a self signed CA cert.
2) Openssl req -x509 -newkey rsa:2048 -keyout private/ca-key.pem -out ca-cert.pem -days 7300 -nodes -subj "/CN=ca-cert/C=[]/ST=[]/L=[]/O=[]" -text

NOTICE:

1) "/C=[]/ST=[]/L=[]/O=[]" is part of the CA cert and is the same as given in CSR-s (only once).

3) Openssl ca -days 7300 -batch -policy policy anything infiles [file_name_of.csr]

NOTICE:

The above steps are not necessary when signature is made by local IT infrastructure/personnel.

4.7.11 Preparing the certificate set to deploy

4.7.11.1 Convert certificates

Ensure that all involved certificates are present in .pem (Base64 encoded X.509) format.

The examples below show the conversion of certificates with openssl.

1) For PKCS#12 formatted with .pfx file use

   a) `openssl pkcs12 -in [file_name].pfx -out [combined_file_name].pem -nodes`

NOTICE:

You will be prompted for pfx file password. The [combined_file_name].pem contains the private key and certification path in .pem format so that you can edit with a text editor and copy-paste necessary parts into deployment files.

1) For PKCS#7 formatted with .p7b file use

   a) `openssl pkcs7 -print_certs -in [certificate].p7b -out [certificate].pem`

1) For DER encoded binary X.509 file use

   a) `openssl x509 -inform der -in [certificate].cer -out[certificate].pem`

4.7.11.2 Combining certificates

Step by Step

1) Collect all trusted root (CA) certificates and combine them into one file named ca-cert.pem.

NOTICE:

In normal case you will have only one CA certificate file. Additional certificates may occur when e.g. OCSP responder is a global responder and has its own Verification Authority certificate.

---

2) Before adding the OCSP responder certificate to the CA certificate file, add the OCSP signing trusted extension if it is not already added:

- `openssl.exe x509 -in ocsp-ca-cert.crt -out ocsp-ca-with-trust.pem -trustout -addtrust OCSPSigning`

3) Collect intermediate CA certificates in a given trust chain and combine them with the given machine certificate e.g. When trust chain is CA-ImCA1-ImCA2-Server, CA cert goes into ca-cert.pem. ImCA1 and ImCA2 go into server-cert.pem.

NOTICE:

If the OCSP responder does not include for its response the certificate used to sign the response, certificate to the ocsp-cert.pem file must be added. If certificates to build the trust chain are needed, intermediate certificates must be used.

4.7.11.3 Preparing a deployment

Create a deployment folder for the target machine (e.g. named after CN in server-cert.pem)

Step by Step

1) Get corresponding private key file and copy it to the deployment folder as server-key.pem

2) Get the ca-cert.pem and copy it to the deployment folder.

3) Get ocsp-cert.pem and copy it to the deployment folder.

4) Get server-cert.pem and copy it to the deployment folder.

5) Copy server-cert.pem in deployment folder to client-cert.pem in deployment folder.

6) Copy server-key.pem in deployment folder to client-key.pem in deployment folder.

4.7.12 Deploying certificate set

4.7.12.1 How to Deploy to System Manager node

Step by Step

1) Stop OpenScape Xpert Config Server service.
2) Copy prepared certificate set to [OSX_install_dir]\certificates\htems (overwrite existing files with the same names).
3) Start OpenScape Xpert Config Server service.

4.7.12.2 How to Deploy Windows Turret

Step by Step

1) Stop OpenScape Xpert Client.
2) Copy prepared certificate set to [TT_install_dir]\Trading_E\Tb\certificates \htems (overwrite existing files with the same names).
3) Start OpenScape Xpert Client.

4.7.12.3 How to Deploy to Linux Turret

Step by Step

1) Copy the prepared ca-cert.pem, ocsp-cert, server-cert.pem and client-cert.pem to /etc/cert/htems (overwrite existing files with the same names).
2) Set access rights by invoking following commands:
   - `cd /etc/cert/htems`
   - `chmod 644 *.pem`
3) Copy prepared server-key.pem and client-key.pem to /etc/cert/htems/.key (overwrite existing files with the same names)
4) Set access rights by invoking following commands:
   - `cd /etc/cert/htems/`
   - `chmod 400 *.pem`

4.7.12.4 How to Deploy to MLC

Prerequisites

Files must be saved in MLC

Step by Step

1) Copy the prepared ca-cert.pem, ocsp-cert, server-cert.pem and client-cert.pem to /etc/cert/htems (overwrite existing files with the same names).

2) Set access rights by invoking following commands:
   - `cd /etc/cert/htems`
   - `chmod 644 *.pem`
   - `chown mlcadmin:certificate *.pem`
3) Copy prepared server-key.pem and client-key.pem to /etc/cert/htems/.key (overwrite existing files with the same names)
4) Set access rights by invoking following commands:
   - `cd /etc/cert/htems/.key/`
   - `chmod 420 *.pem`
   - `chown mlc:certificate *.pem`
5) Restart MLC
   - `/etc/init.d/mlc restart)`

4.7.13 Handling of unencrypted Audit log traffic

Audit log on SM is generated by user actions from Config Server and from OSXMP by Wildfly. As default the audit logs are switched on and sent to Windows Event Log unencrypted. Audit logs can be switched off using the registry value

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unify \OpenScapeXpert\EnableAuditLogs.

The default value of this key is 1.

4.7.13.1 How to switch off Audit log for Config Server and OSXMP

Step by Step

1) In registry set HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unify \OpenScapeXpert\EnableAuditLogs to 0
2) Stop and Start OpenScape Xpert Config Server service.
3) Stop and Start OpenScape Xpert Wildfly service.

4.7.13.2 How to switch on Audit log for Config Server and OSXMP

Step by Step

1) In registry set HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Unify \OpenScapeXpert\EnableAuditLogs to 1
2) Stop and Start OpenScape Xpert Config Server service.
3) Stop and Start OpenScape Xpert Wildfly service.

4.8 Installing Hotfixes

4.8.1 How to Install Hotfixes for System Manager Software

A System Manager hotfix can contain one or multiple components, depending on the change. The steps for installing the hotfix can include stopping services, replacing files, changing configuration files, changing registry or other steps.

Step by Step

As the hotfixes can be very different, please follow the steps attached to each release hotfix.

4.8.2 How to Install Hotfixes for MLC or OpenScape Xpert Client Software

Step by Step

1) Copy the hotfix files to the `C:\ProgramData\Unify\OpenScapeXpert\download` folder on all SMs in the cluster. For OpenScape Xpert clients these are the `turret-<version>.zip` and the `turret-<version>.deb`, for MLC the `mlc-<version>.deb`.

NOTICE:

If multiple system managers are used in a cluster, this step has to be repeated on all attached system managers.

---

2) Select the **Hotfixes** menu in the side navigation in OSXMP, and press the **Scan from Disk** button.

3) A warning appears notifying that software installation on the device(s) will be started immediately.

- If you want to start the scanning for Hotfixes and immediate software update on the assigned devices press the **OK** button
- If you want to interrupt the scan process press the **Cancel** button.

4) If the required software version is different from the installed one then open the Edit panel of the OSX Client or MLC, on which the new hotfix should be applied.

5) Select the installed hotfix version in the **Required Software** field on the **General** tab.

When you update the Required Software a warning appears notifying that software installation on the device(s) will be started immediately.

- If you want to save edited properties and start installation on assigned device press the **OK** button
- If you want to interrupt the save process press the **Cancel** button

4.9 Upgrade

4.9.1 Upgrade of an OpenScape Xpert Standalone Server from V6 to V7 or from V7 to V7

Prerequisites

OpenScape Xpert V6 or V7 is installed (there is no cluster).

The OpenScape Xpert V7 installation DVD should be in the DVD ROM drive, or the installation files have to be unzipped in a temporary folder on a hard disk drive.

IMPORTANT:

It is recommended to save a database backup into a folder other than that of the OpenScape Xpert system. If the installer aborts the upgrade due to an error, the old software will be deleted from the server (there is no rollback). The installer should start again, although the upgrade option is not available any more.

Step by Step

1) Run `OpenScapeXpertSetup.exe`
2) Click **Next** on the welcome page and decide for the removal or upgrade of the installed version.
3) Select **Upgrade the current OSX installation and database** and click **Next**. The installer checks if MariaDB are installed.
4) Accept the License Agreement and click **Next.**
5) Select **New standalone server or new cluster** at server type and click **Next.**
6) Verify the list of components to be installed and click **Next** and **Finish.**

   Previous manual changes in configuration file merge into a new default one automatically. In case of a conflict, you have to resolve the conflict with kdiff3 tool that pops up automatically during upgrade.

   The installer upgrades the components, starts the services and creates shortcuts in the Windows Desktop and in the Start Menu. It also updates the Registry and saves the installation log to the <`SM_install_dir`>, as `.Setup Log <date> #<counter>.txt`

NOTICE:

Clicking on **Cancel** at any point, the setup quits and the upgrade aborts. The old version is still available.

4.9.2 Upgrade of an OpenScape Xpert Standalone Server from V7 to V8

Prerequisites

OpenScape Xpert V7 is installed (there is no cluster).

The OpenScape Xpert V8 installation DVD should be in the DVD ROM drive or the installation files have to be unzipped in a temporary folder on a hard disk drive.

IMPORTANT:

It is recommended to save a database backup to a separate folder, not in the OpenScape Xpert system. If the upgrade is aborted due to an error, the previous software will be deleted from the server (there is no rollback). The installer should start again, although the upgrade option is not available any more.

Save the current password of the **https.keystore** and the **osx.truststore**.

IMPORTANT:

When updating from V7 to V8, the users table will modified. Please avoid changing your default user settings during this update. Any changes made will be reverted to the default settings after the update is complete.

Step by Step

1) Run `OpenScapeXpertSetup.exe`.
2) Click **Next** on the welcome page choose to remove or upgrade the installed version.
3) Select **Upgrade the current OSX installation and database** and click **Next**. The installer checks if JAVA Runtime Environment and MariaDB are installed on the system.
4) Accept the License Agreement and click **Next.**
5) Enter the current password of the https.keystore and osx.truststore, then click **Next**. Leave the text fields for setting the default passwords empty.

   IMPORTANT: Setting an incorrect password may prevent OpenScape Xpert SM Portal from starting again.

6) Select **New standalone server or new cluster** for server type and click **Next**.
7) Verify the list of components to be installed, then click **Next** and **Finish**.

Previous manual changes in the configuration file are automatically merged into a new default file. In case of conflicts, the **kdiff3** tool opens automatically during upgrade and allows you to resolve the conflicts. If the system is upgraded from a version prior to V7.5.0, **kdiff3** will not be activated for the `standalone.xml`.

The installer upgrades the components, starts the services and creates shortcuts in Windows Desktop and Start Menu. It also updates the Registry and saves the installation log to the `< SM_install_dir>`, as `.Setup Log <date> #<counter>.txt`.

NOTICE:

If you click **Cancel** at any step, the setup quits and the upgrade is aborted.

4.9.3 Upgrade of an OpenScape Xpert Cluster from V6 to V7 or from V7 to V7

Overview

Upgrading the servers of a cluster is performed server-by-server. As the servers are equal regarding their role (they can be either primaries or backups depending on the locations), you can start the upgrade on any of them.

- The first server has to be upgraded as a standalone server. It will be deatched from the cluster during upgrade.
- The other servers have to be upgraded one-by-one as a backup server. They will be detached from the cluster and attached to one of the previously upgraded servers during upgrade, building a new cluster.

This way you'll have two working clusters throughout the upgrade, the old with decreasing number of servers and the new with increasing number of servers until the last one is attached to the new cluster.

The clients fail over to a backup server according to the SM Priority list of their location while the primary is down. As soon as the upgrade is finished, the clients connect back to the primary. At the end of the whole upgrade process, all the clients are connected again to their primary. The SM Priority List of the locations after upgrade is the same as before.

IMPORTANT:

All the cluster servers must be upgraded to the same software version.

If you don't plan to use a server any more, make sure the server isn't primary in any locations, detach it from the cluster and uninstall the software on it.

Do not modify server priorities during the upgrade. If you'd like to change priorities, do it before or after the upgrade.

It is recommended to save a database backup on the first server to be upgraded into a folder other than that of the OpenScape Xpert system. If the installer aborts the upgrade due to an error, the old software will be deleted from the server (there's no rollback). The installer must be started again, but the upgrade option is not available any more.

4.9.3.1 How to Upgrade the First Server

Prerequisites

OpenScape Xpert V6 or V7 is installed on the servers of a working cluster.

The OpenScape Xpert V7 installation DVD should be in the DVD ROM drive, or the installation files have to be unzipped in a temporary folder on a hard disk drive

Step by Step

1) Run `OpenScapeXpertSetup.exe`.

2) Click **Next** on the welcome page.

   The installer finds the installed version and asks for your decision about remove or upgrade.

3) Select **Upgrade the current OSX installation and database** and click **Next**.

   The installer now checks if MariaDB are installed.

4) Accept the License Agreement and click **Next.**.

5) Select **New standalone server or new cluster** at server type and click **Next**.

6) Verify the list of components to be installed and click **Next** then **Finish** at the end.

Previous manual changes in configuration file merge into new default one automatically. In case of a conflict, you have to resolve the conflict with kdiff3 tool which pops up automatically during the upgrade.The installer first disconnects the cluster, then upgrades the components, starts the services, creates shortcuts to the Windows Desktop and in the Start Menu, updates the Registry and saves the installation log to the `<SM_install_dir>`, as

`Setup Log <date> #<counter>.txt`

The log of smdbtool is saved as

`<SM_install_dir>\databasetools\smdbtool_disconnect-cluster_log.txt`

NOTICE:

Clicking on **Cancel** at any point quits Setup and aborts the upgrade. The old version is still available.

4.9.3.2 How to Upgrade the Other Servers

Prerequisites

OpenScape Xpert V6 or V7 is installed on the servers of a working cluster.

The OpenScape Xpert V7 installation DVD should be in the DVD ROM drive, or the installation files have to be unzipped in a temporary folder on a hard disk drive

Step by Step

1) Run `OpenScapeXpertSetup.exe`.

2) Click **Next** on the welcome page.

   The installer finds the installed version and asks for your decision about remove or upgrade.

3) Select **Upgrade the current OSX installation and database** and click **Next**.

   The installer now checks if MariaDB are installed.

4) Accept the License Agreement and click **Next.**

5) Select **Add this server to an existing Cluster** at server type and click **Next**.

   The installer asks you if you are sure to delete the database and recreate the cluster.

6) Click **OK** to proceed or **Cancel** to go back to select the server type again.
7) Enter the IP addresses of a previously upgraded server and click **Next**.
8) Enter the IP address of the server that will act as license server.
9) Verify the list of components to be installed and click **Next** then **Finish** at the end.

Previous manual changes in configuration file merge into new default one automatically. In case of a conflict, you have to resolve the conflict with kdiff3 tool which pops up automatically during upgrade.

The installer now detaches the server from the cluster, upgrades the components, attaches the server to the new cluster, starts the services, creates shortcuts to the Windows Desktop and in the Start Menu, updates the Registry and saves the installation log to the `<SM_install_dir>`, as

`Setup Log <date> #<counter>.txt`

The log of smdbtool is saved as

`<SM_install_dir>\databasetools\smdbtool_cluster_log.txt`

NOTICE:

Clicking on **Cancel** at any point quits Setup and aborts the upgrade. The old version is still available.

4.9.3.3 Unlock System Managers and Set the Priorities

After all the servers have been upgraded, all System Managers must be unlocked and their priorities in the locations must be set up manually according to your needs.

4.9.4 Zero Downtime Upgrade

Zero Downtime allow the Clients (OSX Client, MLC) in the OpenScape Xpert system to work even with limited functionalities.

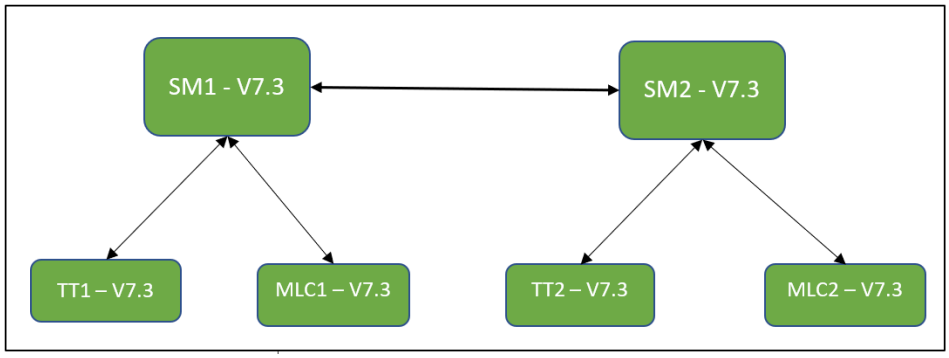
Zero Downtime Upgrade is only possible with Cluster configuration (there should be at list a 2 SM Cluster).

The example below describes a Zero Downtime Upgrade scenario for a 2 SM Cluster with OpenScape Xpert clients (software version: V7.3 to V7.4) for which the automatic upgrade feature is enabled.

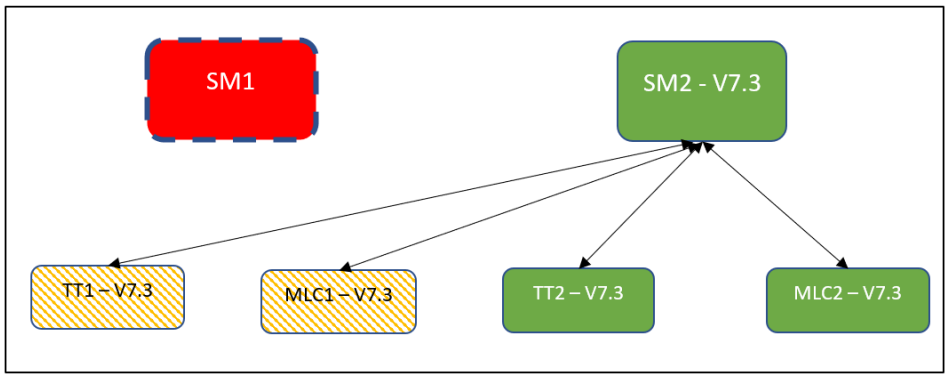
System start state:

- System Manager 1 (SM1)
- OSX Client 1 (TT1) connected to SM1, configured to SM1 location
- Multi Line Controller 1 (MLC1) connected to SM1, configured to SM1 location

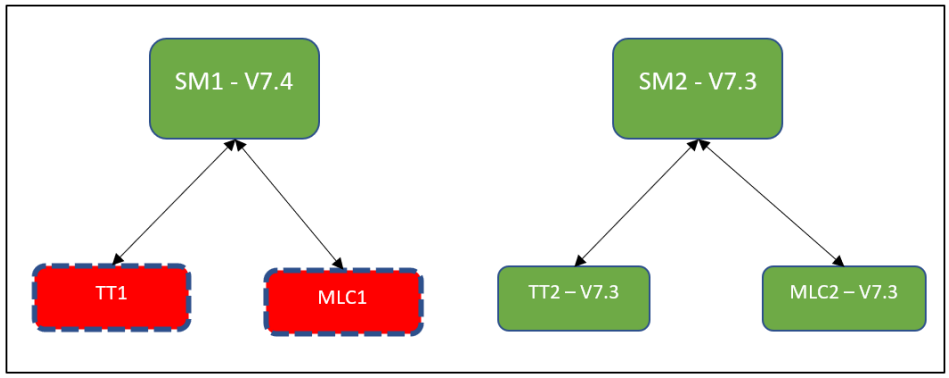
- System Manager 2 (SM2)
- OSX Client 2 (TT2) connected to SM2, configured to SM2 location
- Multi Line Controller 2 (MLC2) connected to SM2, configured to SM2 location
- SM2 is attached to SM1
- SM1 is configured as Central License Server for SM2
- All components (SM, OSX Client, MLC) are on the same Xpert software version – V7.3



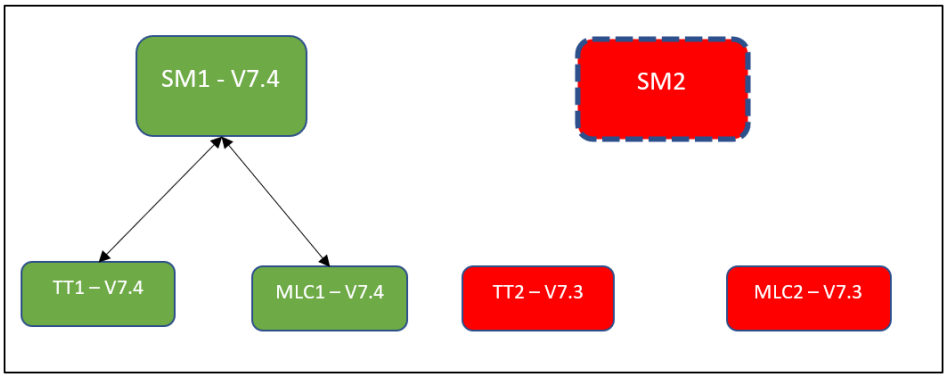
Upgrade step	Result	License status	Client status on SM1	Client status on SM2	Working components
Lock SM1	TT1 displays “No connection to System Manager” After an amount of time TT1 and MLC1 fail over to SM2 according to the location SM priority	OK		TT1, MLC1 yellow TT2, MLC2 green	SM2 TT1, MLC1 TT2, MLC2
Start upgrade on SM1 Installer option: “New standalone server or new cluster”	SM1 detached from SM2 On SM2, SM1 is deleted from SM2 location	No license server (grace period)		TT1, MLC1 yellow TT2, MLC2 green	SM2 TT1, MLC1 TT2, MLC2



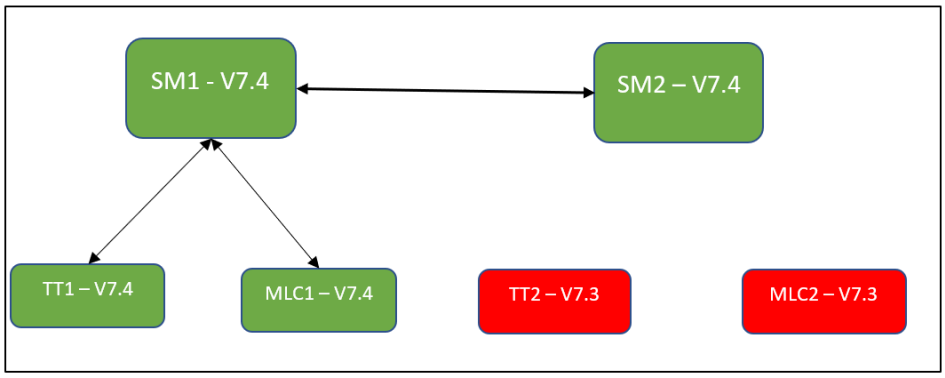
Upgrade step	Result	License status	Client status on SM1	Client status on SM2	Working components
Upgrade SM1 is ready	SM1 is upgraded to V7.4 SM1 is standalone, locked SM2 is standalone	OK SM2 connected to SM1 license server	TT1, MLC1 red TT2, MLC2 red	TT1, MLC1 yellow TT2, MLC2 green	SM1, SM2 TT1, MLC1 TT2, MLC2
Unlock SM1	TT1, MLC1 fail back to SM1 TT1 display: “Downloading new software… Turret will restart.” TT1 and MLC1 start upgrade.	OK	TT1, MLC1 red TT2, MLC2 red	TT1, MLC1 red TT2, MLC2 green	SM1, SM2 TT2, MLC2



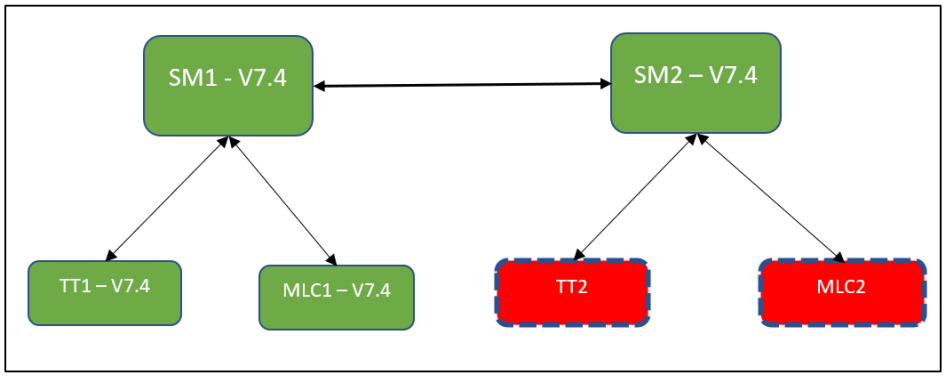
Upgrade step	Result	License status	Client status on SM1	Client status on SM2	Working components
TT1, MLC1 upgraded and restarted	TT1, MLC1 is upgraded to V7.4 and connected to SM1 There are 2 standalone system with central license server: SM1-TT1,MLC1 (V7.4) SM2-TT2,MLC2 (V7.3)	OK	TT1, MLC1 green TT2, MLC2 red	TT1, MLC1 red TT2, MLC2 green	SM1, SM2 TT1, MLC1 TT2, MLC2
Lock SM2	TT2,MLC2 are working without SM2 with limited functions TT2 displays “No connection to System Manager”	OK	TT1, MLC1 green TT2, MLC2 red		SM1 TT1, MLC1 TT2, MLC2



Upgrade step	Result	License status	Client status on SM1	Client status on SM2	Working components
Upgrade SM2 finished Installer option: “Add this server to an existing cluster”	SM2 is upgraded to V7.4 SM2 is attached to SM1, locked	OK	TT1, MLC1 green TT2, MLC2 red	TT1, MLC1 red TT2, MLC2 red	SM1, SM2 TT1, MLC1 TT2, MLC2

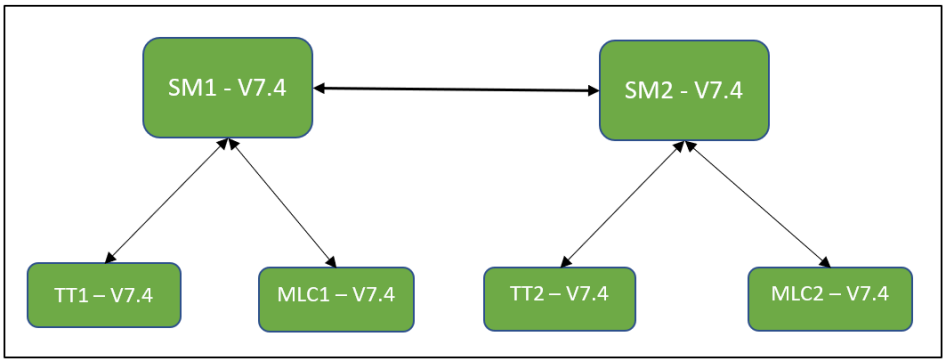


Upgrade step	Result	License status	Client status on SM1	Client status on SM2	Working components
Unlock SM2	TT2, MLC2 start to download and upgrade software. TT2 display: “Downloading new software… Turret will restart.”	OK	TT1, MLC1 green TT2, MLC2 red	TT1, MLC1 green TT2, MLC2 red	SM1, SM2 TT1, MLC1



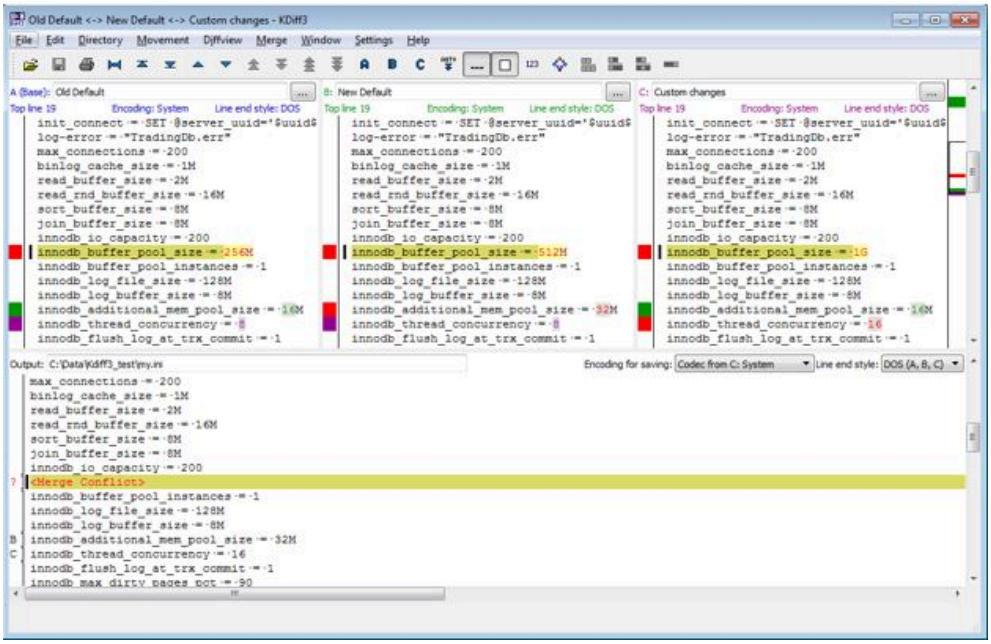
System end state:

- SM2 is attached to SM1
- SM1 is configured as Central License Server for SM2
- All components (SM, OSX Client, MLC) are on the new upgraded Xpert software version – V7.4



4.9.5 How to Execute Manual Merge with KDiff3 During Upgrade

In the System Manager many manual changes in the configuration file **standalone.xml** can be done to increase security. In some cases, unique performance improvements have been suggested to customers in **standalone.conf.bat** and my **ini** files. To keep these changes, the System Manager configuration files are merged during an upgrade with an external tool called Kdiff3. If the tool cannot resolve the conflict by its predefined logic than a merge window will be displayed.



For example, in the above window, innodb_buffer_pool_size was by default 256 M before the upgrade. The new default value is 512M but customer made manual changes in the system before the upgrade to 1G. The merge tool can not decide which one to use, because the same line was changed by multiple sources, so the window is displayed.

The user has the following possibilities:

- The configuration file was changed by intention at the customer. In this case it is suggested to make the merge manually because of the conflict between the new default values and the changes.
- There was no change from customer side. In this case it is safe that the merge is not done. You have to use the new default file, close the window and then select Quit without saving. A window appears in which you have to select "Use default".

The upper sub windows showing the files are the needs to be merged:

- Old Default: This was the default file when the currently installed version was installed.
- New Default: This is the default file when in the version which installer is currently running.
- Custom changes: This is the file that is currently used on the system, containing all the custom changes done after installation (if any).

The large window on the bottom of the screen includes the merge output. This is the result of the merge. In normal case a merge needs to be done with the following steps:

- After the window opens, the first unsolved conflict is selected.
- Decide from the upper three windows which one is the best with the A, B OR C buttons.
- Decide from the upper three windows which one is the best with the A, B OR C buttons.
- Press the  . "Go to Next Unresolved Conflict" button is active. press it and repeat from step2.
- When the  ."Go to the Next Unresolved Conflict: button and the  "Gi ti Orevious Unresolved Conflict" is inactive, then all conflicts are merged.
- Press Save and Close the application.

OPTIONAL:

- You can jump around the differences (Deltas) in the file with the toolbar buttons.
- You can review the automated merge results or make manual changes in the configuration. On the left side of the merge result you see which change was selected by the tool (A,B,C) or change manually (m)

The most important controls in the toolbar are:

 Save

 Go to Current Delta

Go the First Delta

 Go to Last Delta

Go to Previous Delta

Go to Next Delta

 Go to Previous Conflict

 Go to Next Conflict

Go to Previous Unresolved Conflict

Go to the Next unresolved Conflict

Select Line(s) from A

Select Line(s) from B

Select Line(s) from C

4.9.6 Upgrade of the Clients

After the OpenScape Xpert System Manager has been upgraded, the clients connected to it start their self-upgrade automatically with the following exceptions:

Prerequisites

The automatic upgrade for MLCs doesn't work from V5 to V6 and from V6 to V7 because V5 MLCs use Debian 8 (32 bit) OS, V6 MLCs use Debian 8 (64 bita) OS and V7 MLCs use Debian 9 (64 bit) OS. In these cases, all the MLCs in the system have to be reinstalled manually. That means both OS and MLC SW. For more information see OpenScape Xpert Multi Controller.

The automatic upgrade of OpenScape Xpert Clients on Linux OS doesn't work from V5 to V6 if the turret image is different in the two versions.

The automatic upgrade of OpenScape Xpert Clients on Linux OS doesn't work from V6 to V7 because the turret image is different in the two versions

---

NOTICE: Both the turret image and the turret SW of OpenScape Xpert Clients on Linux OS can be upgraded using the OpenScape Xpert Diagnosis Tool if manual upgrade is necessary. For more information see Diagnosis Tool chapter.

The automatic upgrade of OpenScape Xpert Clients on Windows OS doesn't work on versions older that V5 R1.5.0.

The automatic upgrade of OpenScape Xpert Clients on Windows OS from V6 to V7 works only after specific preparation because of different encryption of the communication between the server and the clients.

Step by Step

1) Get the V7 hotfix files of OpenScape Xpert Clients ("turret-7.x.y.z-nnn.zip" and "turret-7.x.y.z-nnn.deb") from the install media of OpenScape Xpert V7 and copy them to the C:\ProgramData\Unify\OpenScapeXpert\download folder.
2) Open the **Hotfixes**.panel from the side navigation menu of OpenScape Xpert Management Portal and click **Scan from Disk.**
3) Edit the OpenScape Xpert Clients you want to upgrade with this method. Select the V7 version at required software on the **General** tab of OSX Client properties and save the properties.

4) Broadcast the changes with the Forced logout option.

NOTICE:

The clients download the new version from the server, upgrade themselves and try to connect to the server. The clients have to wait until the server is upgraded to the same version.

5) Upgrade the System Manager server as described in previous chapters. After the above steps, OpenScape Xpert Clients on Windows OS can connect to the server.

4.9.6.1 How to Configure Version Check

- After the ConfigServer service is restarted, clients reconnect to the server.
- The server detects the version mismatch and sends the download address of the client installation file.

Step by Step

The version check of clients can be switched off by creating the following DWORD entry in the Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Unify\Trading E
\Systemmanager ConfigServer\AppVersionChecking
```

The value 0 means OFF, others mean ON.

If the key does not exist, then it means the version check is switched ON.

4.9.6.2 Download Installation Packages

The clients download the installation package over HTTP and deploy it.

The installation packages published by Wildfly and stored in the folder

`C:\ProgramData\Unify\OpenScapeXpert\download.`

The installation URLs are:

- `https://<server_ip_address>:<port>/download/turret-<version>.zip` for windows turrets,
- `https://<server_ip_address>:<port>/download/turret-<version>.deb` for linux turrets,
- `https://<server_ip_address>:<port>/download/mlc-<version>.deb` for (linux) MLC.

4.9.6.3 How to Change the Port Number for Download

The new port number must be between 1024 and 65535. Otherwise, the default 443 port number will be sent to clients.

Step by Step

1) If the port needs to be changed for any reason, modify the next line in standalone.xml:

   ```
   <socket-binding name=”turret_mlc_files” port
   =”${jboss.http.port:443}”/>
   ```

2) Save the changes in `standalone.xml` and restart the Wildfly server.
3) Create the next DWORD value in the Registry:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Unify\Trading E
   \Systemmanager ConfigServer\UpgradeHttpPort.
   ```

4) Insert the new port number as value and restart the Config server.

4.9.6.4 How to Configure https Session Timeout

You can configure https session timeout in Wildfly for OpenScape Xpert Management Portal.

Step by Step

1) Edit the configuration file "standalone.xml" manually:

   ```
   <SM_install_dir>\WildFly\standalone\configuration
   ```

2) Change default session timeout attribute in line:

   ```
   <servlet-container name="default" default-session-
   timeout="30">
   ```

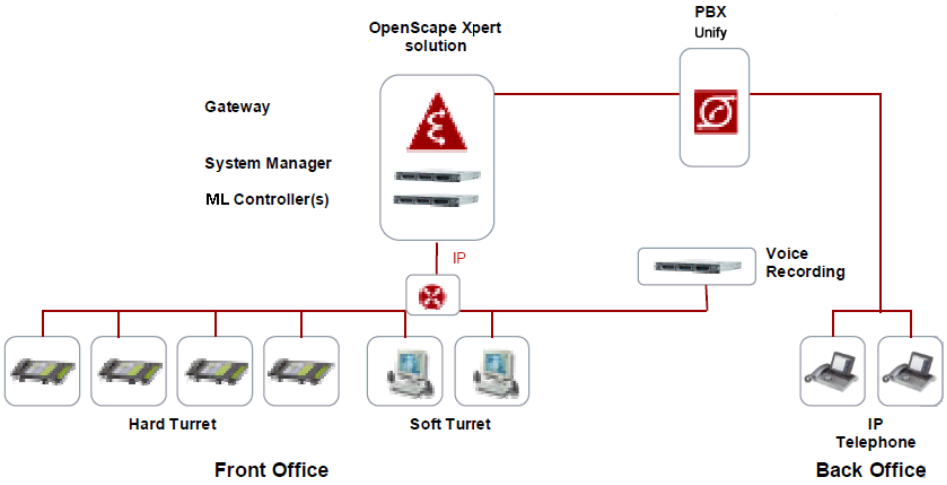
NOTICE:

The default value of session timeout is "30". The value should be an integer measured in minutes.

5 OpenScape Xpert Multi Line Controller — Overview

OpenScape Xpert Architecture

At the heart of the system is the Multi Line Controller (MLC) and System Manager/Database server.



MLC Overlaod Protection

The MLC is a real-time system handling voice calls. The Unify recognized limit for real-time systems is below a CPU utilization of 80%. To keep the application handling voice in real-time and to prevent crashes or bad speech quality, the MLC rejects calls and features causing additional CPU load, once the predefined performance threshold of 80 % has been reached.

To prevent quick mode changes between overload protected and normal mode, a second threshold of 70 % is used to leave overload protection, like a hysteresis.

This feature itself does not need to be configured. It has some new error messages that helps the user to notify the overloaded state of the MLC. To notify the user, a line state has been introduced that clearly indicates MLC overload state on the line key and on SPM channel with an exclamation mark on yellow background.

About MLC Installation

From OpenScape Xpert V4R6.2 on only the following installation methods are recommended:

- Automated Installation via Netinstall
- Manual Installation via DVD

The MLC operating system is Debian (64 bit Version). The Installation via USB device is not recommended anymore and therefore not described in this manual.

5.1 How to Prepare for Debian Installation via Netinstall

To prepare for the automated MLC installation with Debian via Netinstall please proceed as follows.

Step by Step

1) Edit the preseed file:

a) Set the root password and the confirmation:

d-i passwd/root-password password `123456`

d-i passwd/root-password-again password `123456`

b) Add normal user:

d-i passwd/user-fullname string `adminsys`

d-i passwd/username string `adminsys`

d-i passwd/user-password password `skysky`

d-i passwd/user-password-again password `skysky`

NOTICE:

If you don’t redefine them they can be modified later from the operating system.

---

2) Correct the System Manager’s IP address:

```
d-ipreseed/late_command string \
wget http://192.168.10.151/MLC_SW/AutoInst/
S99install.sh -O /target/root/S99install.sh; \
chmod +x /target/root/S99install.sh; \
wget http://192.168.10.151/MLC_SW/AutoInst/
autoinstall.txt -O /target/root/
autoinstall.properties; \
echo '/root/S99install.sh | tee -a /var/log/
mlc-auto-install.log'
> /target/root/.bash_profile; \
sync
```

3) Edit the autoinstall.txt: This file contains attributes given in key value pairs, these attributes are necessary for the initialization script to be able to configure the MLC properly.

a) It is mandatory to correct the System Managers’s IP address and the MLC package name that can be found in `C:\ProgramData\Unify`

`\OpenScapeXpert\download\`. The new MLC packages are named “mlc-<version>.deb".

```
sm_ip=192.168.10.151
```

```
mlc_package=mlc-4.5.5.0-2.deb
```

b) If you want to synchronize the MLC’s system clock with the one from SM, enable ntp_from_sm option.

```
ntp_from_sm=Y
```

c) If you want to redefine the hostname after installation set the host name value to `Y` and set the host name to the desired name.

```
set_host_name=Y
```

```
host_name=MLCHOSTNAME
```

5.2 How to Install Debian via Netinstall

Prerequisites

The steps prior to the installation have been accomplished.

NOTICE:

Please note that the passwords, users and IP addresses in this section are examples!

The Screenshots in this section refer to Debian 6, the actual Debian installer should look similar.

Step by Step

1) Insert DVD1 of Debian package into the optical drive.

NOTICE:

It can be downloaded under: http://cdimage.debian.org

The Installer boot menu will come up.

2) Choose **Advanced options**.

The Advanced options menu appears.

3) Choose **Graphical automated install**.

The screen for the language selection for the installation process appears.

4) Select the language for the installation, e.g. English and click **Continue**. This will be also the default language for the installed system.

The window for the location selection appears.

5) Select your location.

a) Select **other** and click **Continue**.
b) Select the continent, e.g. **Europe** and click **Continue**.
c) Select the country, e.g. **Hungary** and click **Continue**.

6) If your system can't configure the network setting using DHCP, the **Network autoconfiguration failed** message appears. Select **Continue**.

The **Configure the network** window is displayed.

7) You should configure the network manually. Select **Configure network manually** and click **Continue**.

a) Set your IP address, e.g. `192.168.11.104` and click **Continue**.
b) Set the network mask, e.g. `255.255.252.0` and click **Continue**.
c) Set the gateway's IP address, e.g. 192.168.11.254 and click **Continue**.
d) Set the name server's IP address, e.g. `192.168.11.1` and click **Continue**.
e) Set the hostname, e.g. `MLC-Autoinst-01` and click **Continue**.
f) Set the domain name, e.g. `mydomain.com` and click **Continue**.

The **Download debconf preconfiguration file** window is displayed.

8) Set the path to the preconfiguration file (preseed.txt) located on the SM: `http://192.168.10.151/MLC_SW/AutoInst/preseed.txt` and click **Continue**.

The **Partition disks** window is displayed.

9) Select the hard drive of the system and click **Continue**.

After the hard drive installation the system will be installed. This could take some time.

The **Configure the package manager** window is displayed.

10) Select the **Yes** option and click **Continue**.

Normally after this step we have to wait for the installation process to finish. But if your system is attached to the internet or the installer cannot connect to the proper repository, the following warning message appears.

Bad archive mirror

```
An error has been detected while trying to use the
specified Debian archive mirror.

Possible reasons for the error are [...].
```

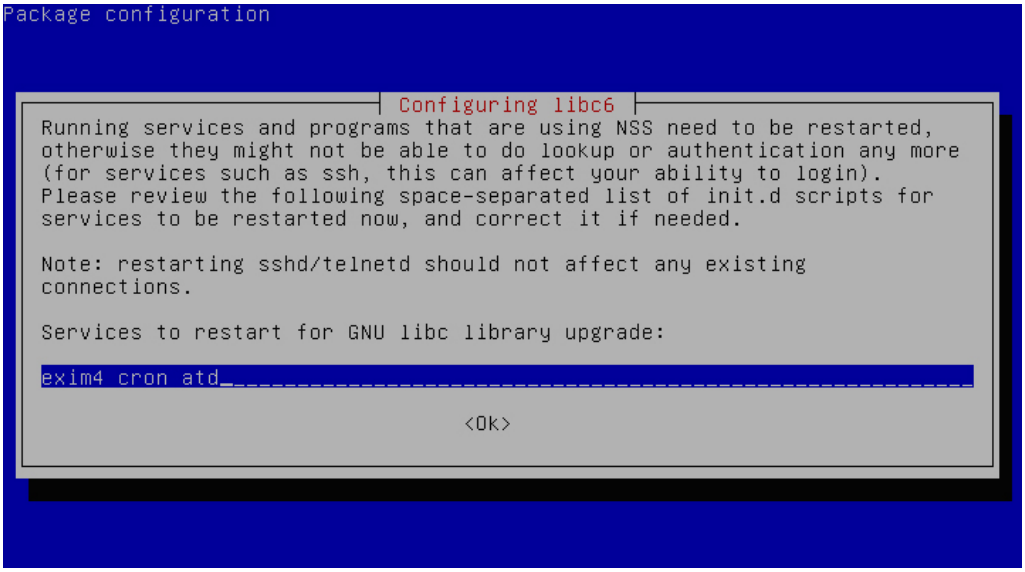
11) Click **Go Back**.

The **Configure the package manager** window is displayed again with the "No network mirror was selected" message.

12) Select the **Yes** option and click **Continue**.

Eject the installation CD after the installation process has finished.

13) The system reboots, and starts up from the hard drive. At first boot you should login as `root` to finish the configuration process. During configuration the system will ask you to restart some of its services.



NOTICE:

The figure above is an example. Depending on the Debian Version and on the delivered packages various windows could appear.

Let the script finish. After it has finished the system will be rebooted.

5.3 Manual MLC Installation with Debian

This section describes the manual MLC installation process for OpenScape Xpert V7 using the DVD1 of Debian (64 bit version) package.

5.3.1 How to Manually Install Debian Using a DVD

This section describes the manual MLC installation process for OpenScape Xpert using the DVD1 of Debian package.

Prerequisites

Download the first DVD from http://www.debian.org an burn it on DVD.

NOTICE:

Please note that the passwords, users and IP addresses in this section are examples!

The screen shots in this section refer to Debian 6, the actual Debian installer should look similar.

Step by Step

1) Insert the DVD into the drive.

The Installer boot menu will come up.

2) Choose **Graphical install** or just **Install** to use the text based install. This section describes the graphical installation.

NOTICE:

Text based installation is more appropriate where space is limited for use of mouse.

The screen for the language selection for the installation process appears.

3) Select the language for the installation, e.g. English and click **Continue**. This will be also the default language for the installed system.

The window for the location selection appears.

4) Select your location.

a) Select **other** and click **Continue**.
b) Select the continent, e.g. **Europe** and click **Continue**.
c) Select the country, e.g. **Hungary** and click **Continue**.

5) If your system can't configure the network setting using DHCP, the **Network autoconfiguration failed** message appears. Select **Continue**.

The **Configure the network** window is displayed.

6) You should configure the network manually. Select **Configure network manually** and click **Continue**.

a) Set your IP address, e.g. `192.168.11.104` and click **Continue**.
b) Set the network mask, e.g. `255.255.252.0` and click **Continue**.
c) Set the gateway's IP address, e.g. 192.168.11.254 and click **Continue**.
d) Set the name server's IP address, e.g. `192.168.11.1` and click **Continue**.
e) Set the hostname, e.g. `MLC01` and click **Continue**.
f) Set the domain name, e.g. `mydomain.com` and click **Continue**.

The **Set up users and passwords** window is displayed.

7) Enter your "root user" password, (e.g.123456) and click **Continue**..

The **Set up users and passwords** window to create an alternative user is displayed.

8) Create a new user to be used instead of the root account, (e.g.adminsys).

a) Enter the full name for the new user and click **Continue**.
b) Enter the user name for the account and click **Continue**.
c) Enter a password for the account and click **Continue**.

The **Partition disks** window to choose the partitioning methode is displayed.

9) Choose **Guided - use entire disk** and click **Continue**.

The **Partition disks** window to select a hard disk is displayed.

10) Select the hard drive of the system and click **Continue**.

The **Partition disks** window to select the partitioning scheme is displayed.

11) Select the first option **All files in one partition** and click **Continue**.

The **Partition disks** overview window to modify the settings is displayed.

12) Select the **Finish partitioning and write changes to disk** option and click **Continue**.

The **Partition disks** overview window to confirm the partitioning is displayed.

13) Select the **Yes** option and click **Continue**.

After the hard drive installation the system will be installed. This could take some time.

The **Configure the package manager** window to scan another medium is displayed.

14) Select the **No** option and click **Continue**.

The **Configure the package manager** window is displayed again ..

15) Select the **Yes** option and click **Continue**.

Normally after this step we have to wait for the installation process to finish. But if your system is attached to the internet or the installer cannot connect to the proper repository, the following warning message appears.

Bad archive mirror

```
An error has been detected while trying to use the
specified Debian archive mirror.

Possible reasons for the error are [...].
```

16) Click **Go Back**.

The **Configure the package manager** window is displayed again with the "No network mirror was selected" message.

17) Select the **Yes** option and click **Continue**.

The **Configuring popularity contest** window is displayed.

18) Select the **No** option and click **Continue**.

The **Software selection** window is displayed.

19) Select the Software you want to install and click **Continue**. SSH Server and the Standard system utilities are needed. With the first DVD the most from the development wanted packages are included.

The **Configuring man-db** window to install the *GRUB boot loader* is displayed.

20) Select the **Yes** option and click **Continue**.

The **Finish the installation** window is displayed.

21) Click **Continue**.

Remove the DVD after the installation process has finished.

5.4 Finalization of MLC Installation

This topic describes the final steps of the MLC installation process.

The MLC has to be prepared for Teaming/Bonding under the Debian operating system.

After the restart of the system copy the mlc package from System Manager, than the following packages from Debian repository:

- nftables
- apparmor-utils
- apparmor-profiles
- psmisc
- sudo
- libpam-pwquality
- debsig-verify
- if necessary tshark and wireshark (mandatory for support)

The packages can be downloaded from:

- https://packages.debian.org/Bullseye/ for Debian11

You can copy these packages per e.g. WINSCP or download it from your System manger with:

`wget:http://….`

If you are connected to the Internet you can download the packages with:

- apt-get install wireshark
- apt-get install tshark

The MLC package is part of the OpenScape Xpert Software and comes with the OSX Software.

5.4.1 How to Configure Ethernet Redundancy for the MLC - Bonding

This section describes the steps to configure bonding on Debian for Ethernet redundancy on the MLC.

Prerequisites

The initial Debian setup procedure has been completed.

You have downloaded the `ifenslave_2.9_all.deb` package from the Debian Website or have connection to the internet!

Step by Step

1) Log in to the new system as “root” using the password set during installation.

2) Edit /etc/network/interfaces file like this.

```
--------------------------------------

auto lo
iface lo inet loopback

auto bond0
allow-hotplug bond0
iface bond0 inet static
address 192.168.1.231/24
gateway 192.168.1.1

dns-nameservers 192.168.1.1
dns-search fritz.box
slaves ens160 ens192
bond_mode active-backup
bond_miimon 100
bond_downdelay 200
bond_updelay 200

----------------------------------------
```

NOTICE:

The addresses above are only examples and must be adapted to the network where the MLC is to be deployed.

3) Install the ifenslave package: `apt-get install ifenslave_2.9_all.deb`

4) Restart network interfaces: /etc/init.d/networking restart

5) Check config:

```
---------------------------------------
cat /sys/class/net/bond0/bonding/mode
cat /sys/class/net/bond0/bonding/updelay
cat /sys/class/net/bond0/bonding/downdelay
cat /sys/class/net/bond0/bonding/miimon
---------------------------------------
```

We want to use active-backup as bonding mode. Bond modes for reference:

```
---------------------------------------
balance-rr or 0
active-backup or 1
balance-xor or 2
broadcast or 3
802.3ad or 4
balance-tlb or 5
balance-alb or 6
---------------------------------------
```

5.5 Enforced Password Policy

This section descibes the changes of the password policy which has been made optional from OpenScape Xpert v5R0 on.

Password Expitration

When a MLC is installed on a system for the first time, the OS is not hardened any more. This makes it possible to log in as root and the password expiration setting is the default value of 99999 days.

If it is not the first time that a MLC is installed on a system (e.g.: upgraded), security related configuration is not affected, so if the system was hardened it remains hardened, and if not, it remains so.

If an MLC is not installed on a system for the first time (e.g.: upgraded), security related configuration is not affected. Therefore, if the system has been hardened on initial installation, it remains hardened and vice versa.

The creation of mlcadmin user, mlcadmins group and sshusers group is not influenced and stays as is.

5.5.1 How to Enable or Disable OS Hardening

To make it possible to easily enable/disable OS hardening, a bash script is introduced.

It is installed to `/var/mlc/mlc.os.hardening.sh`.

Step by Step

It can be used as follows:

- Calling it with the parameter "enable" will enable OS hardening: root logon is disabled, password expiration is set to 90 days.
- Calling it with the parameter "disable" will disable OS hardening: root logon is enabled and password expiration is set to the default 99999 days.
- Calling it without parameter, or with more then one parameter, or with unknown parameter prints the usage of the script.
- Before the script modifies a configuration file, it creates a backup of it called `<filename>_bck`.
- The script logs to `/var/mlc/mlc.audit.log` and prints some info to the standard output.

NOTICE:

Password policies can be configured in:

`/etc/ login.defs` and `/etc/pam.d/common-password`.

root logon can be configured in `/etc/ssh/sshd_config`.

5.5.2 How to install libpam-pwquality

The hardened PAM password configuration uses libpam-pwquality for password policy setting.

Step by Step

For the installation of libpam-pwquality the following options appear:

- If you are connected to the internet, install it with the following command:

  ```
  # apt install libpam-pwquality
  ```
- If you are offline you need to download the package and its dependencies (libpwquality1, libpwquality-common) from the corresponding Debian repository, copy to mlc and install them manually using the following command.

  ```
  # dpkg –i libpwquality-common*.deb libpwquality1*.deb
  libpam-pwquality*.deb
  ```

5.6 How to Install MLC.deb

This section describes the correct installation of the mlc.deb package.

Step by Step

1) Log in to the system as "root" and enter: `dpkg -i mlc-<version-number>.deb, eg. dpkg -i mlc-7.5.0.0-140.deb`

```
root@vLinux-poolvm-02:/tmp# dpkg -i mlc-7.5.0.0-140.deb
Selecting previously unselected package mlc.
(Reading database ... 36222 files and directories currently installed.)
Preparing to unpack mlc-7.5.0.0-140.deb ...
Unpacking mlc (7.5.0.0-140) ...
Setting up mlc (7.5.0.0-140) ...
User (mlc) created
BAD PASSWORD: The password contains the user name in some form
User (mlcadmin) created
BAD PASSWORD: The password contains the user name in some form
User (mlcengr) created
fs.file-max = 64000
kernel.core_pattern = core%t.%p
############################
## Apply security config ##
############################
Firewall

[successful] Save old nftables.conf to /etc/nftables.conf.old
[successful] Copy new nftables.conf to /etc/nftables.conf
[successful] Copy new mlc.nft to /etc/nftables.conf.d/mlc.nft
[successful] Copy new mlc_config.nft to /etc/nftables.conf.d/mlc_config.nft
[successful] Copy new custom.nft to /etc/nftables.conf.d/custom.nft
Restarting nftables...
nftables.service is not active, cannot reload.
Allow nftables on reboot...
Created symlink /etc/systemd/system/sysinit.target.wants/nftables.service → /lib/systemd/system/nftables.service.
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
/etc/ssh/sshd_config changed successfully
Restarting ssh...
Restarting ssh (via systemctl): ssh.service.
ssh successfully restarted
Setting /etc/apparmor.d/usr.bin.mlc to enforce mode.
####################################
## Apply security config finished ##
####################################
```

```
## Apply security config ##
############################
Firewall

[successful] Save old nftables.conf to /etc/nftables.conf.old
[successful] Copy new nftables.conf to /etc/nftables.conf
[successful] Copy new mlc.nft to /etc/nftables.conf.d/mlc.nft
[successful] Copy new mlc_config.nft to /etc/nftables.conf.d/mlc_config.nft
The file /etc/nftables.conf.d/custom.nft already exists.
Restarting nftables...
Allow nftables on reboot...
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
/etc/ssh/sshd_config changed successfully
Restarting ssh...
Restarting ssh (via systemctl): ssh.service.
ssh successfully restarted
Setting /etc/apparmor.d/usr.bin.mlc to enforce mode.
####################################
## Apply security config finished ##
####################################
/home/mlc/.bashrc already configured
/home/mlcadmin/.bashrc already configured
ndsa config read:

mlc script: start
Starting MLC
Error: No NDSAConfig or ServerName is given in /var/mlc/MlcSettings.ini file. Script will stop.
 You have to configure the System Manager IP address. Example command:
 echo 'ServerName=ServerIP' >> /var/mlc/MlcSettings.ini
 where ServerIP is your SM IP address.
After please start the mlc. (/etc/init.d/mlc start)

Processing triggers for man-db (2.9.4-2) ...
root@vLinux-poolvm-01:/tmp#
```

An error is displayed.

2) To configure the System Manager, use the following command: `echo 'ServerName=ServerIP' >> /var/mlc/MlcSettings.ini` , where "ServerIP" is the IP address of the System Manager.

   Example: `echo 'ServerName=192.168.13.30' >> /var/mlc/MlcSettings.ini`

```
root@vLinux-poolvm-01:/tmp#  echo 'ServerName=192.168.13.30' >> /var/mlc/MlcSettings.ini
```

3) To start the MLC process with the User `root` you need to enter the command: `/etc/init.d/mlc start`

   Then the mlcadmin password must be entered again because of security reasons.

4) An error message may appear after

   - the service has been started manually:

```
root@MLC1:~# /etc/init.d/mlc stop
Stopping MLC..... OK
root@MLC1:~# /etc/init.d/mlc start
Starting MLC
ERROR: Not resolved IP address and host name in /var/mlc/SMpriorityList
```

   or

   - after starting the MLC:

```
Starting MTA:Starting MLC
ERROR: Not resolved IP address and host name in /var/mlc/SMprior
 exim4.
Starting pdnsd.
Starting OpenBSD Secure Shell server: sshd.

Debian GNU/Linux 6.0 MLC1 tty1

MLC1 login: _
```

   In this case, check again if the IP address you have entered is correct or if there is an error in one of these files:

   `/etc/resolv.conf`

   `/etc/network/interfaces`

5) Please check if you have the correct DNS setting in these files:

File	Settings
/etc/resolv.conf	search “Domain Name”
/etc/network/interfaces	dns-search “ Domain Name “

   a) If there are missing settings, add them.
   b) Restart the mlc service using: `# service mlc restart`
   c) Check the content of the `var/mlc/MlcSettings.ini` file.

      This file should contain only one line.

      The figure below displayes an example of `var/mlc/MlcSettings.ini` file.

```
ServerName=192.168.13.30
```

Now your MLC will appear at the Systemmanager and can be assigned.

During the installation of the `mlc-<version-number>.deb` package, three new users are created:

- User **mlcadmin** - start / stop the MLC process
- User **mlcengr** - for technicians, just for log access
- User **mlc** - runs the MLC process

```
Setting up mlc (7.5.0.0-140) ...
User (mlc) created
BAD PASSWORD: The password contains the user name in some form
User (mlcadmin) created
BAD PASSWORD: The password contains the user name in some form
User (mlcengr) created
```

The mlc user will be used automatically, no manual login or startup is necessary. It was necessary because of role separation.

The users have predefined passwords from the installation:

- The password for the **mlcadmin** user is: **Mlcadmin*1**
- The password for the **mlcengr** user is: **Mlcengr*1**

These passwords need to be changed every 90 days.

Hardened pass is necessary as well. The requirements are:

- Must contain at least 8 characters.
- Must contain both lowercase and uppercase characters.
- Must contain at least one special character.

5.7 How to Connect from the System Manager to the Multi Line Controller

Step by Step

The SSH (Secure Shell) connection from System Manager SM to the Multi Line Controller MLC can be enabled using one of the following software tools:

- OpenSSH for Windows
- PuTTY
- WinSCP

5.8 Quality of Service (QoS) for OpenScape Xpert

This section describes the feature "Quality of Service".

Packet prioritization has been implemented in OpenScape Xpert from V4R5 on to improve the voice quality. It is possible to change the QoS parameters depending on the customer’s network architecture.

Requirements

The customer’s network switches must support QoS. In order for Layer2 QoS (VLAN Tagging, IEEE802.1q) to work on the MLC, the Linux server has to be configured to use VLANs.

Layer2 Quality of Service (QoS)

Layer2 Quality of Service (QoS) is set using a three-bit field in the "Tag Control Information" (TCI) field of an 802.3 Ethernet frame header. Within this this field a range of eight values (0-7) is possible. These values determine the "Class of Value" (CoS) for any given frame.

Table 1: 802.3 Tagged Ethernet Frame illustrated with "Tag Control Information" (TCI) header field exploded into detailed view:

Preamble	Destinatio Address	Source Address	TCI Header				Length, Etc
			16 bits: Tagged Frame Type	3 bits: 802.1p Priority Field	1 bits: Canonical	12 bits: 802.1q (VLAN ID)	

Table 2: 802.1p Priority Field values and associated meaning:

PCP value	Priority	Acronym	Traffic types
1	0 (lowest)	BK	Background
0	1 (default)	BE	Best effort
2	2	EE	Excellent effort
3	3	CA	Critical applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork control
7	7 (highest)	NC	Network control

Layer3 Quality of Service - Differentiated Services Code Point (DSCP)

Differentiated Services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (QoS) guarantees on modern IP networks. DiffServ can, for example, be used to provide low-latency to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers. DiffServ uses the 6-bit Differentiated Services Code Point (DSCP) field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.

Expedited Forwarding (EF) PHB

The IETF defines Expedited Forwarding behavior in RFC 3246. The EF PHB has the characteristics of low delay, low loss and low jitter. These characteristics are suitable for voice, video and other real time services. EF traffic is often given strict priority queuing above all other traffic classes. Because an overload of EF traffic will cause queuing delays and affect the jitter and delay tolerances within the class, EF traffic is often strictly controlled through admission control, policing and other mechanisms. Typical networks will limit EF traffic to no more than

30%—and often much less—of the capacity of a link. The recommended DSCP for expedited forwarding is 101110B, or 2EH.

Class selector (CS) PHB

Prior to DiffServ, IP networks could use the Precedence field in the Type of Service (TOS) byte of the IP header to mark priority traffic. The TOS byte and IP precedence was not widely used. The IETF agreed to reuse the TOS byte as the DS field for DiffServ networks. In order to maintain backward compatibility with network devices that still use the Precedence field, DiffServ defines the Class Selector PHB. The Class Selector codepoints are of the form 'xxx000'. The first three bits are the IP precedence bits. Each IP precedence value can be mapped into a DiffServ class. If a packet is received from a non-DiffServ aware router that used IP precedence markings, the DiffServ router can still understand the encoding as a Class Selector codepoint.

Assured Forwarding (AF) PHB group

The IETF defines the Assured Forwarding behavior in RFC 2597 and RFC 3260. Assured forwarding allows the operator to provide assurance of delivery as long as the traffic does not exceed some subscribed rate. Traffic that exceeds the subscription rate faces a higher probability of being dropped if congestion occurs. The AF behavior group defines four separate AF classes. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from AF11 through AF43 (see table).

Table 3: Assured Forwarding (AF) Behavior Group:

	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Med Drop	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
High Drop	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

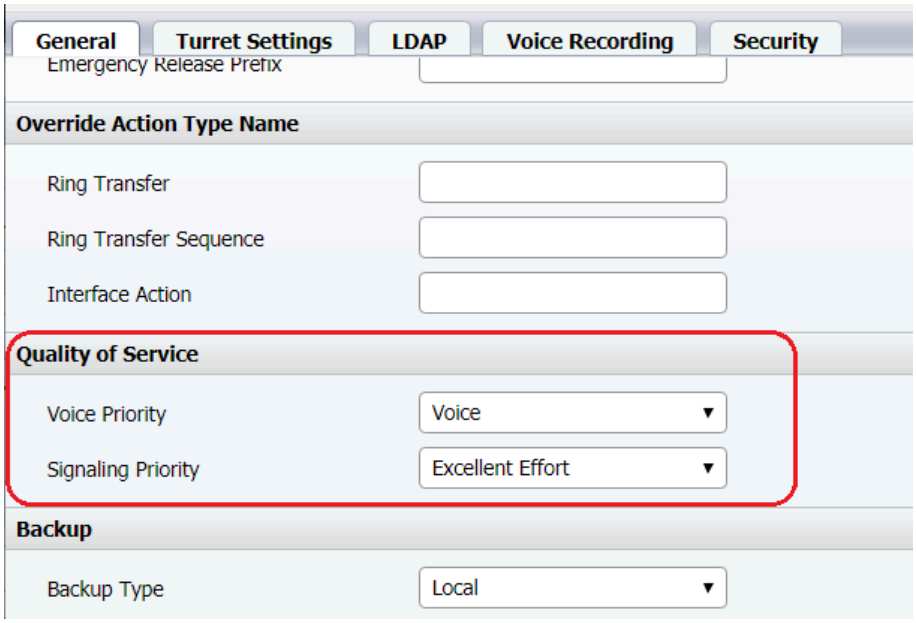
5.8.1 How to Configure QoS Parameters

Step by Step

1) Click **System Properties** on the OpenScape Xpert Management Portal.

   The **System Properties** dialog appears.

2) Locate the **Quality of Service** section in the **General** tab and select one of the possible values.



Possible values:

- Best Effort:

  Flow traffic has the same network priority as regular traffic without being associated with QoS. This traffic type is the same as not specifying priority, and as a result, the DSCP rk and 802.1p tag are not added to sent traffic.
- Background:

  Flow traffic has a network priority lower than Best Effort. This traffic type could be used for traffic of an application doing data backup. Sent traffic contains a DSCP mark with a value of 0x08 and an 802.1p tag with a value of 2.
- Excellent Effort:

  Flow traffic has a network priority higher than Best Effort, yet lower than Video. This traffic type should be used for data traffic that is more important than normal end-user scenarios, such as email. Sent traffic contains a DSCP mark with value of ox28 and 802.1p tag with a value of 5.
- Video:

  Flow traffic has a network priority higher than Excellent Effort and lower than Voice. This traffic type should be used for A/V streaming scenarios such as MPEG2 streaming. Sent traffic contains a DSCP mark with a value of 0x28 and 802.1p tag with a value of 5.
- Voice:

  Flow traffic has a network priority higher than Video, yet lower than Control. This traffic type should be used for real time voice streams such

as VoIP. Sent traffic contains a DSCP mark with a value of 0x38 and an 802.1p tag with a value of 7.

- Control:

  Flow traffic has the highest network priority. This traffic type should only be used for the most critical data. For example, it may be used for data carrying user inputs. Sent traffic contains a DSCP mark with a value of 0x38 and an 802.1p tag with a value of 7Qua.

5.8.2 How to Configure VLAN for Layer 2 QoS on OSX clients and MLC (Debian Linux)

Proceed as follows to install VLAN tools, create VLANs and to set priority mappings on the MLC with Debian Linux operating system.

Prerequisites

The VLAN ID of the customers network environment for the OpenScape Xpert system is known.

Step by Step

1) Load the 8021q kernel module if needed (normally all kernel modules are shipped with a Linux distribution): `modprobe 8021q`

2) Install VLAN tools package to have vconfig available (only in case of MLC, the client image already contains this package):

- `apt-get install vlan` or
- download from `https://packages.debian.org/bullseye/all/vlan/download` and install with: `dpkg -i vlan_2.0.5_all.deb`

3) To create a VLAN, edit the /etc/network/interfaces file. MLC example file (4 is the VLAN ID):

#The loopback network interface

auto lo

iface lo inet loopback

#The primary network inerface

auto eth0

iface eth0 inet manual

auto eth0.4

allow-hotplug eht0.4

iface eth0.4 inet static

address ...

...

vlan-raw-device eth0

OSX client example file:

auto lo

iface lo inet loopback

auto bond0

allow-hotplug bond0

iface bond0 inet manual

slaves eth1 eth0

bond_mode active-backup

bond-miimon 100

bond_downdelay 200

bond)updelay 200

auto bond0.4

allow-hotplug bond0.4

iface bond0.4 inet static

address ...

...

vlan-raw-device bond0

4) Verify the configuration with:

a) `cat /proc/net/vlan/config`

The system responds:

```
VLAN Dev name    | VLAN ID
Name-Type: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
eth0.4       | 4  | eth0
```

b) `cat /proc/net/vlan/eth0.4`

The system responds:

```
eth0.4  VID: 4   REORDER_HDR: 1  dev->priv_flags: 81
                 total frames received        0
                 total bytes received         0
                 Broadcast/Multicast Rcvd     0

                 total frames transmitted     0
                 total bytes transmitted      0
                 total headroom inc           0
                 total encap on xmit          0
Device: eth0
INGRESS priority mappings: 0:0  1:0  2:0  3:0  4:0  5:0  6:0 7:0
EGRESSS priority Mappings:
```

5) Reboot the computer

5.9 Multi Line Appearance with SIP Phones

This section describes the implementation concept and the user interface issues of the feature Multi Line Appearance (MLA) with SIP Phones for OpenScape Xpert from V5R0.2.0 on.

Overview

Shared line events from non OpenScape Xpert clients (normal SIP phones, e.g. OpenStages) using the same lines as the Xpert system are indicated on the Turret GUI. These events are signaled towards the OSX Clients by the MLC the same way as OSX line events. The MLA functionality is hidden from the OpenScape Xpert Clients and is handled completely in the MLC.

From OpenScape Xpert V5 R0.2.0 on, the functionality of the OpenScape Xpert V4R6.4 was re-implemented. The MLC appears as a keyset, with one Primary Keyset (prime line) and maximum 30 secondary lines (secondary lines can be phantom lines, or prime lines of different devices).

Direct line registration to the same PBX from a keyset MLC is not supported. One MLC can have just one Primary Keyset line (prime line)

User Interface OpenScape Xpert Client

The MLC processes MLA status indication messages which it receives from the OSV system. This MLA status information is forwarded to the Client.

This status information already appeared on the Line Keys of the Xpert Client within the OpenScape Xpert environment. With the MLA implementation the line

usage information of other UAs outside the OSX (further referred to as Phones) is indicated in the same way.

Description

- **Line Seized By Another**

  Because of the pre-call seizure being implemented, clicking on a line button (which formerly meant only selecting) now induces real seizure of the line. This means that there is a new line state when another OSX Client selects a Keyset line but has not finished dialling yet. This is indicated by a new colour (a lighter green than the ‘seized and connected/playing tone’). Other OSX Clients are not able to seize on that line.

  This functionality also affects features like Quick Conference, Line Conference, etc. Setting up a line for Call Forward will also mean seizing for the setup duration despite the fact that there will be no call initiation.

  Selecting (thus seizing) an unseized line remains unchanged on the selecting client from the user’s point of view.
- **Line Status Indication**

  The MLA line statuses to be indicated on the OSX Client’s GUI are as follows:

  – idle,
  – active,
  – on hold,
  – ringing.

  There is no visual difference between a line being seized or held by another OSX Client or a Phone. The "idle" and "ringing" state of a Keyset line is indicated on SIP Phones too.
- **Privacy**

  The OSX Privacy is not available (disabled FK and context menu item, SM option ‘Privacy from Beginning’ always unchecked) for Keyset lines. This feature is not working on Keyset lines.
- **Line Conference**

  When several Phones are bridged on a Keyset line that is also participating in an OSX Line Conference, the bridged phones will not increase the number of the LC members since it is the number of conferencing lines, not the number of participating UAs.

Activation/Deactivation

To activate MLA functionality for some lines used by the OSX system these lines need to be configured as Keyset Primary lines in the OSV and the System Manager.

Deactivation: If a line is configured not to be an MLA line in both the OSV and the System Manager, the OSX MLA feature is deactivated for that line.

5.10 Volume Normalization and SPM Voice Indication Feature Tweaks

This section describes the Volume normalization and SPM voice indication feature tweaks.

Overview

Some predefined values can be changed on the MLC by creating and editing the file:

`/var/mlc/voicenorm.cfg`

Example file showing default values

```
5000
100
100
1
4
0.0
1.0
500
```

Make sure the file type is Unix, i.e. line ends are LF, not CR LF like in DOS. Just to be sure, you can convert by:

`dos2unix /var/mlc/voicenorm.cfg`.

Description

This configuration file (voicenorm.cfg) can be used for voice normalization calibration. The application checks the existence of this file by default. If found, it reads the first eight rows, updates it's normalization parameters accordingly, then renames this file to `voicenorm.cfg.old`.

The first eight rows of the file must contain four numbers as follows:

1) The interval between two file readings (32 bit number) in milliseconds
2) VAD threshold, i.e. the highest volume considered a speechless silence, in the range 0-32768 (16 bit number)
3) Number of voice segments (10ms) used for average volume calculations (16 bit number)
4) Number of voice segments (10ms) passed between average volume recalculations and volume adjustments (16 bit number)
5) The scaling between the extremities of the GUI's volume slider is nonlinear, the following simple formula is used to calculate the necessary volume adjustment:
   - $M = D^E / C$, where D is the desired volume (i.e. the current slider position) in the range 0 to 1,
   - C is the current volume of the stream in the range 0 to 1,
   - M is the multiplier, also in the range 0 to 1, to be used for adjustment with the audio samples as multiplicands,
   - E is the value to be configured here (8 bit signed number)
6) The minimum volume level of the volume slider, in the range 0 to 1 (floating point number)

7) The maximum volume level of the volume slider, in the range 0 to 1 (floating point number)

8) The SPM voice indication threshold value (16 bit number). This number shouldn't be higher than 1000.

NOTICE:

The parameter VAD threshold is temporarily present, it will become obsolete as soon as VAD feature implementation will be finished.

The minimum and maximum volume levels are checked when processed, values out of range are set to the closer edge of the range, a max lower than the min is set to the min.

As long as the first row remains unchanged, the MLC parses the file in every 5 seconds, so modification made in the file should be applied in the MLC in that time frame.

5.11 Configuration of Security Settings on MLC

OpenScape expert V7 R5 introduces a new way to manage the firewall on the system in order to enhance security and protect the server from possible attacks. The new firewall is implemented through the nftables service, which has replaced the old firewall script. The installation of the firewall and the configuration is done automatically with the installation of the MLC package. If you want to remove the changes made by the security script on install, you can enter the following command: `/var/mlc/security remove` (After removing the security changes you cant re-enable them unless you reinstall the MLC package. Reinstallation of the MLC will always enable the security enhancements, therefore you need to remove them each time you install a new MLC package).

The nftables service

For basic management of the firewall. we use the nftables service. The nftables service is an one-shot type of service, that can start, stop and restart the firewall. Starting the service means reading and adding the rules from the `/etc/nftables.conf` file to the kernel. The service is automatically started on reboot. It can be controlled with the system command, with the regular options.

Usage: `service nftables <option>`

Options: `start, stop, restart, status`

NOTICE: Since this is an one-shot service, checking the status will not actually tell you if the rules are applied or not. For checking the currently applied list of rules, use the command: `nft list ruleset`. The other commands look as expected.

The default configuration

In the default configuration, the traffic is blocked on both IPV4 and IPV6, except for the connections initiated by the mlc services and some other important exceptions, listed below. Most rules are active for both IPV4 and IPV6, where it

is exclusive to one marked IP version. These rules are available in the `/etc/nftables.conf.d/mlc.nft` file.

Incoming traffic

- TCP

  Destination port: 22 (ssh), 9004, 5060 (sip), 5061 (sip-tls), 5161 (sip-mtls)
- UDP

  Destination port: 9004, 5060 (sip), 5061 (sip-tls), 5100, 2048-65535
- ICMP

  Type: echo-request (ping)

  Only on IPV6: destination-unreachable, packet-too-big, time-exceeded, parameter-problem, echo-reply, nd-router-advert, nd-neighbor-solicit, nd-neighbor-advert, nd-redirect

Outgoing traffic

- TCP

  Destination port: 9004, 5060 (sip), 5061 (sip-tls), 5161 (sip-mtls), 514 (syslog)

  Source port: 22 (ssh), 9004, 5060 (sip), 5061 (sip-tls), 5161 (sip-mtls)

  Source port in the range of 1024-65535 and destination port with 80 (http) or 443 (https)
- UDP

  Destination port: 5060 (sip), 5100

  Source port: 5060 (sip), 5100, 123 (ntp), 53 (domain), 2048-65535
- ICMP

  Type: echo-request (ping)

  Only on IPV6: Accept all

There are some rules that can vary based on the configuration in System Manager. These are stored in the `/etc/nftables.conf.d/mlc_config.nft` file, and the `/var/mlc/mlc.firewall.sh` script will open the firewall for CSTA, SMARTPTT, SIPREC and SIP Outbound Proxy whenever a new configuration is received.

The configuration files

- `/etc/nftables.conf`

  Root configuration file, which includes all nft files from `/etc/nftables.conf.d` folder.
- `/etc/nftables.conf.d/mlc.nft`

  The nft ruleset file for mlc.
- `/etc/nftables.conf.d/mlc_config.nft`

  The nft ruleset file based on the configuration from System Manager.
- `/etc/nftables.conf.d/custom.nft`

  The nft rule set file for custom rules, if the user wish to add other exceptions. The corresponding chains can be appended based on nftables syntax.

NOTICE: If these configuration files already exist during the installation of the MLC, they will be renamed with the ending "_old" and new ones will be created with the configuration explained above. The only exception is the `/etc/nftables.conf.d/custom.nft`, which will not be altered if the file already exists.

Blocking Source Routed Packages and TCP “SYN Flood” attacks

These settings are stored in the kernel configuration file: `/etc/sysctl.conf`. The following modifications are done in this configuration file:

- Blocking Source routed packages: `net.ipv4.conf.all.accept_source_route = 0`
- Increasing the number of not completely built up TCP connections, so that the system can handle more of these: `net.ipv4.tcp_max_syn_backlog = 2048` (default for debian is 512)
- How many times does the system try to build up a TCP connection: `net.ipv4.tcp_synack_retries = 2` (default for debian is 5)

Disabling “MD5” and “96-bit MAC” algorithms in the SSH service

The security script performs the following modifications in the /etc/ssh/sshd_config file:

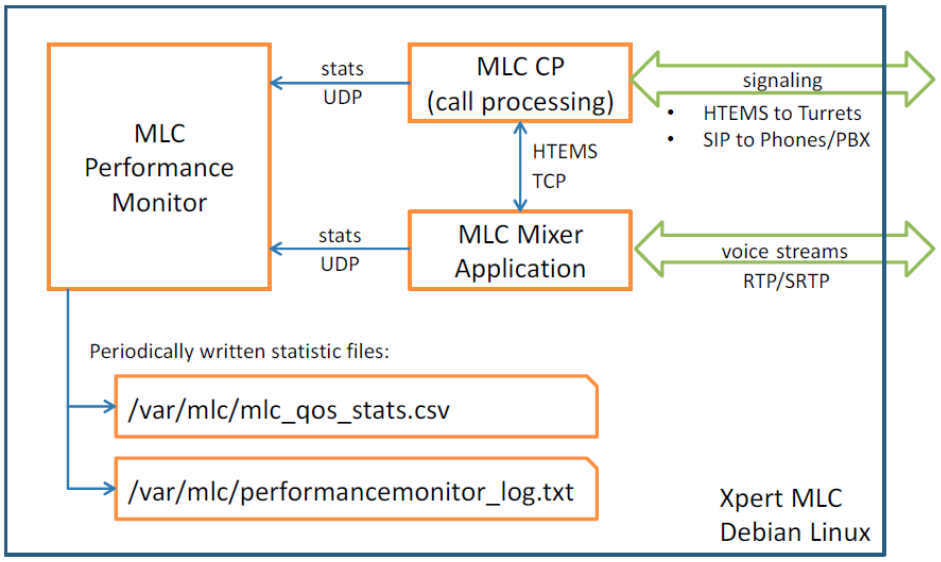
- Deletes the following line: MACs `hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-sha1-96,hmac-md5-96`
- And inserts the following: `MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160`

After deleting the unwanted algorithms from the SSH daemon configuration file the script restarts the SSH service by performing: `/etc/init.d/ssh restart`.

5.12 QoS Statistics

This section describes the Quality of Service (QoS) Statistics available on OpenScape Xpert MLCs for service operations to monitor network quality through the voice streams of the OpenScape Xpert system.

Component overview



How does QoS statistics work?

The MLC Mixer Application periodically sends the QoS statistics (RTP session statistics) for every voice call of the last 60 seconds to the MLC Performance Monitor.

The QoS statistics sent refers to the last 60 seconds only. Internal counters of the MLC Mixer Application are reset right after the data had been sent to the MLC Performance Monitor. This is to prevent alarms on long duration calls for network issues that happened long ago.

The MLC Performance Monitor writes the QoS statistics to the /var/mlc/mlc_qos_stats.csv file in Comma-Separated Values (CSV) file format that can be easily viewed or processed by third party tools. The column header information is printed every 100th line.

What QoS statistics information is available?

The following QoS information is reported by the MLC Mixer Application through the MLC Performance Monitor. Please see table below with column headers and their respective meaning.

Header	Meaning
TimeStamp	Local time on the MLC when the statistics was generated#
OwnIpAddress	Local IP address of the RTP voice stream, IP address of the MLC#
OwnPort	Local UDP port of the RTP voice stream on the MLC#
RemoteIpAddress	Remote IP address of the RTP voice stream, partner IP (SIP or Turret)#
RemotePort	Remote UDP port of the RTP voice stream#
PacketSent	Number of sent packets#
OctetSent	Bytes sent in the RTP voice stream#
PacketReceived	Number of received packets#
OctetReceived	Bytes received in the RTP voice stream#

Header	Meaning
PacketLost	Number of packets lost#
JitterMinMs	Minimum Interarrival Jitter of the last 60 seconds in milliseconds#
JitterMaxMs	Maximum Interarrival Jitter of the last 60 seconds in milliseconds#
JitterAvgMs	Average Interarrival Jitter in milliseconds#
LatencyMinMs	Minimum Latency (delay) in milliseconds#
LatencyMaxMs	Maximum Latency (delay) in milliseconds#
LatencyAvgMs	Average Latency in milliseconds#
DurationMs	Total call duration in milliseconds since beginning. Does not reset.

The QoS statistics CSV file is rotated; a new file is created after its size reaches 10MB and the original file is renamed to: `mlc_qos_stats.csv.1.txt`

10 files are kept, older files are deleted. This behavior is controlled by the:

`/var/mlc/performance_logger_settings.lcp` file in the following section:

```
# rolling file appender
log4cplus.appender.QOS=log4cplus::RollingFileAppender
log4cplus.appender.QOS.File=mlc_qos_stats.csv
log4cplus.appender.QOS.MaxFileSize=10MB
log4cplus.appender.QOS.MaxBackupIndex=10
log4cplus.appender.QOS.layout=log4cplus::PatternLayout
log4cplus.appender.QOS.layout.ConversionPattern=%m%n
log4cplus.appender.QOS.ImmediateFlush=true
```

For an average system with near to maximum load there are ca. 300 lines, ~15kBytes per minute written to the CSV file. With the above default configuration the MLC Performance Monitor will keep 5 days of historical QoS statistics data.

Service operation should customize these settings if needed and/or make sure data is backed up.

Retrictions

There are no QoS statistics reported for calls shorter than 30 seconds. The same applies if the remaining part of the call since the last report is shorter than 30 seconds as statistics can’t be properly calculated for such short durations.

Though the MLC uses a constant 20ms Frame Size, packet sizes are different for SRTP (170 bytes) and RTP (160 bytes) voice streams. This means that for the same duration different number of bytes in the statistics is possible.

Normally calls are bidirectional, consisting of two unidirectional RTP streams. But most of the times the two voice streams don’t start at the very same time, therefore a difference in duration, transferred bytes etc. of the two directions is normal.

5.13 Two Lines On The Same Button - Feature configuration

5.13.1 OSV Configuration

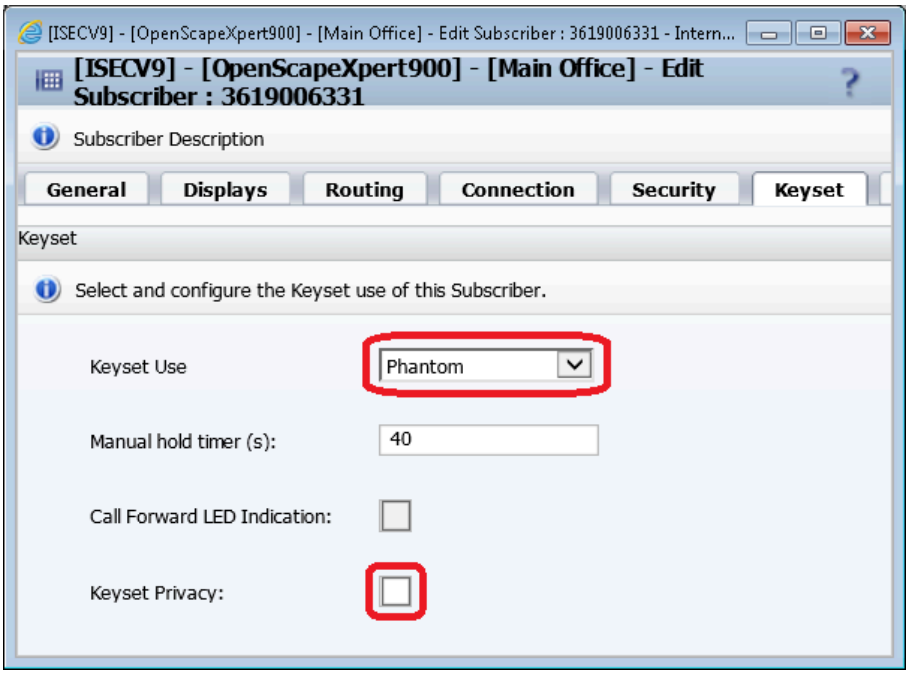
For Main and Backup MLC, a Primary Line should be configured as follows:

- Open the Configuration/OpenScape Voice/Business Group in the CMP.
- Select the regarding Business Group (e.g. OpenScape Xpert 900).
- Expand the **Members** menu and click on the **Subscribers** menupoint.

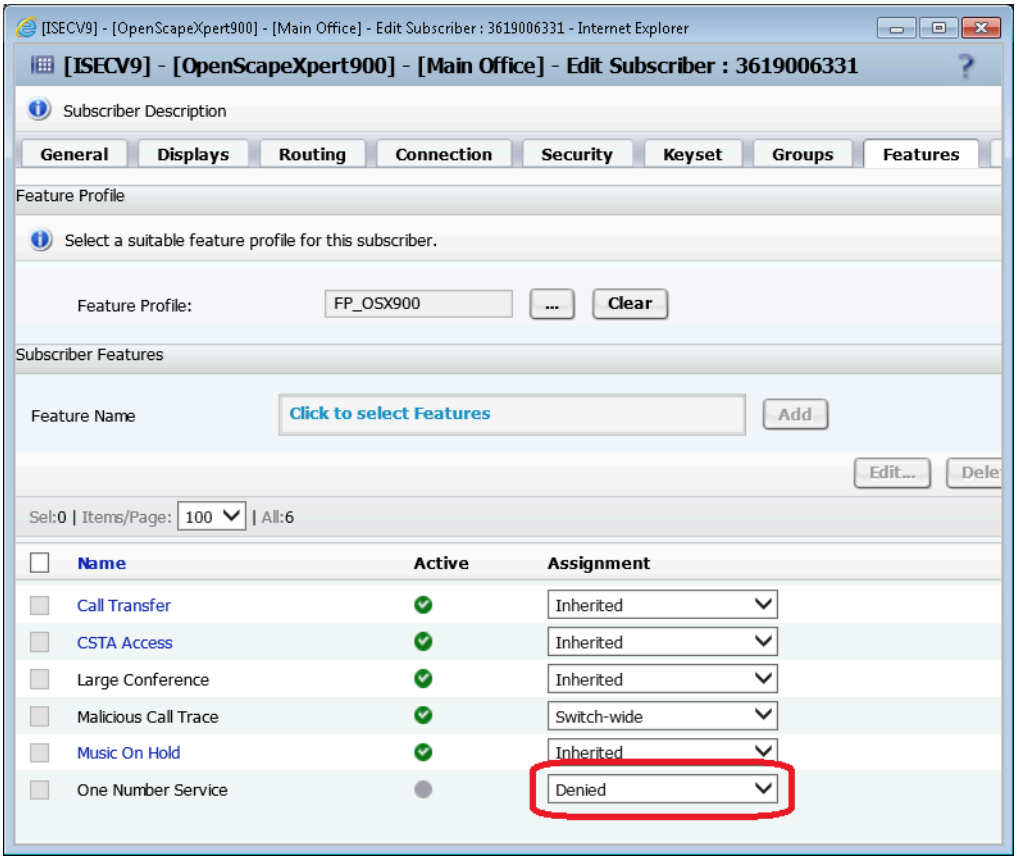
5.13.1.1 MLA Phantom line configuration

The following configuration must be done for MLA Phantom line

- Select and open the regarding line
- Set the field **Keyset Use** to **Phantom** at the **Keyset** tab
- Deactivate the check box **Keyset Privacy**



For the Phantom Keyset functionality, the feature "One Number Service" should not be added or it should be set to **denied** (see below).

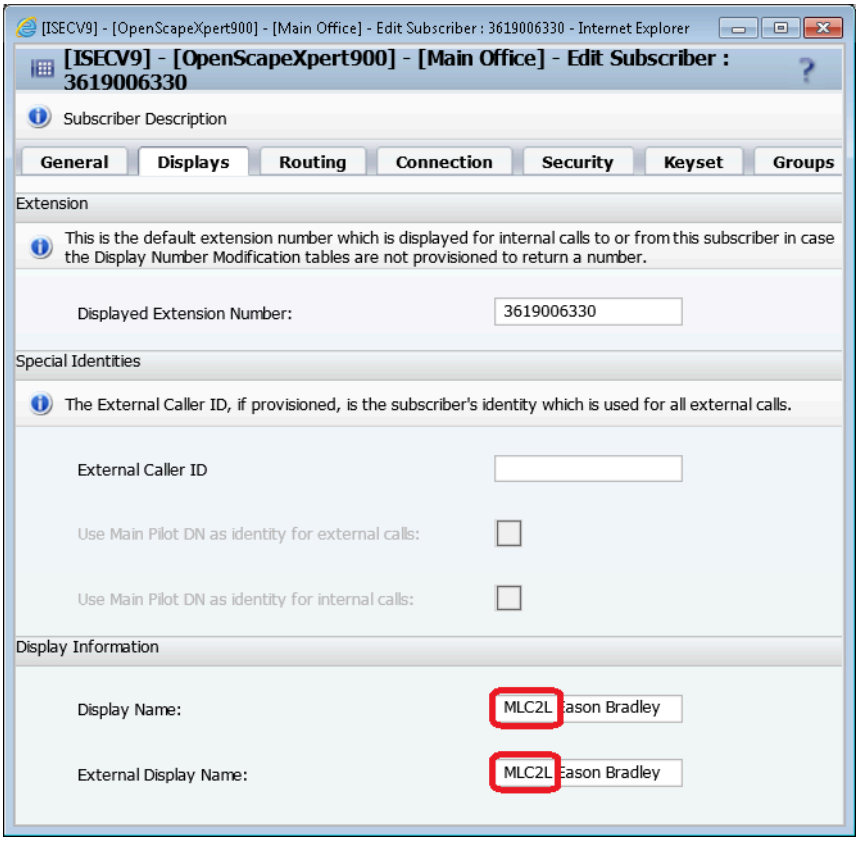


5.13.1.2 MLA Primary line configuration

For the MLA Primary line configuration, the following steps must be done:

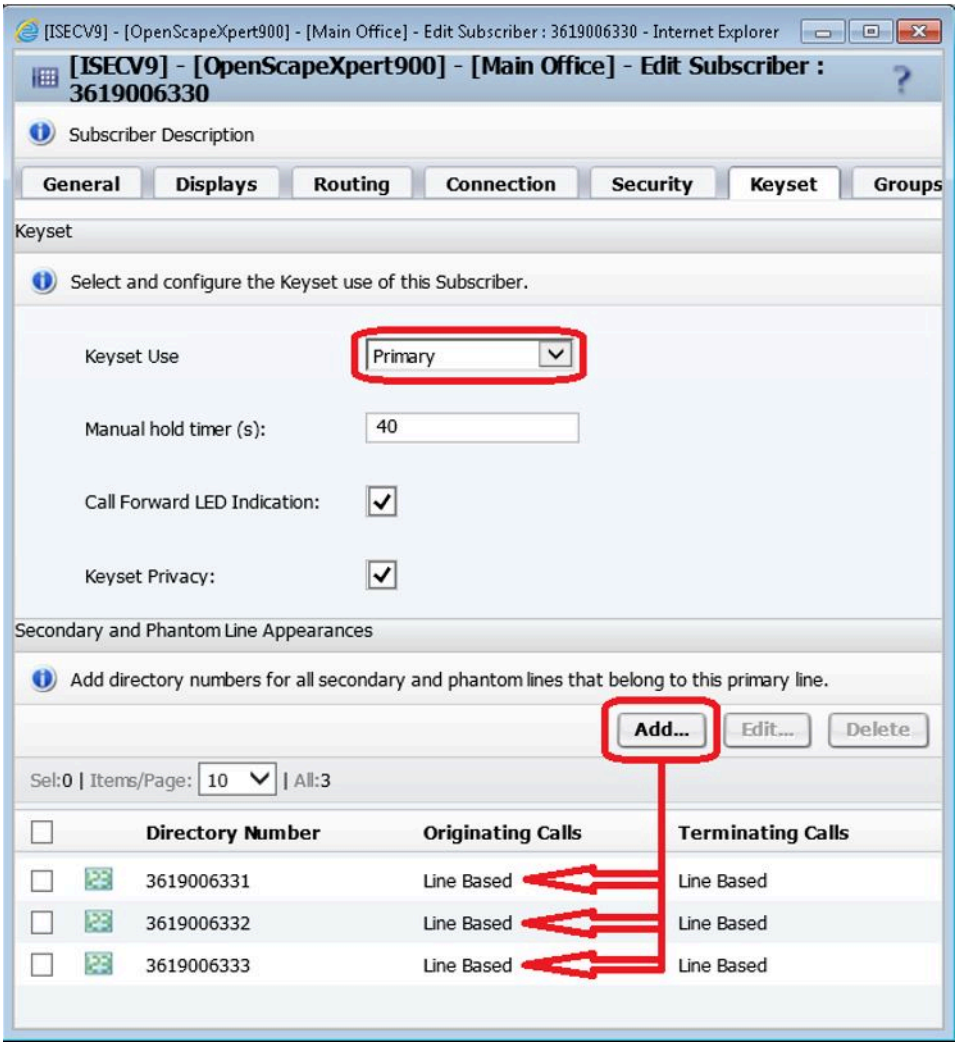
- Look for the line and set it as Primary Line (e.g. +3619006330)
- The following changes should be set in the appeared window:

1) On the **Displays** tab the fields **Display Name** and **External Display Name** should start with the prefix 'MLC2L' (see below)



- On the **Keyset** tab set the **Keyset Use** field to **Primary**

- **Add** phantom lines to this primary line



- Repeat the steps for creating the Primary Line with the same Phantom Lines for the backup MLC

5.13.2 OpenScape Xpert configuration in the CMP

A configuration example of two MLA groups is described below:

1) Primary Line: 6330, Phantom Lines: 6332, 6332, 6331
2) Primary Line: 6334, Phantom Lines: 6333, 6332, 6331

How to Add all the previously configured Primary and Phantom lines to Xpert

1) In the navigation panel click the **MLCs** entry on the **Topology** section.
2) Click the **Lines** entry in the **Topology** section.
3) Click on **Create** and select **Normal Line**

configuration.

Name	URI	Line Group	Registrar	Mlc Assignment	Backup Appearance
6331	3619006331	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.2 - Keyset	backup - 1.100.10.2 - Keyset
6332	3619006332	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.3 - Keyset	backup - 1.100.10.3 - Keyset
6333	3619006333	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.4 - Keyset	backup - 1.100.10.5 - Keyset
6330	3619006330	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.1 - Keyset Primary	Unassigned
6334	3619006334	[Base Line Group]	192.168.15.141:5060	backup - 1.100.10.1 - Keyset Primary	Unassigned

How to Assign Main and Backup MLC for the 2 Keyset Primary lines

1) Click on **Topology** section .
2) Select **Lines** entry.
3) Click on **Unassigned**.
4) Select the required MLC, e.g. Select **Main MLC** for 6330 and **Backup MLC**for 6334.

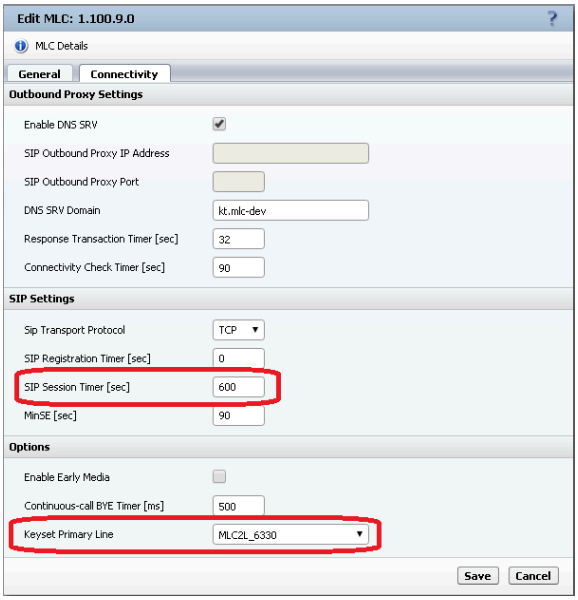
	Name	URI	Line Group	Registrar	Mlc Assignment	Backup Appearance
	6331	3619006331	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.2 - Keyset	backup - 1.100.10.2 - Keyset
	6332	3619006332	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.3 - Keyset	backup - 1.100.10.3 - Keyset
	6333	3619006333	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.4 - Keyset	backup - 1.100.10.5 - Keyset
	6330	3619006330	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.1 - Keyset Primary	Unassigned
	6334	3619006334	[Base Line Group]	192.168.15.141:5060	backup - 1.100.10.1 - Keyset Primary	Unassigned

How to Select MLA Primary lines as Keyset Primary line for Main and for Backup MLC

1) Click on **Topology** > **MLCs**.
2) Click on Node Address of the required MLC.
3) Configure or change the following field in the **Connectivity** tab:

   a) **Keyset Primary Line:** Select the previous added Primary Line from drop-down list.

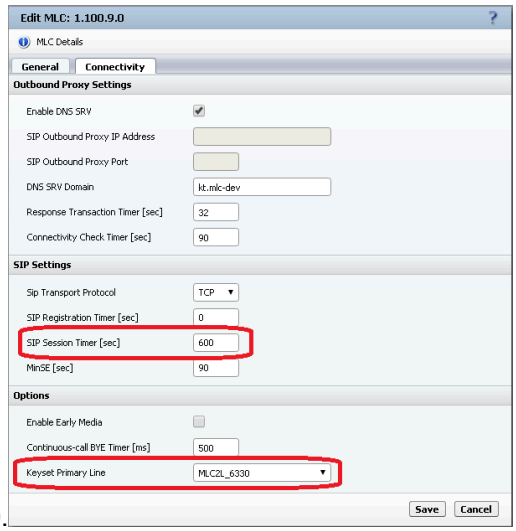
   e.g.For Main MLC, select 6330. For Backup MLC, select 6334



How to Set SIP Session Timer for MLCs to 600

1) Click on **Topology** > **MLCs**.
2) Click on Node Address of the required MLC.
3) Click on the **Connectivity** tab.

4) In the **SIP Settings** area, change **SIP Session Timer [sec]**to 600.



How to Assign Main MLC as "MLC Assignment" and Backup MLC as "Backup Appearance" to each MLA Phantom Line

Assign both Main and Backup MLC to lines, e.g. 6331,6332,6333

Name	URI	Line Group	Registrar	Mlc Assignment	Backup Appearance
6331	3619006331	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.2 - Keyset	backup - 1.100.10.2 - Keyset
6332	3619006332	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.3 - Keyset	backup - 1.100.10.3 - Keyset
6333	3619006333	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.4 - Keyset	backup - 1.100.10.5 - Keyset
6330	3619006330	[Base Line Group]	192.168.15.141:5060	main - 1.100.9.1 - Keyset Primary	Unassigned
6334	3619006334	[Base Line Group]	192.168.15.141:5060	backup - 1.100.10.1 - Keyset Primary	Unassigned

5.13.3 Configuration restrictions

- Feature works with OSV-V9
- Primary line of Main MLC and Primary Line of Backup MLC should contain the same Phantom Lines.
- The MLA Primary lines assigned to Backup and Primary MLC (as Keyset Primary) have a name convention in OSV. This name has to start with "MLC2L"
- The MLA Primary lines assigned to Backup and Primary MLC (as Keyset Primary) can’t be used for creation/answer of a call and they can’t be on Turret Profile or on any OpenStage Phone.
- There can be only Keyset pairs, so one MLA Phantom line can’t be assigned to more than 2 MLA Primary lines in OSV.
- The MLA Phantom line configured for the feature: "Two Lines on the Same Button" in OpenScape Xpert / OpenStage phones can’t be assigned to another MLC as Direct line or to OpenStage phone.
- Direct lines can’t be assigned to MLCs with Keyset Primary line.
- SIP Session Times has to be set to 600 seconds on Backup and Primary MLC, so the OSV can realize faster the loss of MLC.

5.13.4 Functional restrictions

- No privacy on MLA lines.
- After re-establishing the connection with primary MLC, the-line/MLC can restore the "MLA Bridge" in about 5 minutes.
- Consultation/Transfer/Toggle/Conference/Call forwarding/Quick Conference features are not allowed.
- Callback Busy, Emergency Intrusion, Override Busy, Emergency Release are not supported.
- In case of common hold, the other party doesn’t get to hold. If the other party holds the call, the line on the Turret won’t get hold.
- If other party holds 2 lines capable line, the line does not get Music on hold.
- In case of automatic answer, as long as the line doesn’t get to speech unit or SPM, it will not be protected by "Two-Lines" feature.
- After failover, if we disconnect the call from the side of the Turret, the line will remain green for about 30 seconds. If the other sife side disconnects the line, it will get to IDLE state immediately.
- After failover: if the line was active on more speech units, it will be active on one speech unit only.
- After failover: if the primary MLC comes back, the backup MLC losts the connection and the other party disconnects the call, then the line will remain green for about 5 minutes.
- The Line recording is working in case of HTE only for the line of primary MLC. The line of backup MLC won’t be recorded. In case of SIPREC both lines (primary and backup MLC) will be recorded.
- SPM: After re-establishing the connection with primary MLC, the Turret shows "SMP channel tried to bridge but was denied by OSV". This behavior applies until the "MLA Bridge" has not been restored.
- SPM, after failback: SMP voice indicator shows speech activity as long as the "MLA Bridge" is not established.
- After failover: Announcement on lines and DKAs will be disconnected.
- Signal function key does not work.

5.14 Setting up the IPv6 for MLC

The IP Addressing Modes described in chapters 3.1.2.6- 3.1.2.12 are valid for OpenScape Xpret components including MLC.

Please follow the steps in sections 3.1.2.6- 3.1.2.12 and the additional steps for MLC in the following chapters.

5.14.1 How to disable IPv6 for MLC

If MLC is used with IPv4 address and IPv6 is enabled in the system, internal communication problems might occur. Therefore it is highly recommended to

disable IPv6 in all MLC servers where it is not used. To disable IPv6 settings follow the steps below:

Step by Step

1) Login to MLC as root user.
2) Edit the `/etc/sysctl.conf` file:
   a) Paste the following lines:

      net.ipv6.conf.all.disable_ipv6 = 1

      net.ipv6.conf.default.disable_ipv6 = 1

      net.ipv6.conf.lo.disable_ipv6 = 1
   b) Save the changes and enter the following command:

      `#sysctl -p`
3) Reboot the computer.

5.14.2 How to set IPv6 for MLC

Step by Step

1) Open the `/etc/network/interfaces` file in a text editor.
2) Find and change or add line "iface eth0 inet6 ..." line (eth0 can be different) with the following values:
   a) for Stateless Address AutoConfiguration (SLAAC): "iface eth0 inet6 auto"
   b) for Stateful Address Autoconfiguration (DHCPv6) "iface eth0 inet6 dhcp"
   c) for static address: "iface eth0 inet6 static address {IPv6 address} netmask 64"
3) Execute command `/etc/init.d/networking restart`.

5.14.3 How to disable IPv4 for MLC

Step by Step

1) Open the `/etc/network/interfaces` file in an editor (e.g nano).
2) Find the "iface eth0 inet ..." line (From Debian 9 the interface name concept changed, for example: enp0s3).
3) Comment with # sign or delete the line.
4) Repeat the steps above for each interface (eth1, eth2, ...).
5) Execute command `/etc/init.d/networking restart`.

5.14.4 Useful Commands in IPv6 Context

Show IP Adresses

```
>ip addr show
```

Show DNS Name Resolution for a Host

```
>host {host name}
```

Show Reverse DNS Lookup for an Address

```
>host {host address}
```

Show RFC 3484 Rules

```
>cat /etc/gai.conf
```

Show Network Connections and Listeners

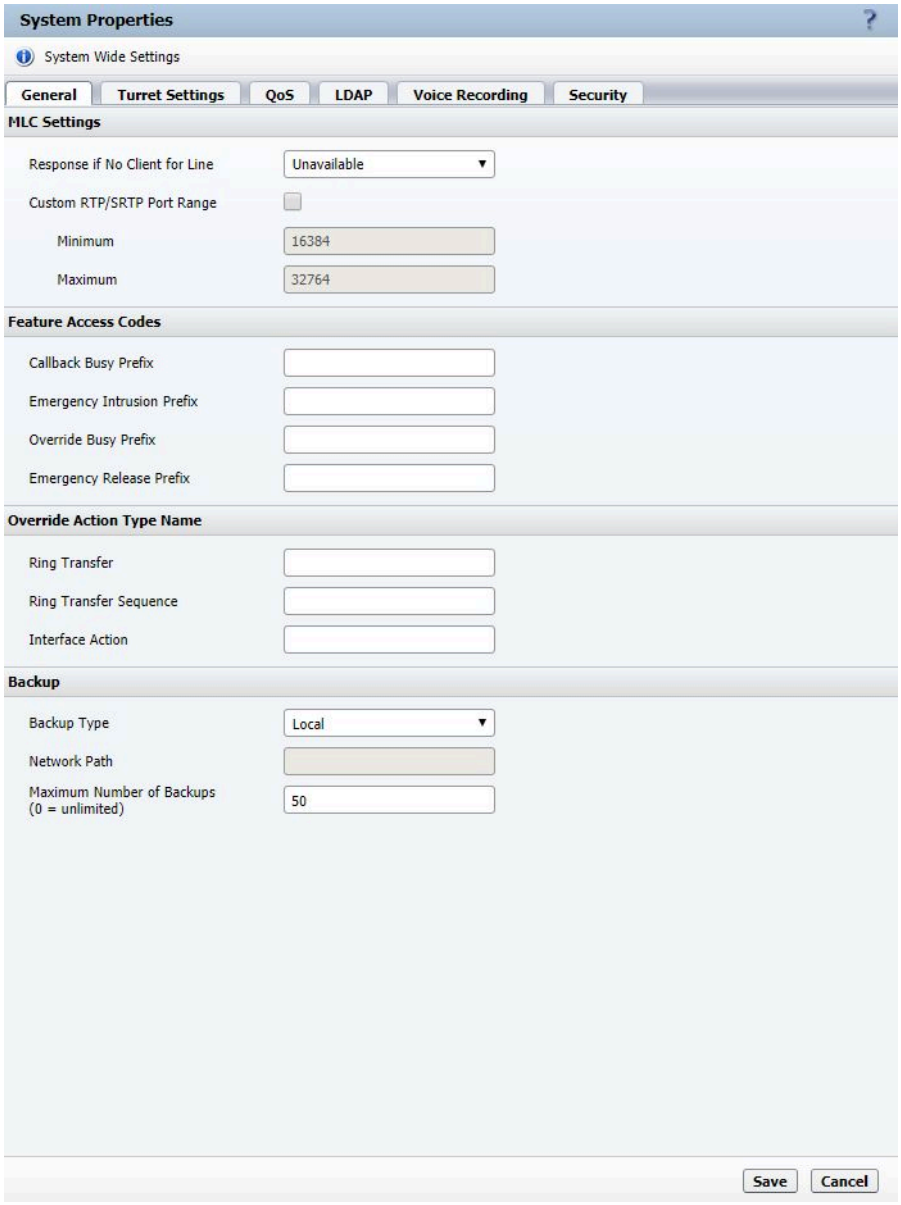
```
>netstat -nap | grep 9004
```

5.15 How to Configure Custom RTP/SRTP Port Range

Step by Step

1) Click **System Properties** on the OpenScape Xpert Management Portal. The **System Properties** dialog appears.

2) Select the **General** tab containing all fields for the general settings.



3) Enter/select the settings in MLC Settings area:

- **Custom RTP/SRTP Port Range**is set to default. The default values are the following:

  Minimum: 16384

  Maximum: 32764

NOTICE:

If **Custom RTP/SRTP Port Range** checkbox is enabled, minimum and maximum values can be set between 2048 and 65535. Maximum value must be greater than the minimum value and it is recommended to set a range greater than 2000.

5.16 Voice Recording Configuration

5.16.1 SIPREC Configuration

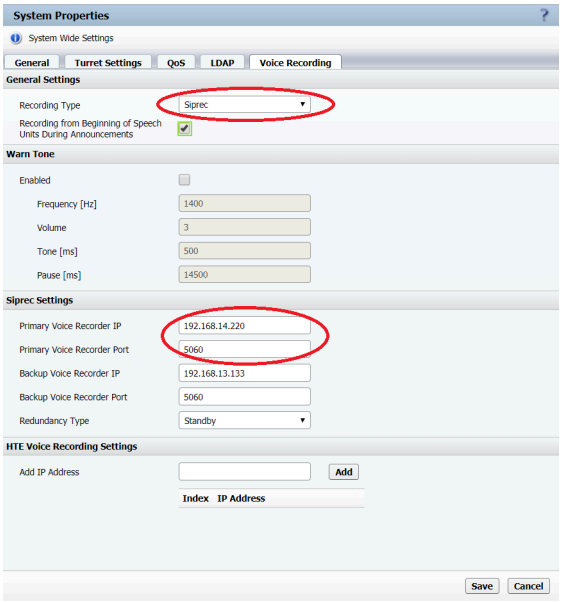
5.16.1.1 Turn on SIPREC Recording Systemwide

Step by Step

1) Click on **System** > **System Properties** > **Voice Recording** tab
2) Select **Siprec** as the type of protocol in **Recording Type** drop-down list.
3) Add the IP address of the primary voice recorder in **Primary Voice Recorder IP** field.

NOTICE:

The default value of the primary voice recorder port is 5060 and is filled automatically if only IP is given.

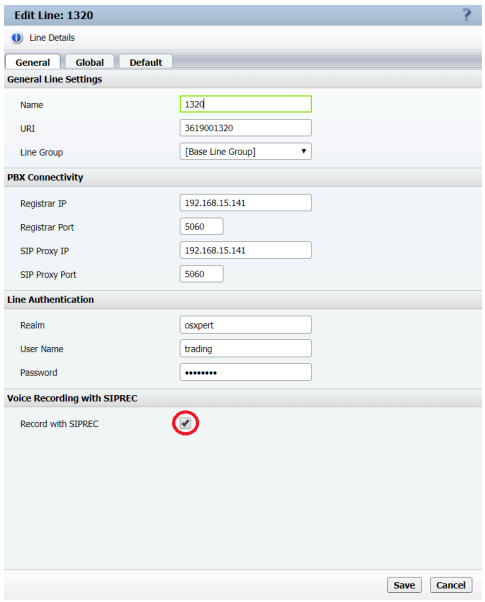


5.16.1.2 Line Recording

Step by Step

1) Click on **Topology** > **Lines**and click on the line name
2) Click on **Global** tab.

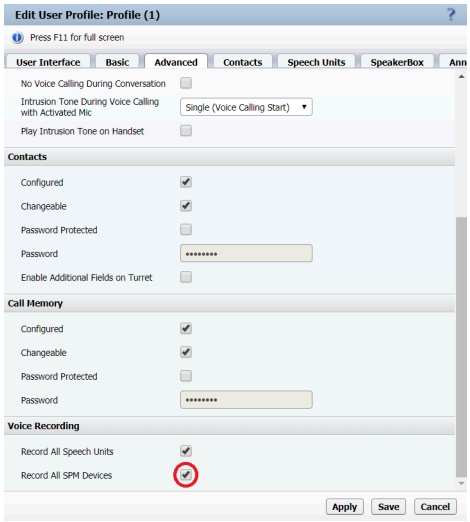
3) Select **Record with SIPREC** in **Voice Recording with SIPREC** tab.



5.16.1.3 SPM Recording

Step by Step

1) Click on **Profile** and click on the selected profile name.
2) Click on **Advanced** tab
3) Select **Recording ALL SPM Devices**



5.16.1.4 Speech Unit Recording

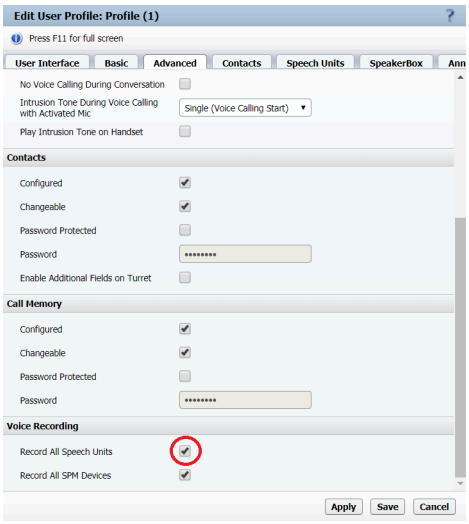
Prerequisites

SU recording is allowed in the profile.

The line is configured for SU recording via **From Beginning**

Step by Step

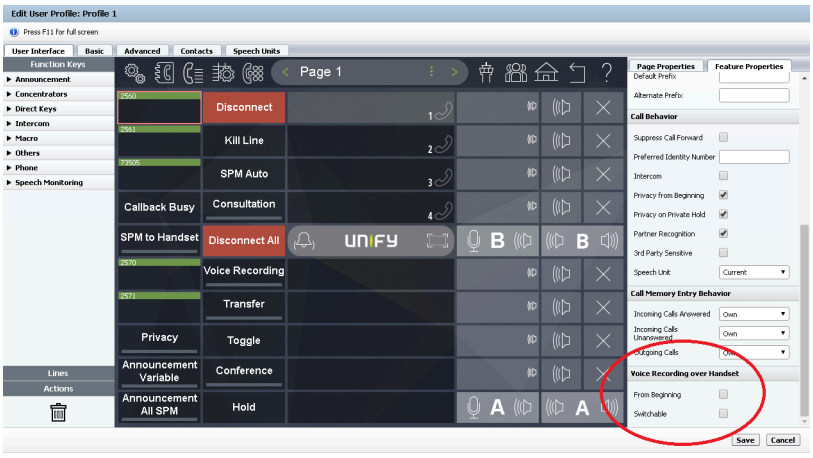
1) Select **Profile**
2) Click on the selected profile name
3) Click on the **Advanced** tab and select **Record All Speech Units**



5.16.1.4.1 How to Configure the Line individually

Step by Step

1) Select **Profile**
2) Click on the selected profile name
3) Select a line
4) Click on **Feature Properties** tab
5) Select **From Beginning** or **Switchable**

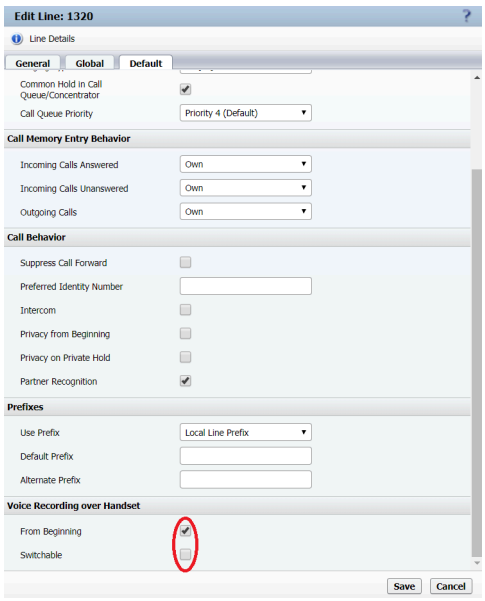


5.16.1.4.2 How to Configure the Line globally

Step by Step

1) Click on **Topology** and select **Lines**
2) Click on the line name
3) Select **Default** tab

4) In the **Voice Recording over Handset** field select **From Beginning** or **Switchable.**

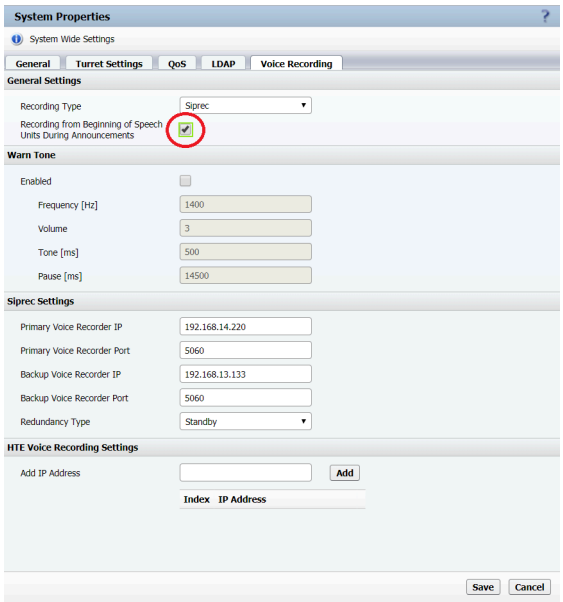


5.16.1.5 Announcement recording

5.16.1.5.1 Turn on Announcement Recording Systemwide

Step by Step

1) Click on **System** > **System Properties**
2) Select **Voice Recording** tab
3) Select **Recording from Beginning of Speech Unit During Announcements**



5.16.1.5.2 The influence of Speech Unit Recording Settings on Announcement

TT settings	1	2	3	4	5	6	7	8
Recording from beginning of SU during announcement (System properties)	off	off	on	on	on	on	off	on
Record all SUs (Profile/ Advanced)	off	on	on	on	on	on	on	off
HS rec from beginning (Profile/Line/Feature prop.)	on	on	on	off	off	on	on	on
HS rec switchable(Profile/Line/ Feature prop)	off	off	off	off	on	on	on	on
Announcement Recording on TT (sw=switchable)	off	off	on	on	on	on	off	off

5.16.1.6 SIPREC Double streaming

Step by Step

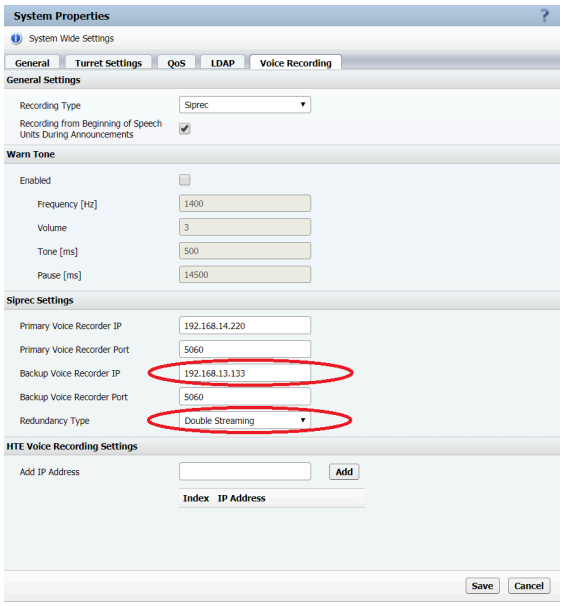
1) Click on **System**
2) Select **System Properties** > **Voice Recording** tab
3) In **Siprec Settings** section add **Backup Voice Recorder IP**

NOTICE:

The default value of the Backup Voice Recorder Port is 5060 and is filled automatically if only IP is given.

---

4) Change the **Redundancy Type** to **Double Streaming**

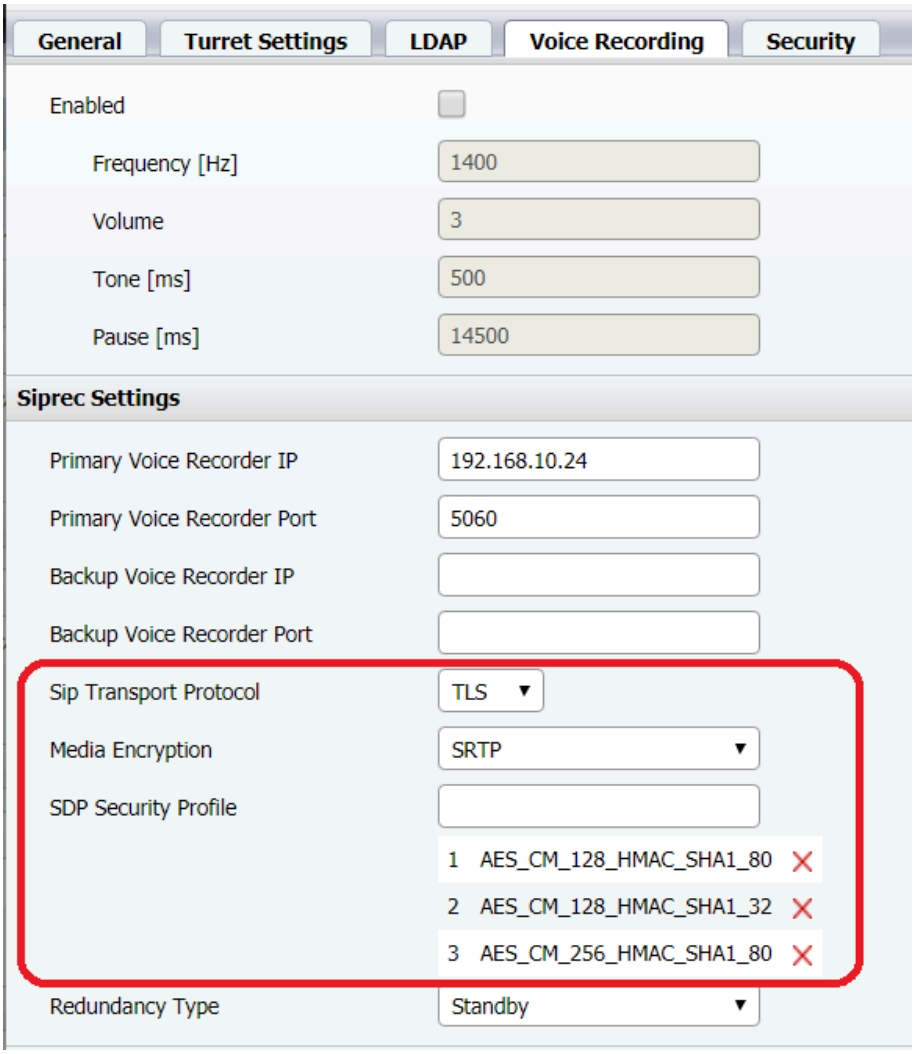


5.16.1.7 Enable Secure SIPREC

Step by Step

1) Navigate to **System > System Properties > Voice Recording** tab.
2) Select **TLS** for **Sip Transport Protocol** in **Siprec Settings**.
3) Select **SRTP** or **RTP+SRTP** for **Media Encryption**.

4) Add the necessary **SDP Security Profiles**.



5.16.1.8 Restrictions

5.16.1.8.1 Line Recording and multiple SUs participating
OpenScape Xpert does not provide information about all Xpert clients that were participating in the same Call via their Speech Units, i.e.:only one Speech Unit is forwarded as an Xpert side participating in Line Recordings.

5.16.1.8.2 Conferences on SPM
When a Line that participates in a conference is on SPM, conference members are not all forwarded in the XML metadata to the SRS.Only call information of the actual Line which is on SPM is sent. It applies to the Quick Conferences (Line Conference) and 3 way SIP conferences.

5.16.1.8.3 Muting SPM Channel
It does not affect recording data (start/end time) although the channel will not be recorded (only silence).

5.16.1.8.4 Muting SPM Unit
It does not affect recording at all. The voice will be recorded.

5.16.1.8.5 Announcement and Speech Unit interactions

- If you have a recorded basic call on the same Speech Unit you can do an Announcement Variable without recording. After the announcement is finished you do not start again the recording of the (new) basic call.
- If you have a recorded basic call and on the same Speech Unit you can do an Announcement Variable with recording. After the announcement is finished you do not create a new entry for the remaining basic call and the recording continues as an announcement recording.

5.16.1.8.6 Recording indication on the Xpert Client GUI

Recording configuration is displayed on Lines and SPMs with a hollow red circle. Active recording is indicated as a full red circle (Recording icon) and recording errors are indicated as yellow exclamation marks.

Recording indications reflect only the relevant entity's recording state and do not reflect if there is active recording in the whole system for that call at all.

Example:

- TT1 SU1 is recording Line1
- TT2 seizes Line1 too (shared line) but recording fails for some reason

Result:

- TT1 SU1 is recording Line1
- TT2 SU1 indicates error recording: a user might falsely think his voice is not recorded.

  SU and Line recording interactions: When a Line is configured for recording but the SU is not, there won't be a recording indication on the SU. Recording will be indicated on the Line Key only.

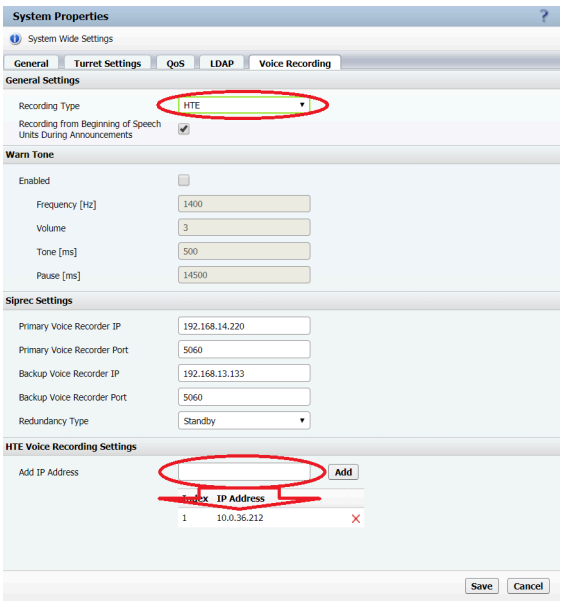
5.16.1.9 HTE Recording Configuration

5.16.1.9.1 Turn On HTE Recording Systemwide

Step by Step

1) Click on **System** > **System Properties** > **Voice Recording tab**
2) Change **Recording Type** to **HTE** in **General Settings** section.

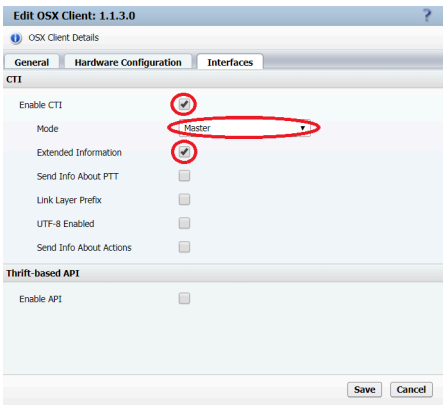
3) Enter an IP address to **Add IP Address** in **HTE Voice Recording Settings** section and press the **add**.button.



5.16.1.9.1.1 How to Setup a Master Turret

Step by Step

1) Click on **Topology** > **OSX Clients**
2) Select a client by Node Address
3) Click on **Interfaces** tab
4) Select **Enable CTI**
5) Change to **Master** in the **Mode** drop-down list
6) Select **Extended Information**

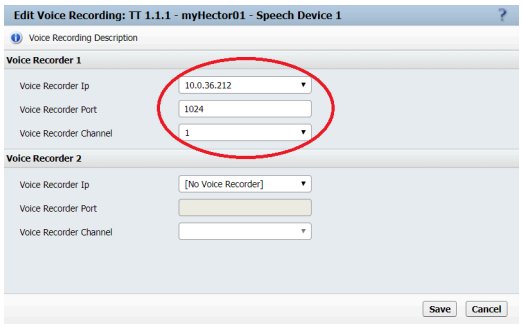


5.16.1.9.1.2 Assign Recorder to Device

Step by Step

1) Click on **Topology** > **HTE Voice Recording**
2) Select the Device (Speech Device, SMP or line)

3) Select the **Voice Recorder IP** and the other settings if necessary.



5.17 CSTA presence indication for DKA

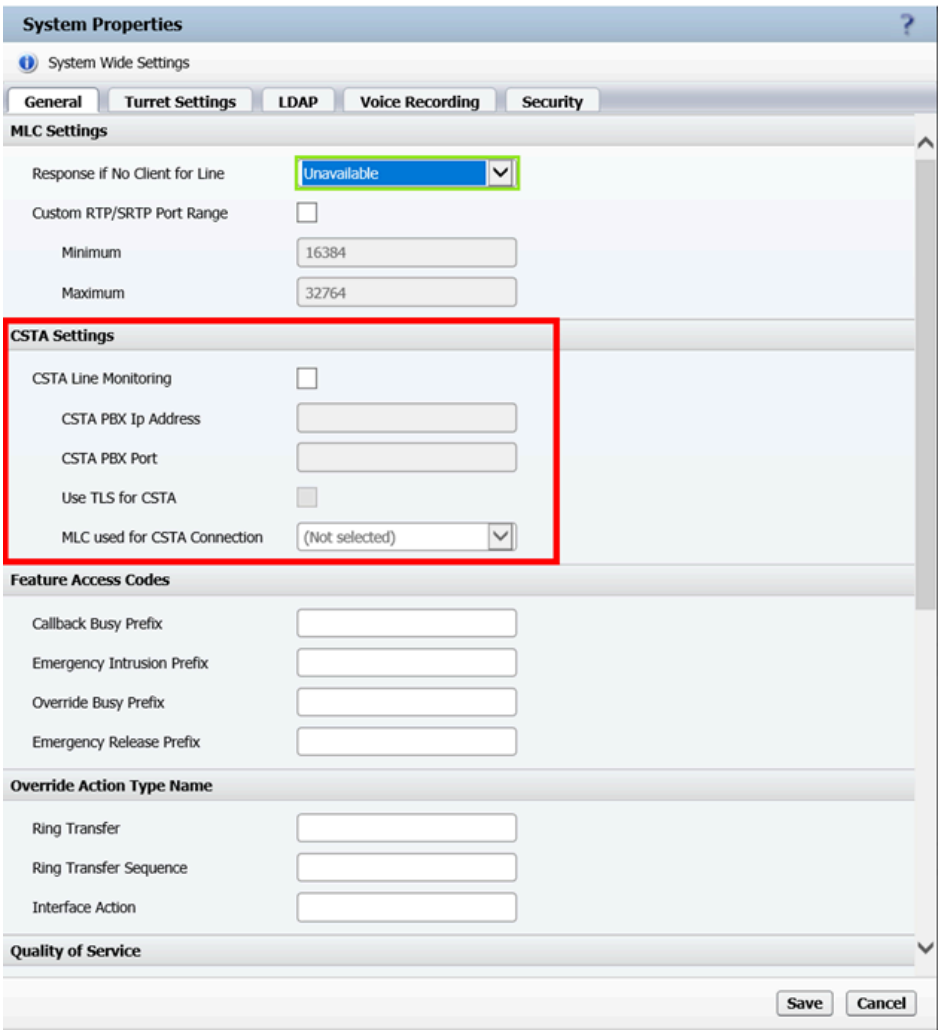
Users can view the presence status of the DKA (speed dial key) target numbers or lines. OpenScape Xpert system can perform a line monitoring in the company's PBX via the CSTA. DKA target numbers or lines can only be monitored if they are extensions in the company's PBX.

- One SM can only have one MLC connected to the CSTA interface of the PBX.
- The suggested configuration is one separate MLC for CSTA functionality.

5.17.1 Configuring the presence indication for DKA in OpenScape Xpert

Step by Step

1) Navigate to **System Properties > General**.



2) Select the **CSTA Line Monitoring** checkbox to enable the feature.
3) Enter the IP address of the CSTA server in the **CSTA PBX IP Address** field.
4) Enter the port address of the configured CSTA application in the **CSTA PBX Port** field.
5) You may select the **Use TLS for CSTA** checkbox to enable the TLS for the CSTA connection.
6) Select an MLC from the dropdown list which will be used for the CSTA connection.

If the CSTA Line Monitoring is enabled but the selected MLC is not available, then a system notification will be displayed on the Dashboard. The following errors might appear:

- Selected MLC is not available (red status in MLC list)
- Selected MLC is unassigned (white status in MLC list)

5.17.2 Configuring the CSTA interface for DKA in OpenScape 4000

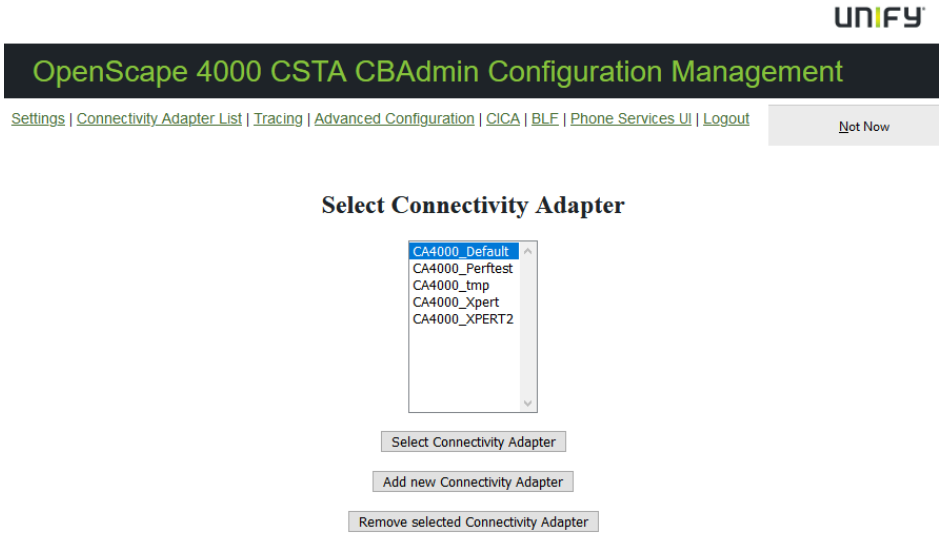
Step by Step

1) Add a new Connectivity Adapter:

a) Navigate to **Assistant > Expert Mode > CSTA.**

b) Click on **Add new Connectivity Adapter**.

c) Enter a name and click on **Add CA**.



2) Select the new Connectivity Adapter and configure the following:

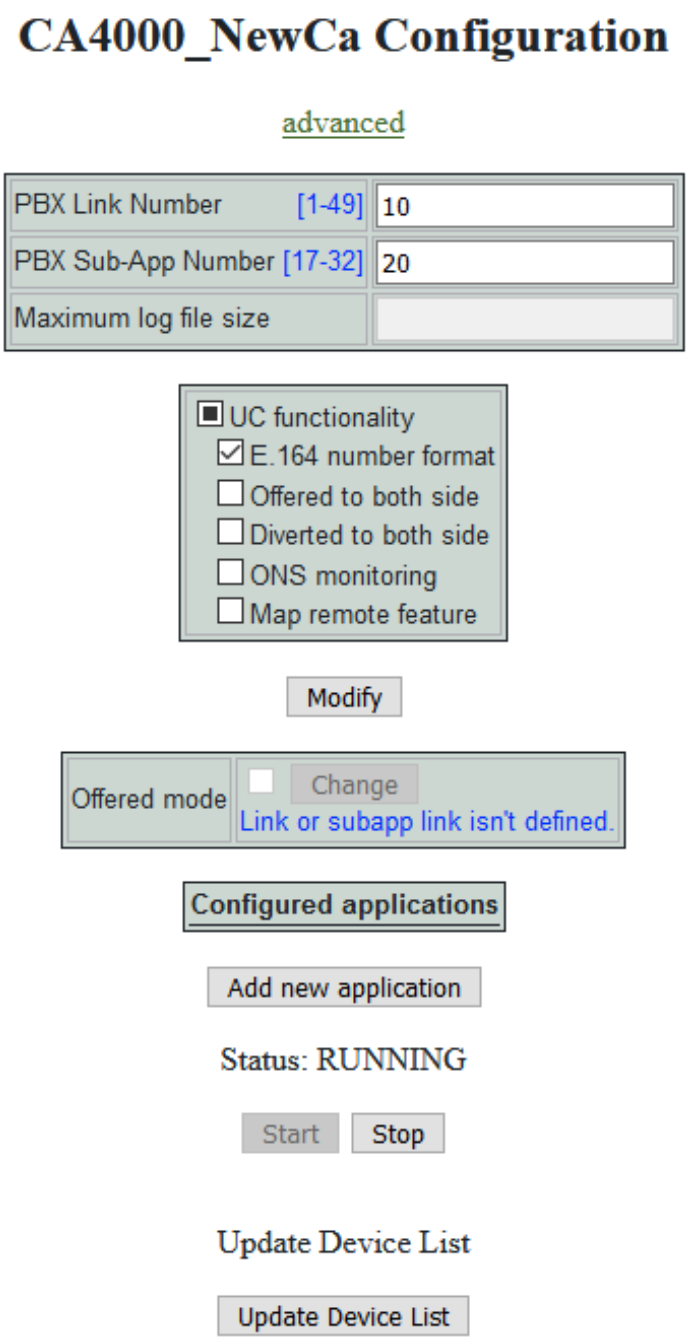
a) Enter the PBX link Number.

b) Enter the PBX Sub-App Number.

c) Optionally select the **E.164 number format** checkbox.

a) Click **Modify**.

For RMX persistence, a manual update is needed: EXEC-UPDAT:UNIT=A1,SUSY=ALL.

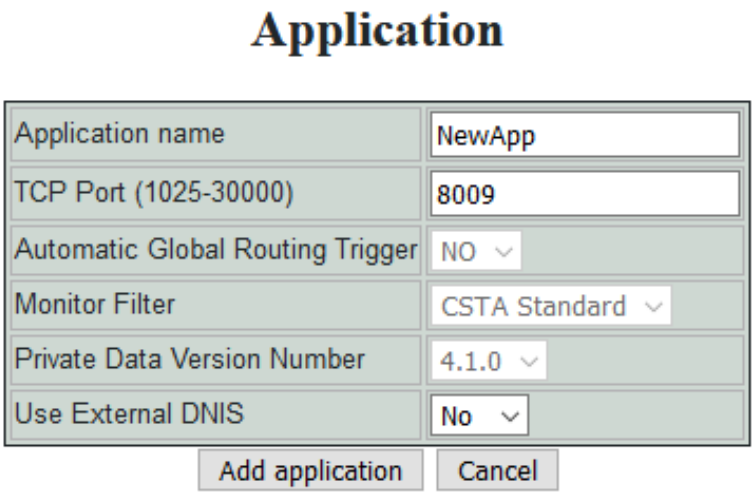


3) Click on **Add new application** and configure the following:

a) Enter the Application name.

b) Enter the TCP Port.

c) Click on **Add application**.

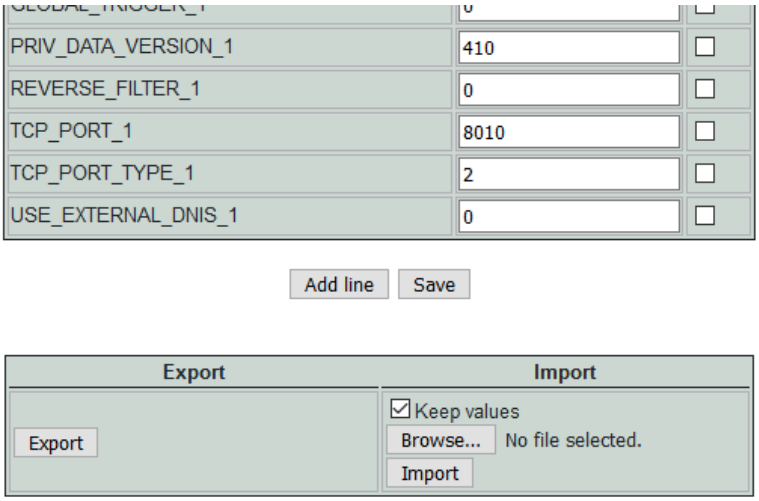


4) Click **Advanced** link and add the following parameter:

a) Click on **Add line**.

b) Enter the name of the parameter SNAPSHOT_DATA_IN_RESPONSE_<port 1-4> and add the value 1

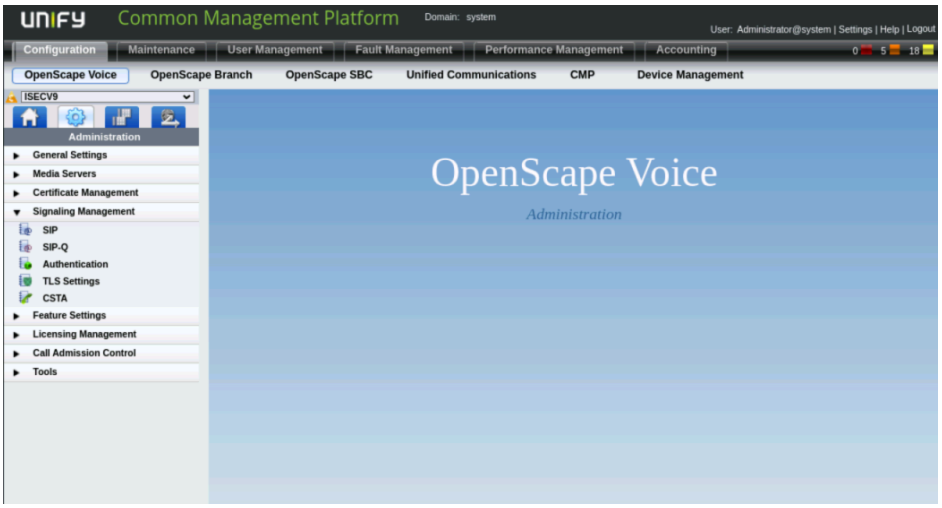
c) Click on **Save**.



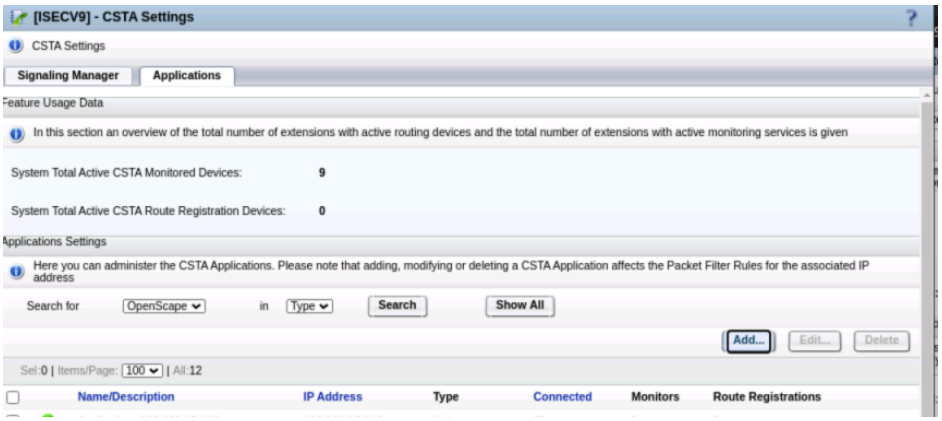
5.17.3 Configuring the CSTA interface for DKA in OpenScape Voice

Step by Step

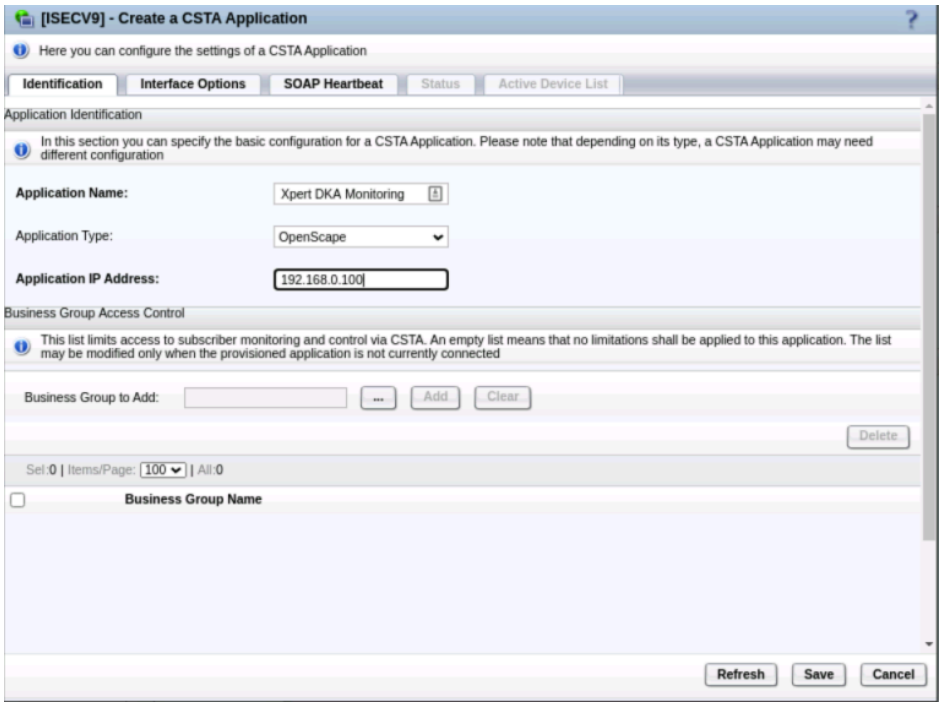
1) Open CMP: Navigate to **Configuration > OpenScape Voice > Administration > Signaling Management > CSTA**



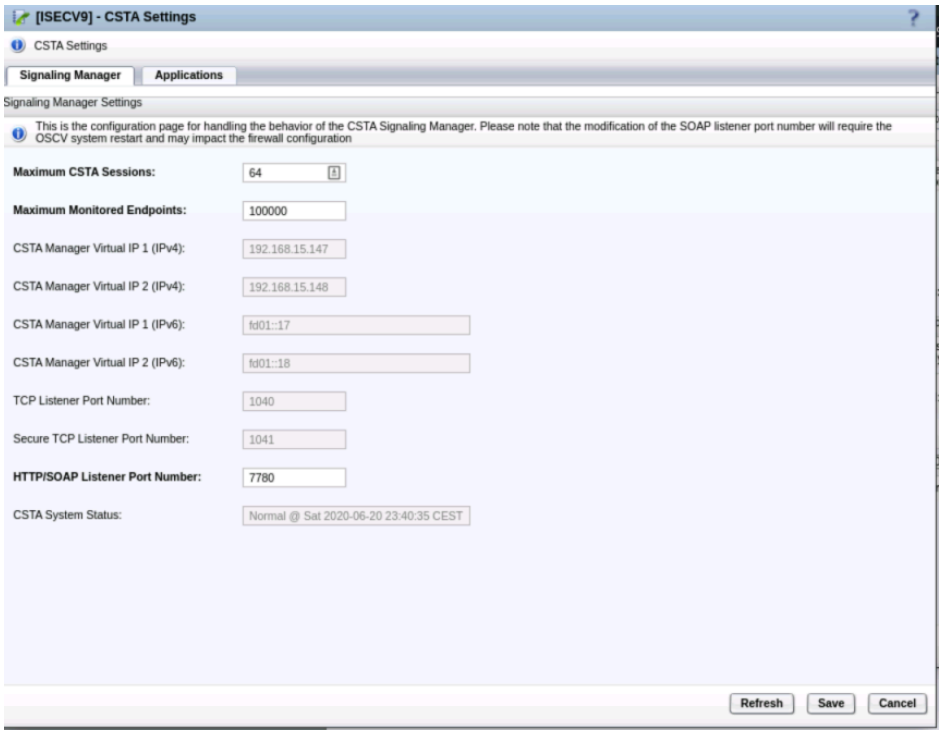
2) Navigate to **Application Tab > Application Settings > Add**



3) Add the IP address of "MLC used for CSTA Connection" as a new CSTA application



4) Navigate to **CSTA Settings > Signalling Manager tab**to configure CSTA IP/Port



NOTICE: When TLS is used for the CSTA connection, **the certificate, the privacy key** and **the trust store** has to be set manually on the MLC. See chapter Install certificate for CSTA TLS connection

5.17.4 Install certificate for CSTA TLS connection

The CSTA TLS settings are similar as the SIP TLS settings, the difference consists of the configuration directory, which is: `/etc/cert/csta`

Step by Step

1) Copy CA certificate(s) to file path:
   `/etc/cert/csta/ca-cert.pem`
2) Copy MLC certificate (chain) to:
   `/etc/cert/csta/client-cert.pem`
3) Copy MLC private key to:
   `/etc/cert/csta/.key/client-key.pem`
4) Check ownership and permissions of the file.

   The user/group owner and the permissions are set up on the MLC package installation and updates. It is not recommended to change these permissions.

   The followings are the default settings:

   - `-rw-rw-r-- 1 mlcadmin certificate 4844 Aug 1 15:52 ca-cert.pem`
   - `-rw-rw-r-- 1 mlcadmin certificate 2217 Aug 1 15:52 client-cert.pem`
   - `-r---w---- 1 mlc certificate 1828 Aug 1 15:52 .key/client-key.pem`

5.18 Manually install certificates for SIP connection

5.18.1 Installing certificate for SIP TLS connection

Step by Step

1) Copy CA certificate(s) to file:
   `/etc/cert/sip/ca-cert.pem`
2) Copy MLC certificate (chain) to:
   `/etc/cert/sip/client-cert.pem`
3) Copy MLC private key to:
   `/etc/cert/sip/.key/client-key.pem`

4) Check ownership and permissions of the file.

The user/group owner and the permissions are set up on the mlc package installation and updates. It is not recommended to change these permissions.

The followings are the default settings:

- `-rw-rw-r-- 1 mlcadmin certificate 4844 Aug 1 15:52 ca-cert.pem`
- `-rw-rw-r-- 1 mlcadmin certificate 2217 Aug 1 15:52 client-cert.pem`
- `-r---w---- 1 mlc certificate 1828 Aug 1 15:52 .key/client-key.pem`

5.18.2 OCSP configuration for SIP

OCSP revocation check is performed when AIA with OCSP URI is available in the certificate. The response is validated with the Root CA certificates (/etc/cert/sip/ca-cert.pem) and the certificates in the verified certificate's chain.

When the OCSP response does not contain the signing certificate, it must be added to the OCSP certificate store "/etc/cert/sip/ocsp-cert.pem".

For Explict Trust Model (see UCR CYB-048000) an OCSP Signing trust must be added to the selft-signed certificate, (openssl x509 -in certificate.pem -out certificate-trusted.pem -trustout -addtrust OCSPSigning) and the trusted certificate must be appended to the ca-cert.pem file.

5.19 Configure MLC continuous SIP Message Tracing

MLC continuous SIP Message Tracing is activated by default. SIP Message Trace PCAP files are automatically created under /var/mlc, the PCAP file actively written to is /var/mlc/sip_trace.pcap. With the default settings the MLC creates a new sip_trace.pcap file after 100MBs and keeps a maximum of 10 files.

5.19.1 Disk space considerations

With the default settings, 10 x 100MB SIP Message Trace files 1GB of disk space is needed on the partition for /var/mlc. The MLC has a watchdog to prevent its partitions from filling up. The MLC minimum disk space requirements (currently: 50GB+) is not changing as the partition watchdog will always free up enough space by deleting the oldest traces. Having 50+ GB available can hold multiple months of trace data for MLC systems under heavy load.

SIP Message Trace PCAP files of 100MB cover around 1 hour of SIP traffic for an MLC system establishing 3.000 calls per hour, which is the maximum dynamic load (3.000 BHCA) the MLC is rated for.

5.19.2 Changing parameters

MLC continuous SIP Message Tracing can be turned on and off and its parameters can be adjusted in:

```
/var/mlc/mlccp_logger_settings.lcp
```

The MLC application automatically detects any changes made to this file. A reboot is not needed.

Look for the SipTraceFile part in the LCP config file.

5.19.2.1 Activating SIP Message Tracing

Trace level should be on TRACE (Default):

```
log4cplus.logger.SipTraceFile=TRACE,
SipSession log4cplus.additivity.SipTraceFile=false
```

Deactivating SIP Message Tracing.

5.19.2.2 Change the trace level from TRACE to INFO

```
log4cplus.logger.SipTraceFile=INFO,
SipSession log4cplus.additivity.SipTraceFile=false
```

5.19.2.3 Setting SIP Message Tracing file sizes

With the default settings the MLC creates a new sip_trace.pcap file after 100MBs and keeps a maximum of 10 files.

```
# sip trace appender
log4cplus.appender.SipSession=log4cplus::RollingFileAppender
log4cplus.appender.SipSession.MaxFileSize=100MB
log4cplus.appender.SipSession.MaxBackupIndex=10
```

5.19.3 Locating the proper PCAP file for diagnosis

When collecting diagnosis data trace file modification dates of the /var/log/sip_trace.pcap files can help to find the relevant SIP Message Trace PCAP file that should be provided.

NOTICE: All trace files should be provided, if you are not sure which is the correct file.

5.20 Using Unify Office lines in MLC

Starting with version V7.5, it is possible to use Unify Office lines as SIP lines in OpenScape Xpert. To use such lines a dedicated MLC is required as a different operation mode is needed for the system to properly work.

5.20.1 Setting Up in MLC

To perform the setup in MLC, follow the steps below:

Step by Step

1) Login to MLC as "root".
2) Stop MLC by running the following command:
   `/etc/init.d/mlc stop`
3) Edit the `MlcSettings.ini` configuration file to add a new line, using the following command:
   `echo 'SipTlsCiphers=kRSA' >> /var/mlc/MlcSettings.ini`
4) Check the `MlcSettings.ini` configuration file to ensure it has been correctly edited, using the following command:
   `cat /var/mlc/MlcSettings.ini`
5) Start MLC again using the following command:
   `/etc/init.d/mlc start`

5.20.2 Setting Up in System Manager

MLC Settings

On MLC General Settings, open the **Operation Mode** tab and select **Unify Office**.

The SIP Registrar and Proxy of Unify Office cannot be used directly. It is mandatory to set the Outbound Proxy Settings on the MLC **Sip Connectivity** tab. The required settings change by region and transport protocol. The list of usable proxies can be found either in Unify Device Installation Service, in the SIPProxy setting of the device, or on the Unify Office service page, Device Setup & Provision SIP device.

At the time writing, the list of TCP outbound proxies contains:

Europe, the Middle East and Africa (EMEA)
sip40.ringcentral.com:5096
South Africa (SA)
sip90.ringcentral.com:5096
Asia Pacific and Japan (APAC)
sip60.ringcentral.com:5096
sip50.ringcentral.com:5096
sip70.ringcentral.com:5096
North America (NA)
sip10.ringcentral.com:5096
sip20.ringcentral.com:5096
Latin America and the Caribbean (LATAM or LAC)
sip80.ringcentral.com:5096

Europe, the Middle East and Africa (EMEA)
sip40.ringcentral.com:5090
South Africa (SA)
sip90.ringcentral.com:5090
Asia Pacific and Japan (APAC)
sip60.ringcentral.com:5090
sip50.ringcentral.com:5090
sip70.ringcentral.com:5090
North America (NA)
SIP10.ringcentral.com:5090
SIP20.ringcentral.com:5090
Latin America and the Caribbean (LATAM or LAC)
sip80.ringcentral.com:5090

NOTICE: Make sure you choose an outbound proxy that fits the region and the MLC SIP Transport Protocol setting.

In case of TLS SIP Transport, set the Media Encryption to **SRTP**.

Line Settings

It is possible to create the line configuration in Unify Device Installation Service, and import the settings on the **Lines** settings page in System Manager.

To configure the lines manually, you can get the required settings can from the **Unify Office Service** page.

SM Line setting on General tab	Setting name in Unify Office
URI	Username
Registrar	SIP domain without port (e.g., sip.ringcentral.com)
Registrar port	Remote SIP port
SIP Proxy	SIP domain without port (e.g., sip.ringcentral.com)
SIP Proxy Port	Remote SIP port
Realm	SIP domain without port (e.g., sip.ringcentral.com)
User Name	Authorisation ID
Password	Password

5.20.3 Using Unify Office

To call an Unify Office line you can use the extension number of that line or dial **00** before the phone number (in E.164 format).

Restriction:

The call forwarding feature is available only for answered calls.

5.20.4 Unify Device Installation Service (Unify DIS)

With Unify Device Installation Service, the SIP Line information can be fetched from Unify Office and converted to the OpenScape Xpert System Manager SIP Line import format. This reduces the manual administration efforts when OpenScape Xpert is used with Unify Office.

Follow the steps below to configure the Unify Device Installation Service (Unify DIS):

Step by Step

1) Log in to the Unify DIS server with your Unify Office administrator credentials.
2) Import data from Unify Office to Unify DIS. Depending on the number of lines, this might take a couple of minutes.

3) Edit the devices you wish to import to OpenScape Xpert, by clicking the **Edit** button.

a) Assign the **OpenScape Xpert** profile to the editing device, by selecting it from the **Profile** drop-down menu.

b) Store the **Profile** change by pressing the **Store** button displayed on the top-left corner of the screen.

c) Continue editing the Device information by pressing **Edit** again. After selecting your Openscape Xpert profile, the fields to be edited will be displayed on the right side of the screen.

Edit the following field:

- **SIPProxy** and **SIPProxyPort**: select an option from the drop-down menu, according to your region and settings.

  E.g.

  SIPProxy: EMEA-TLS: sip40.ringcentral.com

  SIPProxyPort: EMEA-TLS: 5096
- **_idx**: add your running index.

  NOTICE: All Unify Office Devices to be imported to OpenScape Xpert need to have a unique index number, starting from 1.
- **MAC Address**: add an arbitrary MAC address and enter the value of the **_idx** field at the end of it, in brackets, as displayed in the example below:

  E.g. 005056b0cc1a**(4)**

  NOTICE: You must use the same MAC address for all the SIP Lines of OpenScape Xpert installation.
- **Realm**: fill in the Realm field according to your needs.

  E.g.: sip.ringcentral.com

4) After configuring all the Devices/ SIP Lines to be exported from Unify DIS, click the **Generate ConfigFiles** button, displayed next to any of the configured Devices. This will generate the data to be exported for All Devices.

5) Download Devices/ SIP Lines data by pressing the **Download ConfigFiles** button, displayed next to any of the configured Devices.

6) Extract the **configfiles.zip** file. Import the SIP Lines from the excel file named according to your arbitrary MAC address into the OpenScape Xpert System Manager, by navigating to **OpenScape Xpert Management portal** > **Lines** > **Import**.

5.21 Local DNS caching for MLC

This section describes the steps to configure DNS caching for MLC.

DNS caching, as supported by MLC through **systemd-resolved**, involves caching the results of DNS queries to improve the speed of DNS lookups for frequently accessed domain names.

NOTICE: This caching mechanism applies to the entire system, not only to MLC.

5.21.1 Configuration

systemd-resolved is installed by default on Debian and Ubuntu, as a part of **systemd**.

To configure **systemd-resolved** for DNS caching, follow the steps below:

Step by Step

1) Open the `resolved.conf` file, located in `/etc/systemd/resolved.conf`, and edit it according to your needs:
   - Set DNS servers in the **DNS=** section.

     The IP addresses of the DNS must separated by spaces.

     IPv6 addresses must be placed inside square brackets (e.g. [fd01::1]).
   - Uncomment the **DNSStubListener=** section and set it to **yes**.
2) Ensure that `/etc/resolv.conf` is a symbolic link to `/run/systemd/resolve/stub-resolv.conf`.

   For this, run the following command:
   `ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf`
3) Ensure that **systemd-resolved** service is enabled using the following command:
   `systemctl enable systemd-resolved.service`
4) Restart the **systemd-resolved** service using the following command:
   `systemctl restart systemd-resolved.service`

Once the steps above are successfully performed, the **systemd-resolved** stub listener acts as a local DNS server and listens on `127.0.0.53:53`.

Going forward, the `/etc/resolv.conf` file should not be edited directly. If you need to edit the DNS configuration or settings, you can modify the `/etc/systemd/resolved.conf` file as described in step 1, then restart the **systemd-resolved** service for the changes to take effect.

5.21.2 Usage

Once the DNS caching is correctly configured, you do not need to perform any further configuration steps.

The following additional options are available for DNS caching:

- To check statistics about the cache, run the following command:
  `systemd-resolve --statistics`
- To clear the cache:
  `systemd-resolve --flush-caches`

6 Configuration of OpenScape Xpert Turrets and Clients

This chapter describes the steps to configure OpenScape Xpert turrets and clients.

6.1 Configuring OpenScape Xpert Client PCs in Windows 10®

This section describes how the OpenScape Xpert client can be configured correctly at Windows 10 systems and shows some configuration examples.

6.1.1 How to Setup an OpenScape Xpert Client PC in Windows 10

Proceed as follows to setup an OpenScape Xpert client in an Windows 10 environment at the customer's system.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Setup at the AD Server a domain user with password

2) Login with local administrator rights.

3) Set **static IP address**, **Subnet mask**, **Default Gateway** and **Preferred DNS server** at **Internet Protocol Properties** of the network card.

4) OpenScape Xpert client is member of workgroup, join OpenScape Xpert client into Domain:

a) **My computer** (right mouse click) -> **Properties** -> **Advanced system settings** -> **Computer Name** Tab -> **Change**

b) Do not restart the system!

5) Add Local Admin Rights to the Domain User:

a) **Start** -> **Control Panel** -> **User Accounts** -> **Manage User Accounts** -> **Add** -> **"username" / yourdomain.xxx** -> **Administrator**.

b) **Log off** -> **Log on** -> **Restart PC**

6) Check if the name of the OpenScape Xpert client appears under"Computers" in the Active Directory Server.

7) Logon with the domain user:

a) **Switch User** -> **yourdomain.xxx\username**

b) Enter Password.

8) Start Command Prompt: **Start** -> **Command Line** -> **cmd**

- „Ipconfig /all": displays IP address
- „Ipconfig /release": releases IP address
- „Ipconfig /renew": renews IP address (from DHCP Server, if available)
- Check if you can find the IP address is in AD Server under DHCP in menu „Active Leases"

9) Check DNS:

- At the Server: Start -> Command Line -> cmd -> nslookup "yourservername"
- At the OpenScape Xpert PC client: Start -> Command Line -> cmd -> nslookup "yourpcname"

IMPORTANT: From OpenScape Xpert V7 onward the Qos Packet Scheduler does not need to be disabled for the network adapter. For older versions, QoS Packet Scheduler needs to be disabled for the network adapter because it may prevent the turret from connecting to the System Manager server. In this case, please, ensure that the SM server and the clients are in the same VLAN and the network devices are supporting tagged packets. If tagging of the packets is not required then the QoS Packet Scheduler must be disabled to prevent the problem.

6.1.2 How to Install OpenScape Xpert Client SW via Network under Windows 10

Prerequisites

IMPORTANT:

First time software installation and manual software update/ upgrade requires administrator access rights.

Step by Step

1) At the OpenScape Xpert client open a browser and type into the address bar: `https://<SM name or IP>/download`

2) Click on: `SetupOSXpertClient.exe`

a) Assign the correct name of the SMSERVER which administrates and contains the data base.

b) If a proxy server is needed to establish the connection between System Manager and the client, it can be configured in this step.

6.1.3 How to Setup Autologin and Autostart at the OpenScape Xpert Client

Step by Step

1) Login at the OpenScape Xpert client as domain user (yourdomain.xxx \username).

2) **Start** -> type in `regedit` -> click on `Registry Editor` in search results.

3) Go to `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.

4) Adjust the correct “DefaultUserName”: “yourdomain.xxx\username”

5) Setup the new String Value “DefaultPassword” and enter the Password.

6) Copy `OpenScape Xpert Client.lnk` shortcut from Desktop or from Start menu into: **C:\Users%USERNAME%\AppData\Roaming\Microsoft \Windows\Start Menu\Programs\Startup** directory.

Next steps

Configure the firewall.

6.1.4 How to Configure the Firewall Settings at the Client under Windows 10

Step by Step

1) Go to the Firewall settings:
   - **Start** -> Type **Windows Defender Firewall** and click on **Windows Defender Firewall** in search results.
2) Click on **Allow an app or feature trough Windows Defender Firewall** link.
3) Click on **Change settings** button.
4) Click on **Allow another app... button** -> **Browse** -> C: \Program Files (x86) \Trading_E\Tb\Turretip.exe -> **Open** button -> **Add** button.
5) Click on **Allow another app...** button -> **Browse** -> C: \Program Files (x86)\Trading_e\Tb\TurretQaxy.exe -> **Open** button -> **Add** button

With these settings the Client can start and connect to the System Manger. For more information, please refer to IFMDB for a list of used ports.

6.1.5 How to configure IPv6 address for Windows soft clients

The IP Addressing Modes described in chapters 3.1.2.6- 3.1.2.12 are valid for OpenScape Xpert components including Turrets.

Related Windows settings for soft client are the same as for the System Manager. These are also included in sections 3.1.2.6- 3.1.2.12.

6.2 How to change the USB Mode from USB 2.0 to USB 1.0/1.1 on the 6010p V1R0 (X18) Device

Disable USB 2.0 on the OpenScape Xpert 6010p V1R0 (X18) turrets before the OpenScape Xpert application is installed.

NOTICE:

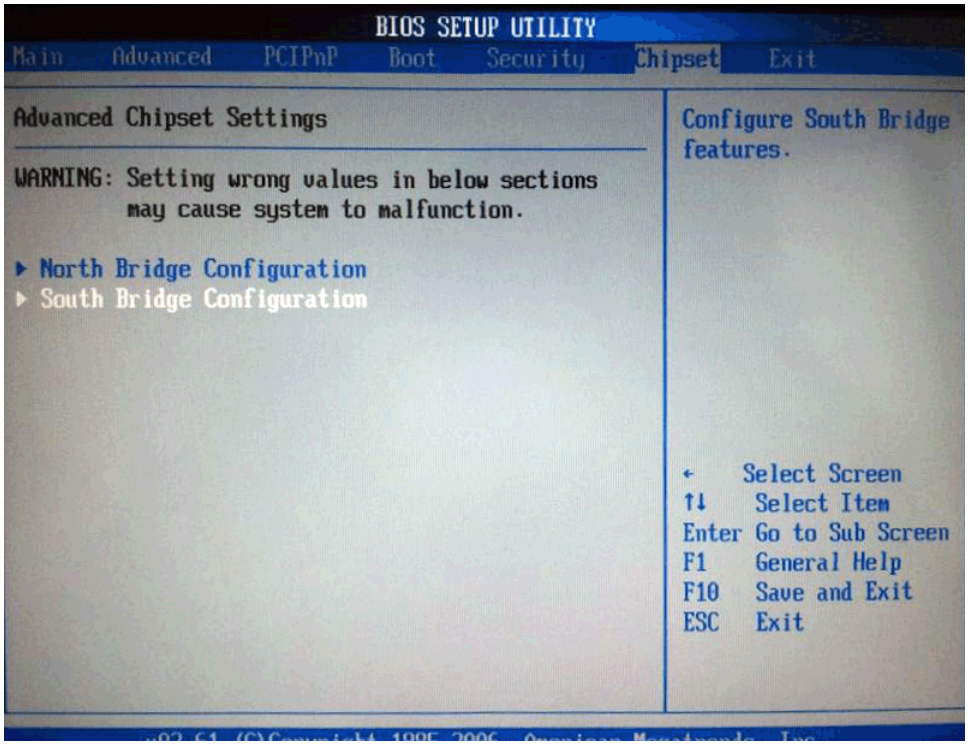
This step must be carried out on OpenStage Xpert V1R0 (X18) devices only.

Step by Step

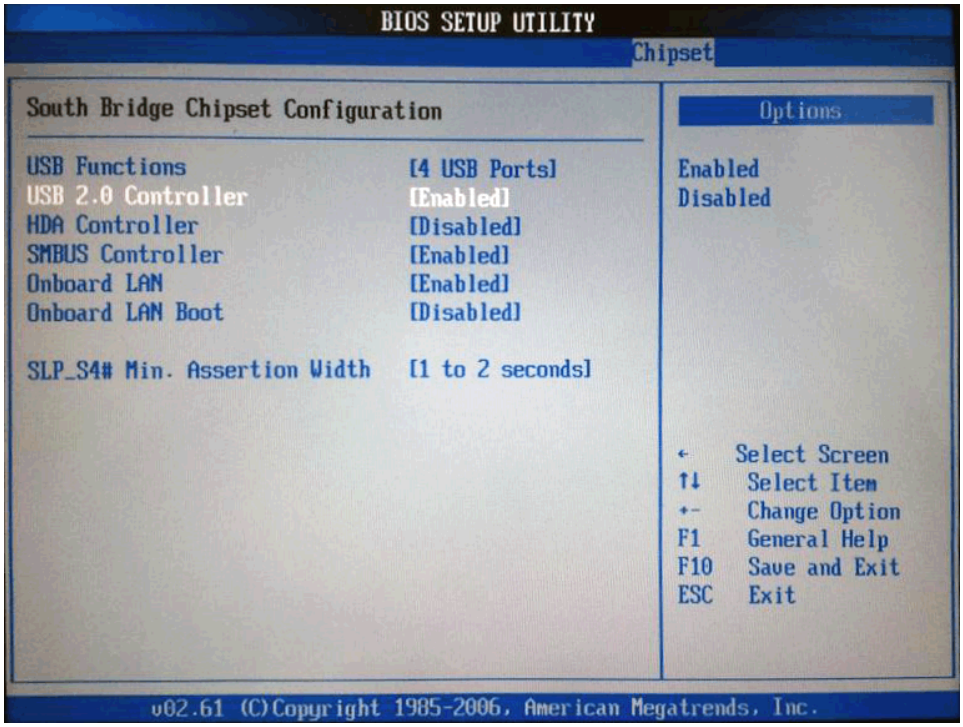
1) Enter the BIOS by pressing the **DEL** key during start up.

   The **BIOS SETUP UTILITY** window appears.

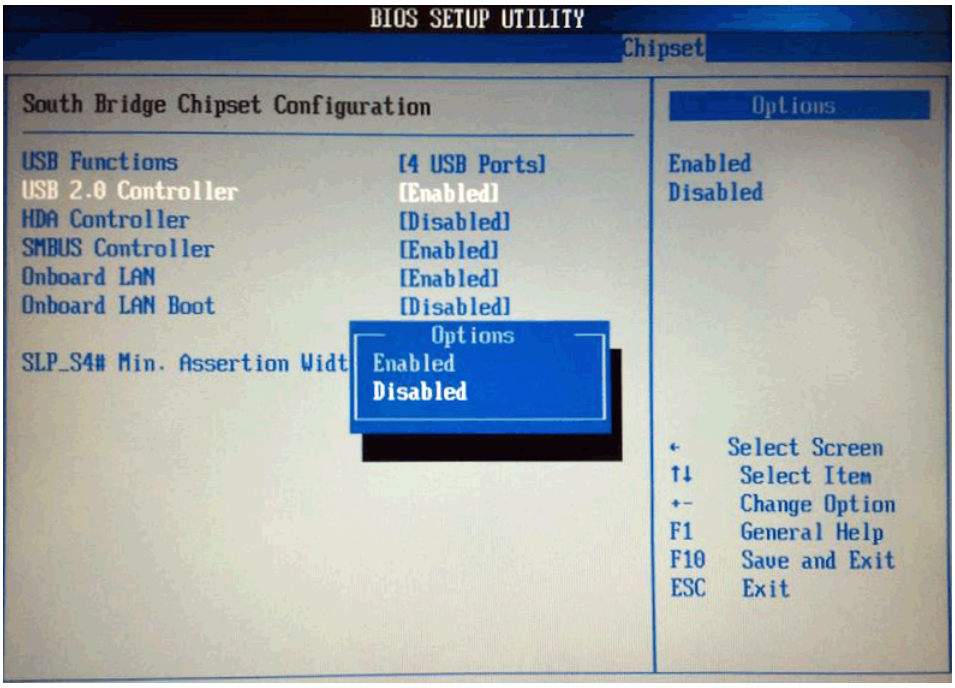
2) Switch to the **Chipset** tab and choose **South Bridge Configuration**:



3) Select the **USB 2.0 Controller**.



4) Change the **USB 2.0 Controller** to **Disabled**:



5) Press the **F10** function key to save the change and exit the BIOS.

The USB 2.0 mode has been changed to USB 1.0/1.1.

6.3 OpenStage Xpert 6010p Linux Image Setup

This section describes the installation of the Linux image on an OpenStage Xpert 6010p device using a USB stick.

The following users are configured in the Linux image:

- `ttengnr` – has read rights on several folders (logs, settings, etc)
- `ttinstall` - can install the .deb packages (used by the Diagnosis Tool)
- `ttadmin` - can configure the system and install packages
- `turret` - can run the OpenScape Xpert client software
- `root` - the superuser - can't be used for login

The passwords for the first 3 users can be found in the .pwds file, which needs to be downloaded with the Linux image (.img).

There is a user for recovery mode:

- user: `tc`
- password: `1qwe!QWE`

6.3.1 How to get the Linux Image

Step by Step

You can download the appropriate Linux image from SWS along with the Xpert system software.

NOTICE:

The Linux images are usually uploaded with major or fix releases. If you're installing a hotfix you must go to the download page of the fix release it's based on in order to get the appropriate Linux image.

6.3.2 How to create a bootable USB stick

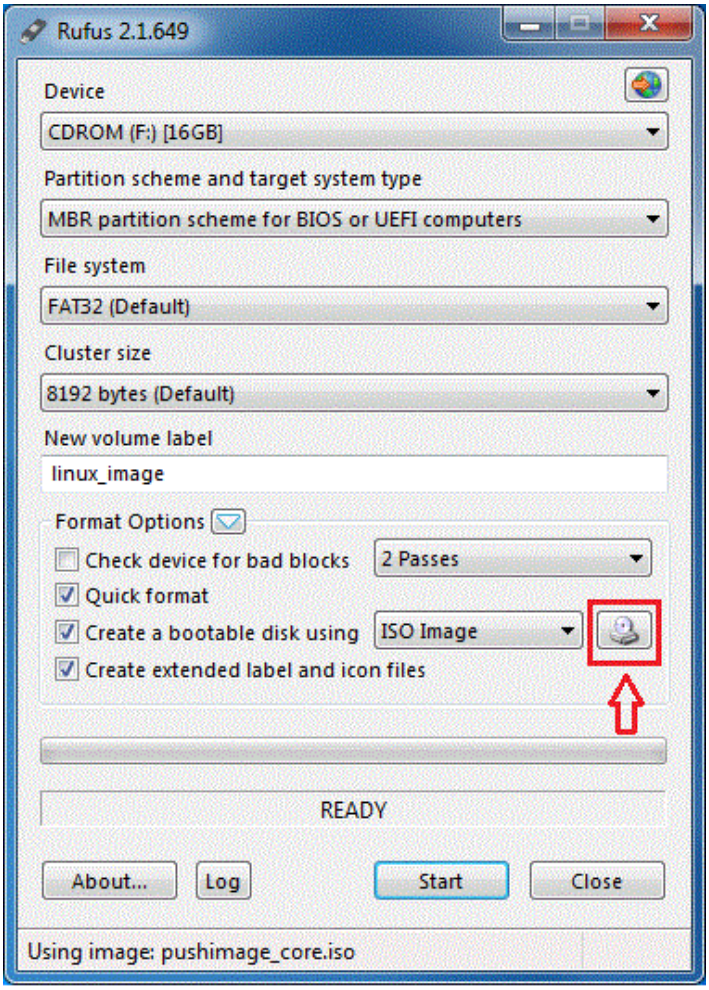
Prerequisites

- For a bootable USB stick the necessary files:
  - the appropriate official Linux image for OpenStage Xpert 6010p V1R0 (X18) or V1R1 (X50)(.img)
  - pushimage_core.iso file
  - Rufus bootable USB creator

Step by Step

1) Download Rufus from: https://rufus.ie/downloads/
2) Plug in a USB stick
3) Run `rufus, e.g. rufus-2.1.exe`

4) The window of Rufus will be displayed. Click on the **Select image** button under the **Format Options** section and browse for the `pushimage_core.iso` file.



5) Set the volume label and click on the **Start** button
6) When it is ready Rufus can be closed. Linux image (.img) for OpenStage Xpert 6010p V1R0 (X18) or V1R1 (X50) needs to be copied to the image folder of the USB stick. (Only 1 .img file can be in the image folder!)
7) It is possible to enable **LLDP-MED** during the installation, by creating an empty `lldp_enabled` file in the `config` directory of the USB stick.

6.3.3 How to install the image from USB stick

Prerequisites

A bootable USB stick containing the appropriate image for theOpenStage Xpert 6010p V1R0 (X18) or V1R1 (X50) has to be created.

Step by Step

1) Temporarily enable USB 2.0 controller (V1R0 (X18) only)

   It is an option to temporary enable USB 2.0 controller for OpenStage Xpert 6010p V1R0 (X18) to make the image installation faster. If you do not want

to enable USB 2.0, continue with the next step. With USB 2.0 enabled the process takes about 3 minutes while on USB 1.0 it can take up to 30 minutes. If you enable USB 2.0 before Linux image installation, you need to disable it after the installation process! If you want a faster installation process, please follow the steps below.

NOTICE:

Never disable the USB 2.0 controller on OpenStage Xpert V1R1 (X50), because it will disable all USB functionality!

---

a) After starting the device press the `Delete` key a few times until the BIOS appears.
b) Open S**outh Bridge Configuration** under the **Chipset** tab.
c) Select the **USB 2.0 Controller** element and enable it.
d) Then save the changes and restart the device.

2) Boot from the USB stick

a) When the device is starting press the F11 key until the **Please select boot device** selection window appears. Select the USB stick as boot device.
b) The OpenStage Xpert device will boot from the USB stick and the Linux image will be installed automatically.

NOTICE:

In case of OpenStage Xpert 6010p V1R1 (X50), you need to enter the following BIOS password : **afquo**

---

c) After the installation, please remove the USB stick and reboot the device.
d) If you have enabled USB 2.0 before installation, do not forget to disable the USB 2.0 controller in BIOS!

6.3.4 How to configure static IPv4 address

Prerequisites

By default the Linux turret is configured to use both IPv4 and IPv6 addesses assigned via DHCP, and network interface bonding. The turret can also apply network configuration (e.g. VLAN ID) from LLPD-MED traffic when using network interface bonding and DHCP. If static IPv4 address is required, please follow the steps below.

Step by Step

1) After starting the client the turret user will be logged in automatically.

2) Change to ttadmin user (ttadmin password can be found in .pwds file).

```
su ttadmin
```

3) Change to root (ttadmin password can be found in .pwds file).

```
sudo su
```

4) Edit the network configuration file for the `bond0` interface to use static IP:

```
nano /etc/systemd/network/60-bond0-settings.network
```

NOTICE:

The network configuration file for the `bond0` interface can be found at the following path: `/etc/systemd/network/60-bond0-settings.network`

5) Edit the `[Network]` section as displayed below:

```
[Network]
Address=<IPv4-address>/<CIDR-notation-of-mask>
Gateway=<IPv4-gateway>
DNS=<IPv4-DNS-nameserver-1>
DNS=<IPv4-DNS-nameserver-2>
Domains=<domain-1> <domain-2>
DHCP=ipv6
```

6) Restart networking using the following command:

```
systemctl restart systemd-networkd
```

IMPORTANT:

Starting with Debian 9 (Strech) the individual network interface names are different from previous versions of Debian. For OpenStage Xpert 6010p V1R0 (X18) the interface names are ens36 and enp1s3 and for OpenStage Xpert V1R1 (X50) the interface names are enp1s0 and enp4s0. Other off-the-shelf products may have different interface names.

6.3.5 How to Change Hostname

Step by Step

1) Edit the hostname file: `nano /etc/hostname`.
2) Change the localhost hostname in the `/etc/hosts` file also: `nano /etc/hosts`
   a) Edit the following line: `127.0.0.1 <new hostname>`
3) To make the change active please reboot the turret.
4) Check the hostname with the following command: `hostname`.

6.3.6 How to Install the OpenScape Xpert Client Software

Step by Step

There are the following ways to install OpenScape Xpert client software:

- With Central Image Distribution, using the Diagnosis Tool: Please see section How to Install the OpenScape Xpert Client Application.

- Automatic software update

6.3.7 How to Configure the X11 VNC Server on a Linux Client

Prerequisites

You can use X11 VNC server to establish graphical connections to an OpenScape Xpert Linux client. In this way you can interact with the client GUI remotely. The X11 VNC server is preinstalled on all OpenScape Xpert Linux clients but it is disabled by default.

Step by Step

1) Enable and configure VNC

a) On your PC start putty (http://www.putty.org) and enter the IP address of the Linux client into the **Host name (or IP address)** field on the **Category** - **Session** tab.

b) Change to the a **Category** – **Connection** – **SSH** – **Tunnels** tab and set the Source port to `5900` and the Destination to `<IP address of the client>:5900` and press **Add**.

c) Go back to **Category** - **Session** tab and press **Open**.

d) Login with `ttadmin` user and change to root user with the following command: `sudo su`

e) Start the VNC server with the following command: `x11vnc -auth guess -passwd <a-strong-password>`

2) The recommended VNC clients

Probably the X11 VNC server will work with any VNC client. However we recommend using one of the following clients:

a) RealVNC Viewer (https://www.realvnc.com/)

b) TightVNC (http://www.tightvnc.com/)

c) UltraVNC (http://www.uvnc.com/)

3) Disable VNC

Once the session is terminated the X11 VNC server stops automatically. If you need to connect again you have to re-enable it.

6.3.8 Custom firewall settings

The client uses nftables as firewall.

Nftables rules are divided into configuration files in `/etc/nftables.conf.d`.

If custom changes are required, it is suggested to use the `/etc/nftables.conf.d/custom.nft` configuration file where the user can add custom rules.

By default, connections via API interfaces are allowed.

NOTICE: After editing the configuration files, for the changes to be applied you must reload the nftables service: `systemctl reload nftables`

Disable the Thrift-based API if it is not in use:

Navigate to `/etc/nftables.conf.d/turret.nft` and comment out the following rules:

```
# tcp dport 9007 ct state new,established accept comment
"TurretAPI local"

# tcp sport 10052 ct state related,established accept
comment "TurretAPI remote"

# tcp sport 9007 accept comment "TurretAPI local"

# tcp dport 10052 accept comment "TurretAPI remote"
```

Disable the CTI port if it is not used:

Navigate to `/etc/nftables.conf.d/turret.nft` and comment out the following rules:

```
# tcp dport 9000 ct state new,established accept comment
"CTI"

# tcp sport 9000 ct state related,established accept
comment "CTI"
```

How to Configure Custom CTI Port

In the System Manager Admin you can change the CTI application port from the default 9000 to any desired <Application Port> value.

To use this port on the turrets you need to change the port in the Linux firewall as well.

Step by Step

1) In `/etc/nftables.conf.d/turret.nft`, edit the **Input** rule as follows:

   Change

   ```
   tcp dport 9000 ct state new,established accept comment
   "CTI"
   ```

   to

   ```
   tcp dport <Application Port> ct state new,established
   accept comment "CTI"
   ```

2) In `/etc/nftables.conf.d/turret.nft`, edit the **Output** rule as follows:

   Change

   ```
   tcp sport 9000 ct state related,established accept
   comment "CTI"
   ```

   to

   ```
   tcp sport <Application Port> ct state
   related,established accept comment "CTI"
   ```

6.3.9 How to configure static IPv6 address

The IP Addressing Modes described in chapters 3.1.2.6 - 3.1.2.12 are valid for OpenScape Xpert components including Turrets

Prerequisites

By default, the Linux turret is configured to use both IPv4 and IPv6 addresses assigned via DHCP, and network interface bonding. The turret can also apply network configuration (e.g. VLAN ID) from LLDP-MED traffic when using network interface bonding and DHCP. If static IPv6 address is required, please follow the steps below.

Step by Step

1) After starting the client, the turret user will be logged in automatically.
2) Change to ttadmin user (ttadmin password can be found in passwords file):
   `su ttadmin`
3) Change to root (ttadmin password can be found in passwords file: `sudo su`
4) Edit the network configuration file for the `bond0` interface to use static IP:
   `nano /etc/systemd/network/60-bond0-settings.network`

   NOTICE:

   The network configuration file for the `bond0` interface can be found at the following path:
   `/etc/systemd/network/60-bond0-settings.network`

5) Edit the `[Network]` section as displayed below:

```
[Network]
Address=<IPv6-address>/<CIDR-notation-of-netmask>
Gateway=<IPv6-gateway>
DNS=<IPv6-DNS-nameserver-1>
DNS=<IPv6-DNS-nameserver-2>
Domains=<domain-1> <domain-2>
DHCP=ipv4
```

6) Restart networking using the following command:
   `systemctl restart systemd-networkd`

   IMPORTANT:

   Starting with Debian 9 (Strech) the individual network interface names are different from previous verions of Debian. For OpenStage Xpert 6010p V1R0 (X18) the interface names are ens36 and enp1s3 and for OpenStage Xpert V1R1 (X50) the interface names are enp1s0 and enp4s0. Other off-the-shelf products may have different interface names.

6.4 Audio Best Practice

This section describes how to configure the audio settings in order to provide the best audio performance on the client devices.

Overview

The audio analysis detailed in this section was commissioned by Unify to verify changes made to the turret's acoustic parameters and collect information concerning the ambient acoustic environment, review the various hardware and software configurations used by the Traders, observe how the Traders are using the technology and collect firsthand information about the type and nature of problems being experienced.

The objective of this section is:

- to make recommendations to the project team how to optimize the configuration for optimal acoustic performance and
- to identify any malfunction which negatively impacts acoustic performance and put in place a corrective action plan.

Correct Installation of Speaker Module (s) and/or Microphone

Please verify the correct installation of the OpenScape Xpert client device and connected equipment as described in the OpenStage Xpert First Installation guide which is delivered with the hardware (Order No. A31003-X2040-J100-X-7631).

- If two speaker modules are connected to the same PC-client/OpenStage Xpert 6010 only one speaker module can have a microphone connected.
- If two speaker modules are connected to one PC-client or OpenStage Xpert 6010 and one of the speaker modules has a microphone connected, the two speaker modules must be interconnected via the RJ45 jack (INT) of the modules. For this connection a standard CAT5e 1:1 patch cable must be used. The cable must not be longer than 2 meters or 6.5 feet. No other device may be connected.
- There is an additional USB-A host port (USB 3) on the speaker module. It serves for the LED control of a supported Gooseneck microphone. No other device may be connected to this port.
- For the analogue microphone signal there is an RJ10 jack (MIC) on the speaker module. Only a supported Gooseneck microphone may be connected.
- For optimal acoustic performance it is recommended to connect an external microphone rather to the Speaker Module than to the turret itself. Please note that moving the microphone from the turret to the Speaker Module causes configuration changes via the System Manager. Justification:
  - The hardware echo canceller in the Speaker Module offers better performance.
  - Less demands upon the performance of the Turret.
  - Unused speech devices can be disabled. Disabling a speech device will improve the performance of the Turret.
- The USB cable of the Gooseneck microphone is for the LED indicator control only; separate audio connector is used to the microphone port.

6.4.1 How to Set the SPM Channel Volume

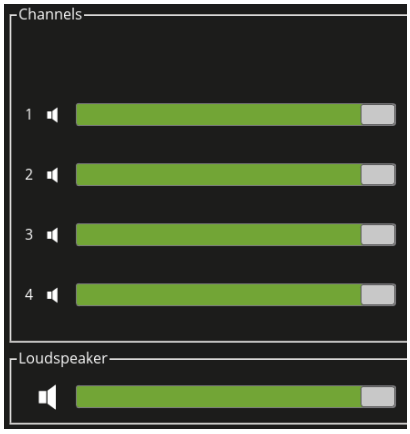
Proceed as follows to reconfigure the SPM channel's volume settings. The volume sliders should be on the maximum position if a speaker module is connected.

Prerequisites

The client device has added Speaker Module(s).

Step by Step

1) De-assign the Speaker Module from the client device.
2) Click **Menu** -> **Common Functions** -> **SPM properties** to open the SPM P roperties dialog.
3) Set the volume of the channels and the loudspeaker to maximum and press OK.



4) Re-assign the Speaker Module again.

The channel volume slides should be on maximum.

6.4.2 How to Configure Normalization Settings

Proceed as follows to configure the normalization settings for SPM. The normalization function should be disabled if a speaker module is connected.

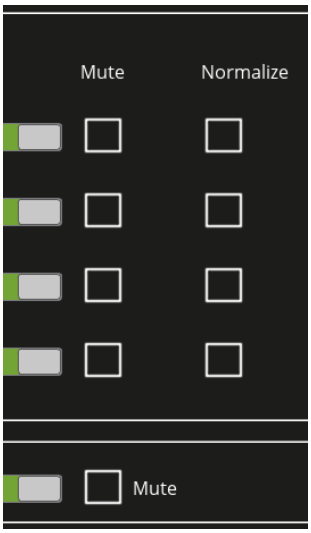
Prerequisites

The client device is connected to a Speaker Module and normalization is enabled for all SPM channels.

Step by Step

1) Click **Menu** -> **Common Functions** -> **SPM Properties** to open the SPM Properties dialog.

2) Deselect the **Normalize** check boxes and click **OK**.



3) Normalization can be switched on when the sources have too different volume levels, which can not be compensated using the volume adjusters on the Speaker Module.

By default normalization should be OFF and only activated if a problem with uneven volume levels arises.

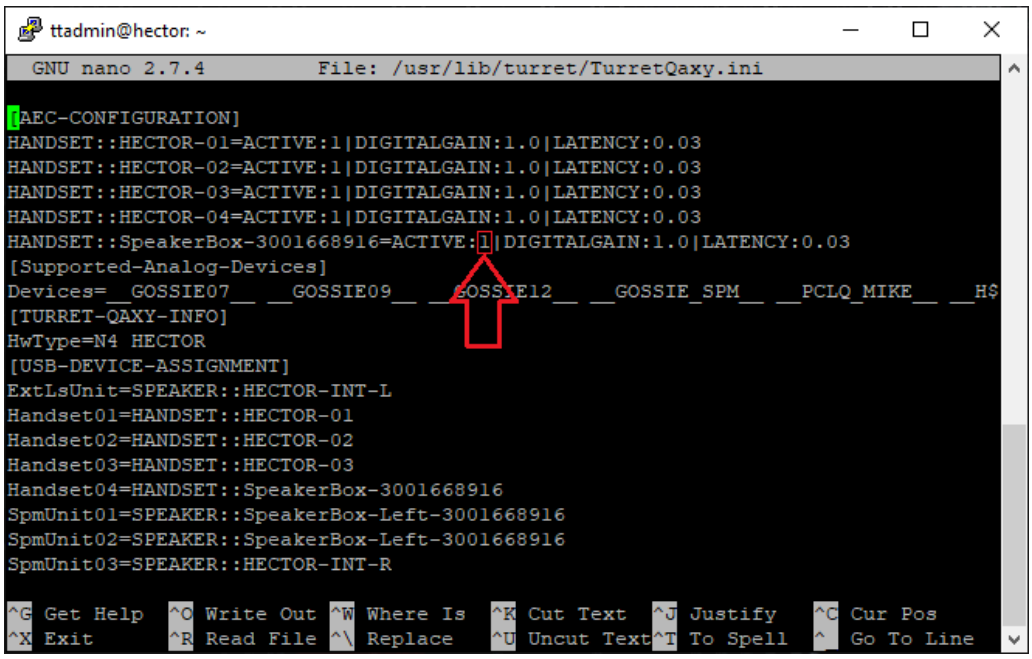
6.4.3 How to Verify Echo Cancelation Settings

Proceed as follows to verify that echo cancellation is enabled on the OpenScape Xpert Client device in the TurretQaxy.ini file.

Step by Step

1) Open the TurretQaxy.ini file with a text editor (Linux turret: nano, Windows soft client: Notepad).

2) Verify that echo cancellation is enabled (ACTIVE:1) as shown in the figure below.



3) Reconfigure the OpenScape Xpert Clients if necessary.

6.5 Active Directory Authentication for the Clients

The System Manager can be configured to authenticate Turret users with their Active Directory username and password, instead of their profile password. With Active Directory authentication configured, the System Manager can check for profiles with the same name as the AD user name, and authenticate with its AD password against the AD.

It is possible to specify a default domain for the authentication.

- For users in the default domain, the domain name can be omitted from both the login name and profile name.
- If the user is not in the default domain, the full username@domain format can be used for both login name and profile name.

6.5.1 How to Configure Active Directory Authentication for the Clients

Prerequisites

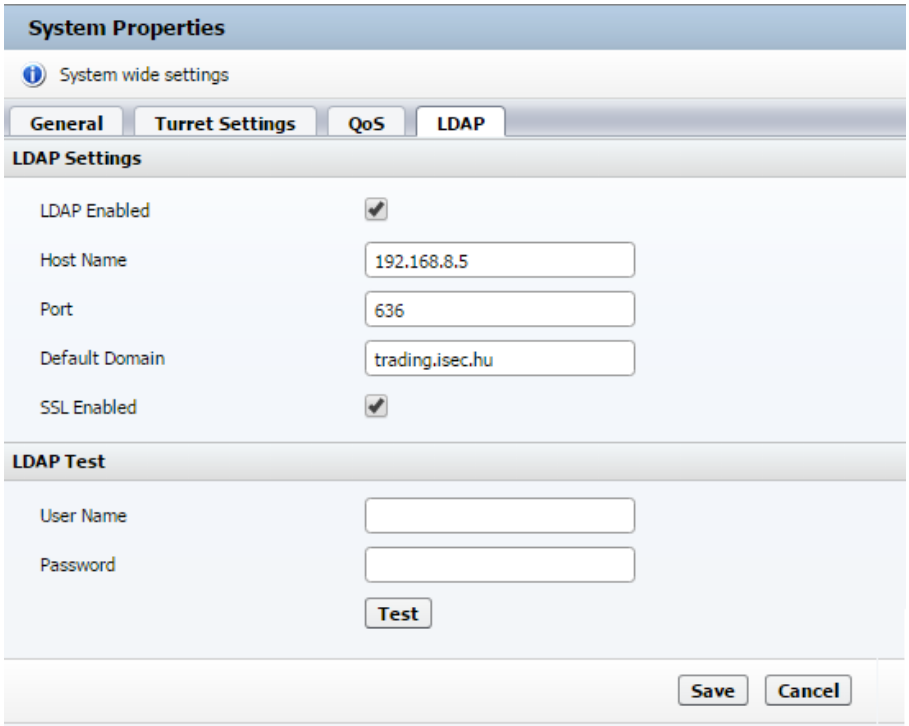
OpenScape Xpert System Manager is installed.

Supported operating systems for the Domain Controller are Windows Server 2008 R2 and up.

For SSL secured authentication, TLS1.2 protocol must be enabled in the Domain Controller.

Step by Step

1) Click **System Properties** on the OpenScape Xpert Management Portal. The **System Properties** dialog appears.
2) Select the **LDAP** tab containing all fields for the LDAP configuration.



3) Enter/select the settings in LDAP settings area:
   - Check the **LDAP Enabled** checkbox.
   - **Host Name**: The name or IP address of the Domain Controller. Cannot be empty if the LDAP Enabled checkbox is checked.
   - **Port**: The port of the Domain Controller that is connected to. Default is 389 for non-SSL, and 636 for SSL connection. Accepted values are 1-65535.
   - **Default Domain**: Optional. If the username to be authenticated does not contain the @domain part, the default domain is used during authentication.
   - **SSL enabled**: check to use SSL during authentication, uncheck otherwise. A certificate must be installed, see chapter 4.7.7.5 How to Prepare for using Secure LDAP Connection on page 68.
4) Optional: Test the connection:
   a) In the **LDAP test** area, enter a valid Active Directory username and password. Note that if the user is not in the default domain or default domain is not entered, then the full username@domainname format must be used.
   b) Press the **Test** button.
   c) The System Manager tries to authenticate the username and password with the currently provided settings. A message box pops up with the authentication result.

   This result can be one of the following:

   - Authentication successful,

- Invalid credentials (connection is OK, but username or password is invalid),
- Could not connect to host,
- LDAP configuration error with OpenLDAP error code.

5) Click **Save** to confirm your settings.

6.6 OpenStage Xpert V1R1 (X50) - Overview

This chapter is about to describe the special features and capabilities of the OpenStage Xpert 6010p V1R1 (also referenced to as N5 or X50) device.

6.6.1 OpenStage Xpert 6010p V1R1 Analog Audio

The OpenStage Xpert 6010p V1R1 device holds 5 USB audio chips, just like the N4, but uses a different audio topology:

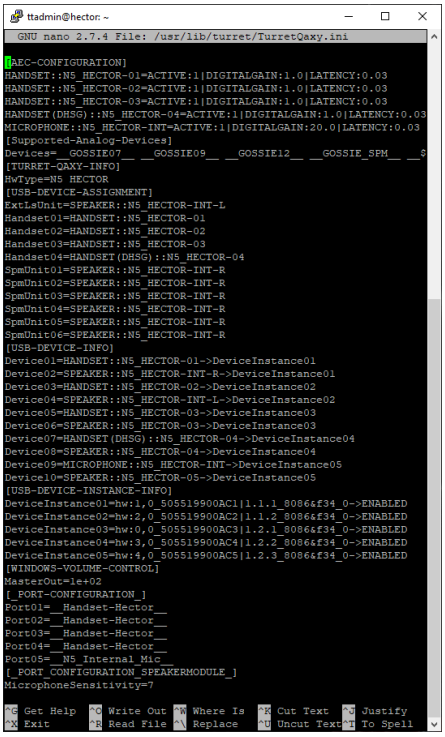
- USB device 1 → Handset 1 AND Internal right loudspeaker
- USB device 2 → Handset 2 AND Internal left loudspeaker
- USB device 3 → Handset 3 AND external loudspeaker (jack plug on the bottom)
- USB device 4 → Handset 4 AND external loudspeaker (jack plug on the bottom)
- USB device 5 → Internal microphone AND external loudspeaker (jack plug on the bottom)

The main differences from OpenStage Xpert 6010p V1R0 (X18):

- The 5th device handles an internal microphone, which is not present in the OpenStage Xpert 6010p V1R0 (X18).
- The 4th handset plug is a combined 4p/8p connector. It enables to connect a normal handset/gossie etc, or to connect a DHSG capable headset as well.

So from TT SW point of view the OpenStage Xpert 6010p V1R1 offers 5 speech units, and 5 speakers. From the 5 speech units only 4 can be used at the same time, the device assignment will configure which 4 to use.

All the device instances and devices in the `TurretQaxy.ini` are listed in the same logic as in the earlier version of OSX. The default assignment is as: (the internal microphone is not used by default, but can be enabled by reconfiguring the device assignment).



From the handset hook/mute features point of view there is no differences from the OpenStage Xpert 6010p V1R0.

6.6.2 The Internal Microphone

The OpenStage Xpert 6010p V1R1 internal microphone is a standalone microphone that is built into the body of the OpenStage Xpert 6010p V1R1.

It has a LED which can light up when the microphone is active.

To be able to activate the microphone it has to be enabled manually in the TurretQuaxy.ini for one chosen Handset (MICROPHONE::N5_HECTOR-INT) and that handset must be configured as "Microphone without a speaker" in the OpenScape Xpert Management Portal.

When a call is established on the speech unit on which the internal microphone is configured the microphone will become active and its LED will lit.

On mute and on disconnect the internal microphone and its LED will turn off.

Only one microphone can be active at a time. Two active microphones e. g. internal microphone + Gossie09 are not supported.

6.6.3 DSHG Interface

The OpenStage Xpert 6010p V1R1 device is equipped with a standard DHSG capable interface. The 4th handset plug is a combined connector: you can connect the normal handset/microphones just like to the other 3 plugs, but you can also connect a DHSG device’s (base station) AUX cable - which is a 8pole RJ jack.

In the case the user wants to use a supported wireless headset, connect the base station to the port 4 via the AUX cable of the base station.

To configure the wireless headset, the followings have to be done:

- In the `TurretQaxy.ini`: in the “device assignment” section configure the device to the desired speech unit.
- In the SM: according to the configuration in the TurretQaxy.ini, set the speech unit type to “Headset” and set it as “With cradle”.

Having a DHSG capable device connected and configured to the Turret, you can answer, disconnect calls (according to the configured speech unit) via the wireless earpiece and/or base station just like by desk phones. The ringer of the wireless device (base station and earpiece) is synchronized with the Turret internal ringer (just the normal ringer) – but all wireless devices have their own ringtones audible on the base station and in the earpiece.

6.6.3.1 DHSG Headset Usage

The behavior of the wireless headset device can be imagined well compared to the behavior of the handset devices with cradle.

For example when the handset is on-hook (so it is on the cradle) and the user answers a call with the Turret GUI, the call can be heard from the open-listening speaker and not from the handset, because the handset is on the cradle. But the user can switch to using the handset by lifting up the handset from the cradle, making the handset off-hook. That model is applied to the wireless headset with a subtle difference.

Since the user must be able to answer and disconnect the calls from a distance (wireless setup) the software does not bind the on and off-hook states to the physical connection of the headset and the cradle. That way the user can answer and disconnect calls with the built-in button on the headset, but that also drives the switching mechanism between the headsets own on and off-hook states. So instead of monitoring the headsets physical location/position, the user must monitor the corresponding Turret GUI speech unit icon to get the state of the headset (is it on or off-hook).

Icon	State
	On-hook state, the headset is not active.
	Off-hook state, the headset is active.

6.6.3.2 DHSG Supported JABRA Wireless Devices

Required settings

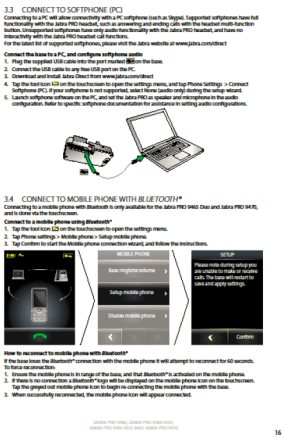
- The devices must be connected as Desk phone with Jabra LINK adapter.

- DHSG adapter type (remote call control mode) must be set up.
- Open phone line when headset is undocked setting must be On.
- Recommended Clear dial tone switch setting is setting ‘A’.

For further details on how to set these settings for the supported devices see their corresponding user manuals.

JABRA PRO 9470

Supported JABRA device firmware versions are 3.15.2 and 3.13.2.



3.3 CONNECT TO SOFTPHONE (PC)

Connecting to a PC will allow connectivity with a PC softphone (such as Skype). Supported softphones have full functionality with the Jabra PRO headset, such as answering and ending calls with the headset multi-function button. Unsupported softphones have only audio functionality with the Jabra PRO headset, and have no connectivity with the Jabra PRO headset call functions.

For the latest list of supported softphones, please visit the Jabra website at www.jabra.com/direct

Connect the base to a PC, and configure softphone audio

1. Plug the supplied USB cable into the port marked on the base.
2. Connect the USB cable to any free USB port on the PC.
3. Download and install Jabra Direct from www.jabra.com/direct
4. Tap the tool icon on the touchscreen to open the settings menu, and tap Phone Settings > Connect Softphone (PC). If your softphone is not supported, select None (audio only) during the setup wizard.
5. Launch softphone software on the PC, and set the Jabra PRO as speaker and microphone in the audio configuration. Refer to specific softphone documentation for assistance in setting audio configurations.

3.4 CONNECT TO MOBILE PHONE WITH *BLUETOOTH*®

Connecting to a mobile phone with Bluetooth is only available for the Jabra PRO 9465 Duo and Jabra PRO 9470, and is done via the touchscreen.

Connect to a mobile phone using Bluetooth®

1. Tap the tool icon on the touchscreen to open the settings menu.
2. Tap Phone settings > Mobile phone > Setup mobile phone.
3. Tap Confirm to start the Mobile phone connection wizard, and follow the instructions.

How to reconnect to mobile phone with Bluetooth®

If the base loses the Bluetooth® connection with the mobile phone it will attempt to reconnect for 60 seconds.

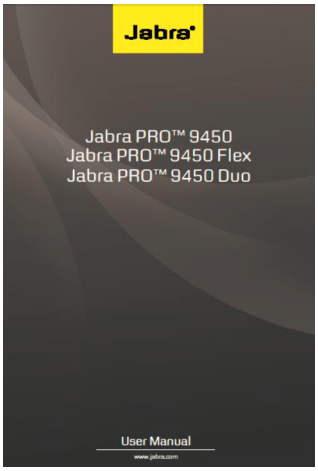
To force reconnection:

1. Ensure the mobile phone is in range of the base, and that Bluetooth® is activated on the mobile phone.
2. If there is no connection a Bluetooth® logo will be displayed on the mobile phone icon on the first Screen. Tap the greyed out mobile phone icon to begin re-connecting the mobile phone with the base.
3. When successfully reconnected, the mobile phone icon will appear connected.

16

JABRA PRO 9450

Supported JABRA device firmware versions are 3.15.2 and 3.13.2.



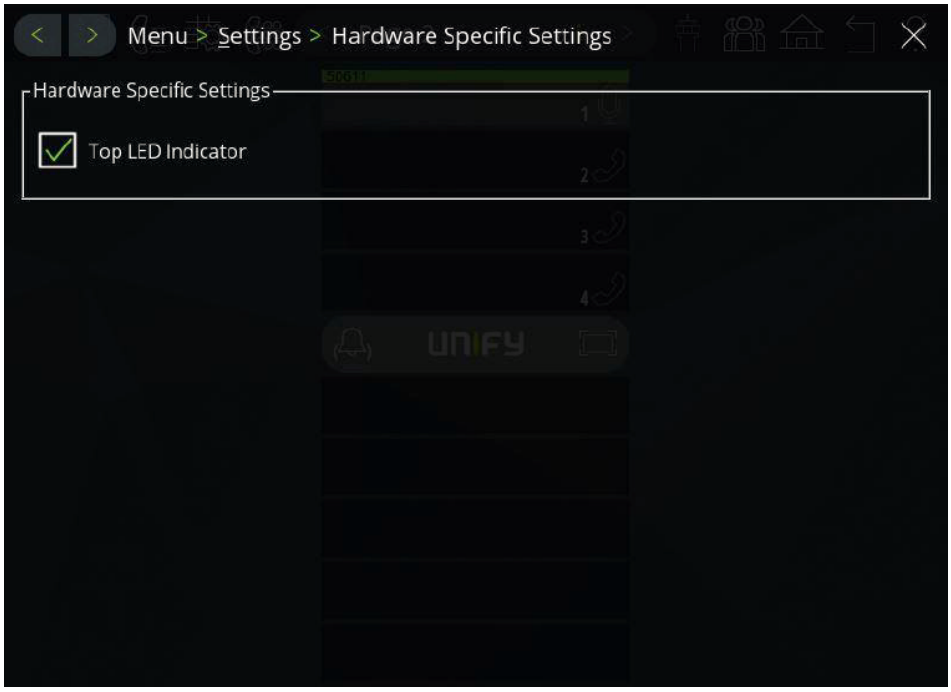
Alternative solution for setting up numerous devices

- Install Jabra Direct PC Suite
- Connect the device through USB
- Select the connected device in the Jabra Direct software
- Load device settings from the `configurator .xml` file (under the **Options** menu).

6.6.4 Top LED Indicator

The OpenStage Xpert 6010p V1R1 has a LED on the top right corner which is used to provide visual signalization for various types of calls. In the following these will be detailed.

The signalization can be switched on and off in the menu of the OSX Client which is in the **Menu -> Settings -> Hardware Specific Settings**:



This setting is only visible when the OSX Client is running on an OpenStage Xpert 6010p V1R1 otherwise the setting is hidden.

The setting is on/active by default.

Incoming call that is displayed in the call queue:

In case of an incoming call that is displayed in the call queue the LED is blinking with normal speed in turquoise color.

Incoming call that is not displayed in the call queue:

If the incoming call is not shown in the call queue (call queue is full or “Display in Call Queue” is switched off in the linekey) the LED will still be off until an active / basic call is created.

Active / basic call:

When an active / basic call exists the led will continuously lit with green color.

- Seized line:

  When a line has been seized the LED continuously lit with green color.
- Outgoing call during ringback tone:

  During ringback tone the LED is continuously lit with green color.

Intercom call:

In case of an intercom call the LED is blinking fast with red color.

Priorities:

In case of more types of calls there is a priority list that defines how the led behaves.

Priority list:

1) Intercom call
2) Incoming call
3) Active call

If more calls exist and a higher priority call ends the led will switch to the indication of a call that is under the higher priority call.

7 Diagnosis Tool — Overview

This chapter describes the Diagnosis and Offline Update tool providing a more convenient way for service technicians to analyze and update OpenScape Xpert components remotely and centralized.

Functional Overview

The main purposes of this tool are:

- Collecting log and dump files of OpenScape Xpert components (Linux based Turret and MLC).

  NOTICE:

  Beginning with V6 the log and dump download and logging settings can not be done for the SM through the Diagnosis tool.

- Remote administration of this components.
- Offline updating the OpenStage 6010p devices.

With this tool these tasks can be done remotely on any PC that is in the same network as the components to be analyzed.

Prerequisites

- ".Net 4.6.1" or later is necessary for the operation of the Diagnosis Tool.

7.1 How to Initially Define Password and Export Path

It is necessary to initially enter connection information before the tool can detect devices in the network. The default export folder can be changed.

Step by Step

1) To open the **Options** dialog, select **Tools** -> **Options**.

   The Options dialog appears.

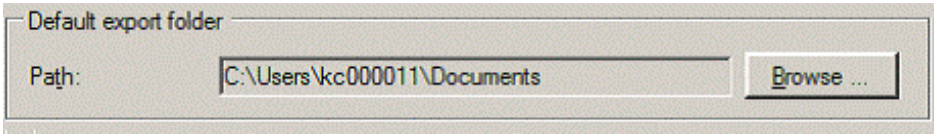
2) Enter the username and password in the respective fields.

3) Check the Store Passwords field to store the password on the computer.

   NOTICE:

   If the Store Passwords is checked, the program will save the password. Please keep in mind that passwords are not stored securely, so use this feature only on trusted machines.

4) By default the export folder points to the user's documents. To change the path, click the **Browse** button and select the new folder.



5) To return to the main window click **OK**.

The **Options** dialog disappears.

7.2 How to Search Devices in the Network according to IP Range

Because the network in which the Diagnosis Tool resides can be quite large, it is possible to enter an IP range for search purpose.

Prerequisites

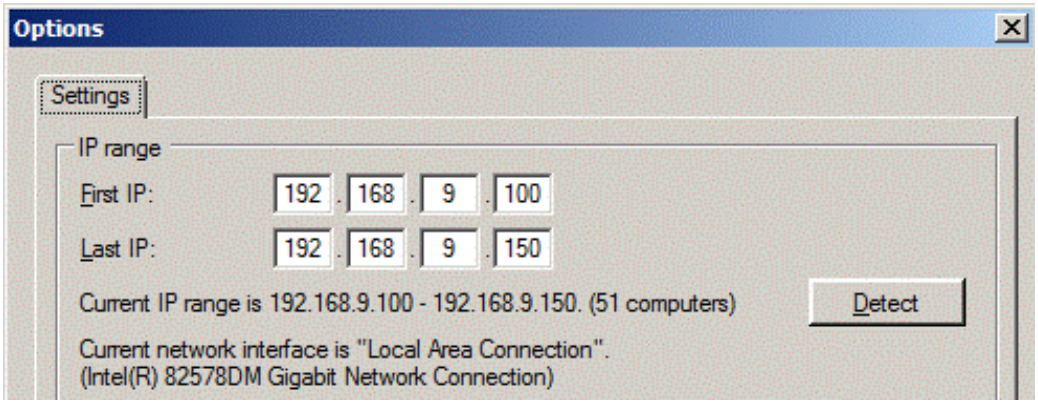
The user name and password for the communication with the MLC and Linux client have been entered.

Step by Step

1) To open the **Options** dialog, select **Tools** -> **Options**.

   The Options dialog appears.

2) By default the range of the network is detected automatically. To manually detect the network's IP range, click the **Detect** button.



   The IP range and the total number of computers are displayed.

3) Enter a custom IP range in the **First IP** and **Last IP** fields and click **Detect**.

   NOTICE:

   The detected IP range contains all the existing IP addresses in the network. Entering values beyond that range will result in unnecessary long waiting times.

4) To return to the main window click **OK**.

   The **Options** dialog disappears.

5) Click the **Update List** button in the main window.

6) To stop the search process manually click the **Stop** button.

As a result the connected devices in the network are displayed in the main window. The tool's search process works as described below:

The program pings a given IP. If this is not successful, the process aborts and the program proceeds to the next IP in the range.

If the pinging was successful the program looks for shares on the target device. Based on existing share names it checks if the device is a Turret.

7.3 How to Export Log and Dump Files

The export process can be started manually or scheduled after a search has been finished or stopped by the user.

Step by Step

To manually export the zip file containing the log files and dump files, select the desired computers in the list and proceed as follows:

- Click the **Export Selected** button or
- select the **Log files** -> **Export Selected** command.
- To export the files of all computers displayed, select the **Log files** -> **Export All** command.

The zip file(s) is (are) stored in the folder specified in the **Options** menu. The name of the zip file is the date and time of the exporting process that created it. The contents of the zip file are a text file, with information about the export, and some folders. Each computer's log and dump files are placed in a separate directory. The names of these directories contain the host names of each computer.

7.4 How to Filter OpenScape Xpert Software

The result of the search can contain too many components to handle easily. This problem can be solved by the filter function. The filter applies case insensitively for all columns of the component list which can contain MLCs and Clients at the same time. The criteria selection also works on all rows.

Step by Step

1) By default the service is ready to use and filters by **Name** and **IP** address.

2) Everything is visible when nothing is selected to filter by, or the search bar is empty.

3) Specify the preferred criteria by clicking **Search in...**.and checking the choices that you want to search in.

4) Start typing what you are looking for.

NOTICE:

The filter does not utilize regular expressions, but it c an find case insensitively any entries containing the entered text as sub-string.

The component list can be filtered by:

- – **Name**
  – **IP**
  – **Type**
  – **Trading Name**
  – **Version**
  – **Database Server** (address)
  – **Operating System**
  – **Kernel Version**

  and any combination of these.

NOTICE:

The components can also be ordered by the columns as well by clicking on any of the header names.

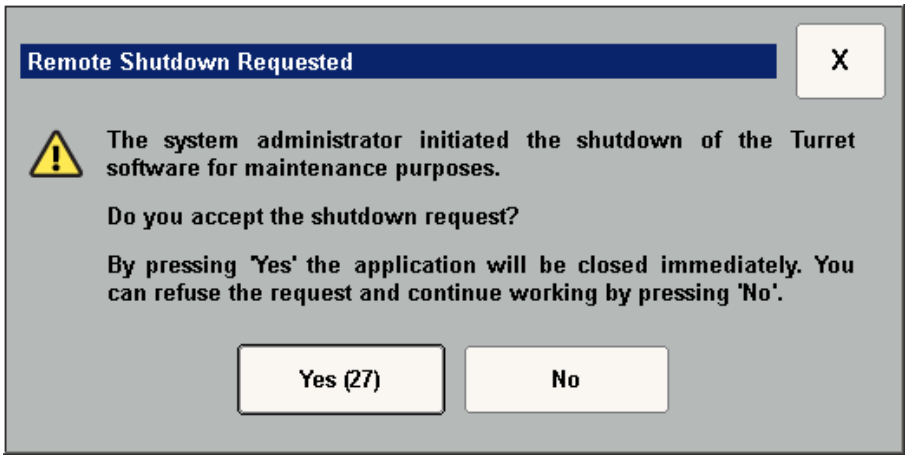
7.5 How to Remotely Restart OpenScape Xpert Clients

Proceed as follows to remotely restart turrets for maintenance purposes.

Step by Step

1) Select one or more devices of the same type.
2) Right click on the selected device.
3) Restart the OpenScape Xpert Client Device.

4) If the Turret software is running at the moment, a warning dialog appears which informs the user about the remotely initiated shutdown.



The user can either accept or refuse this request. By pressing ‘Yes’ button on the dialog, or by pressing the RETURN (ENTER) key on the keyboard, the request will be accepted, and the Turret software will shut down. By pressing ‘No’ button on the dialog, or by pressing the ESCAPE key on the keyboard, or by pressing the ‘X’ in the top right corner, the request will be refused, and the user can continue using the Turret software. On the ‘Yes’ button, there is a counter, which counts down in every second, started from 30. If this counter reaches zero, the button will be pressed automatically, so if the user doesn’t press any buttons or keys listed above for up to 30 seconds, the Turret software will shut down.

7.6 Logging Settings

This section describes the feature logging of the Diagnosis and Updater tool.

Overview

The program can be used to modify the logging settings of OpenScape Xpert components. It uses SSH access for Linux clients.

The list of LCP files on Different Components

Data logging is done via lcp files where the logger settings are stored.

- Turret
  - TurretIp_logger_settings.lcp
  - TurretQaxy_logger_settings.lcp
  - TurretLauncher_logger_settings.lcp
  - TurretUpdaterService_logger_settings.lcp

- MLC
  - mlccp_logger_settings.lcp
  - mixerApplication_logger_settings.lcp

NOTICE:

TurretUpdaterService_logger_settings.lcp file is available on Windows soft clients only.

NOTICE:

Logging settings must not be changed for mixed (Windows and Linux) clients at the same time because of lcp file content differences.

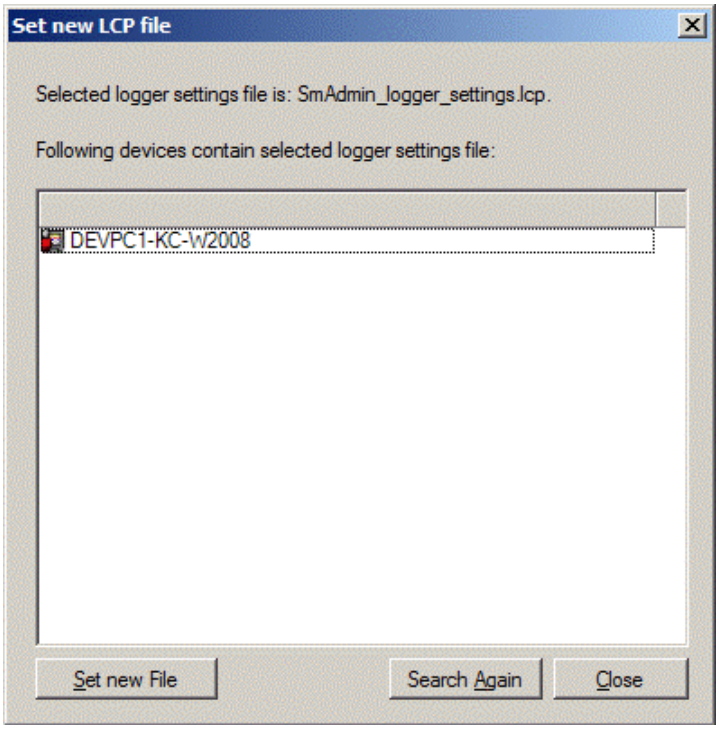
7.6.1 How to Define New Settings

Proceed as follows to define new logger settings on the desired components.

Step by Step

1) Select the devices to be modified in the main window list view.
2) Go to the **Tools** menu and press **Set new Logger settings file on selected** button.
3) In the opening window, search for the LCP file to be uploaded to the selected computers.

   After this a window appears that contains those devices that have the selected LCP file present because logger settings can only be overwritten.



4) The following options appear:
   - Refresh the list by clicking the **Search Again** button.
   - To finalize the process click the **Set new File** button.

After this the new LCP file will be copied to the selected devices and a backup file is also created on each, in case the user wants to roll back changes

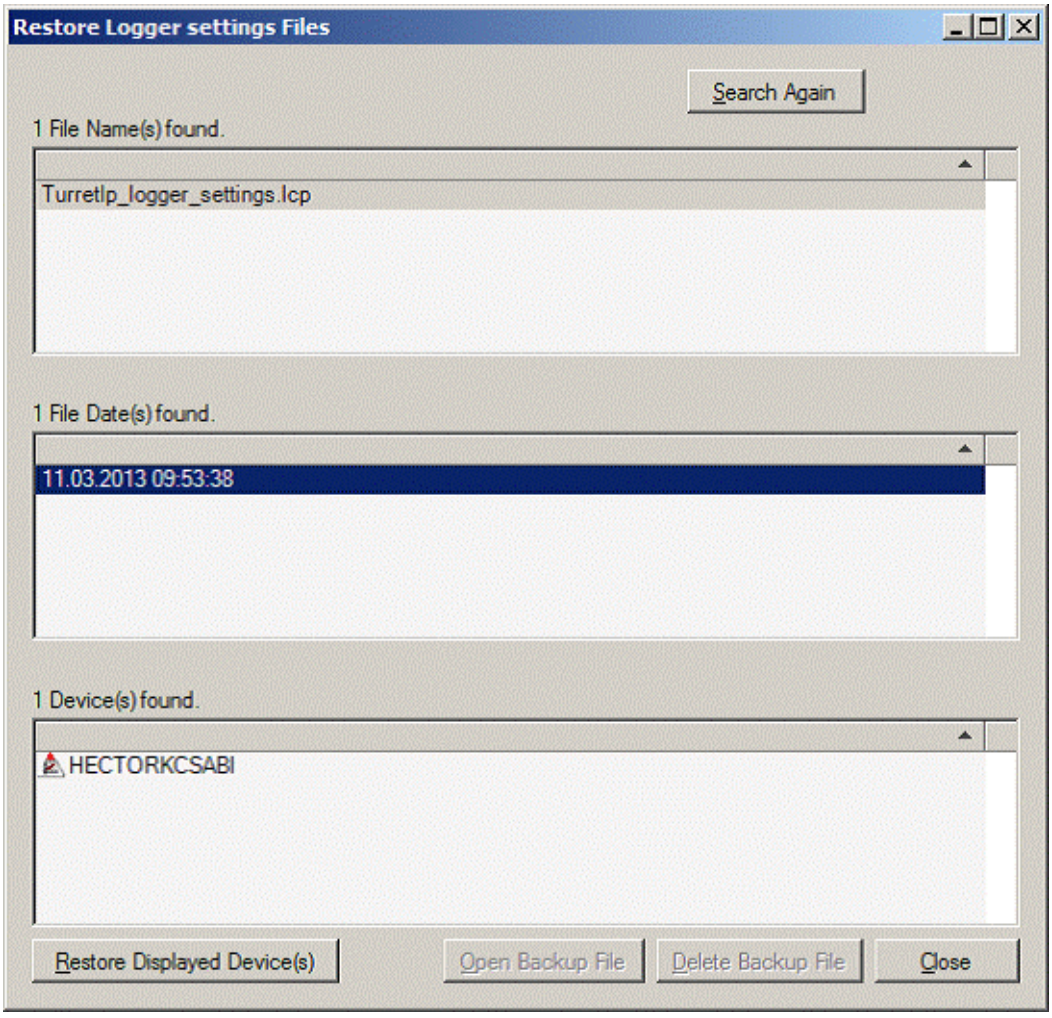
7.6.2 How to Restore Logging Settings

Proceed as follows to restore logging settings on the desired components.

Step by Step

1) Select the devices to be restored in the main window list view.
2) Go to the **Tools** menu and press **Restore Logger settings file on selected** button.

   The **Restore Logger settings Files** dialog appears.



This window has three lists. The upper one shows the different kinds of backed up LCP files found on the previously selected devices. I

3) The following options appear:

- f you select an LCP file, the middle list will contain dates on which backup files were created from that kind of LCP.
- Finally, selecting a date will show the list of devices in the bottom list, on which backed up LCPs are present with the given date.
- The restore process can only target dates. If you click on a single device, the corresponding backup LCP file can be opened, edited or deleted using the **Open Backup File** or **Delete Backup File** button respectively.

4) To restore the displayed devices, click the **Restore Displayed Devices** button.

7.7 Security Updates on Linux OpenStage Xpert Clients

Security updates can be installed via deploying a new OpenStage Xpert Client image which incorporates the fixes. Unify releases regularly updated OpenStage Xpert Client images.

7.8 Central Image Distribution

This section describes the backup and restore process of images as well as the installation of a fresh Linux image on OpenStage Xpert 6010p devices using the OpenScape Xpert Diagnosis Tool. 1st you should create a file server (referenced as backup server) where you can store the factory Linux image and the backups of Windows and Linux images of the OpenStage Xpert 6010p clients for restoring them at any time.

For the backup server you should use a Debian Linux server (all steps were validated with Debian). Due to the high disk space, network traffic and CPU permanence requirements using a live MLC as a backup server is not supported. Always use a separate Debian server for this purpose!

7.8.1 How to Create a User for Central Image Distribution.

Prerequisites

You can create a separate user for writing and reading the images (optional, just for security resons). The `/home/<username>/imbackups` folder will be the place where backups are going to be stored.

Step by Step

1) Add the user by entering: `adduser backupuser`

2) When requested enter a new password for the user, then repeat is

3) Enter the full name of the user (e.g. `Backup User`)

4) Finish the operation by pressing the `y` key.

7.8.2 How to Enable SSH Login for the Central Image Distribution User

Prerequisites

You have to create a separate user for handling the image backups as described in the previous section.

Step by Step

1) Open the sshd_config file for editing by entering: `nano /etc/ssh/sshd_config`
2) Scroll down until the following line: AllowGroups
3) Add the backupuser group as allowed group: `AllowGroups backupuser`
4) Hit `Ctrl + X` on your keyboard to exit nano and hit `Y` to save the changes.
5) Restart the SSH service with: `/etc/init.d/ssh restart`

7.8.3 How to Install Packages on the Backup Server for Central Image Distribution

Prerequisites

Before you begin make sure that the public repositiries /etc/apt/sources.list file are configured correctly. These are needed for the installation of the following packages.

Step by Step

1) Update the packages list: `apt-get update`
2) Install OpenSSL server: `apt-get install openssl`
3) Check whether the dd tool is available: `dd --version`

7.8.4 How to Create SSH Certificate for Central Image Distribution

Step by Step

1) Login with the newly created user.

2) Enter the following commands (leave passphrase empty):

```
backupuser@backupserver: ~$ ssh-keygen -m PEM -t rsa -b
4096

Generating public/private rsa key pair.

Enter file in which to save the key (/home/
backupuser/.ssh/id_rsa):

Created directory '/home/backupuser/.ssh'.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/
backupuser/.ssh/id_rsa.

Your public key has been saved in /home/backupuser/.ssh/
id_rsa.pub.

The key fingerprint is:

5a:8d:93:30:a9:5a:f3:6a:67:d1:28:ef:ee:11:b5:a8
backupuser@backupserver

The key's randomart image is:

+--[ RSA 2048]----+

| |

| . |

| + . |

| . = = |

| + ooS . |

| o.+o+.. |

| . Eo+. |

| ..+. |

| ..*+ |

+-----------------+

backupuser@ ImageServer:~$
```

3) Create an empty authorized_keys file in the .ssh folder and add the public key to the authorized_keys file:

```
cd /home/backupuser/.ssh

cat id_rsa.pub > authorized_keys
```

7.8.5 How to Configure Diagnosis Tool for Central Image Distribution

Step by Step

1) Copy the private key (filename: `id_rsa`) to a drive, which is available for the Diagnosis Tool.

2) Open **Options** under the **Tools** menu and configure the **Backup Server** settings.
   a) Enter the backup server's IP address.
   b) Enter the user name (`backupuser`).
   c) Browse for the `id_rsa` private key file.
3) Under the **Passwords** section in the **Linux Turret's** field enter the user `ttinstall` and the password `trading`.

   This is necessary for finding the Linux client in Diagnosis Tool and to install the Turret Debian package).

7.8.6 How to Create a Backup Folder for Central Image Distribution

Step by Step

1) Log in to the backup server with the backupuser user
2) Create a folder with the name `imbackups` in the user `home` directory: `mkdir imbackups`
3) Set the folder right so the Diagnosis Tool can read it: `chmod 766 imbackups`

7.8.7 How to Prepare the Linux Image for Central Image Distribution

Step by Step

Copy the Linux image for all devices (OpenStage Xpert N4 / N5, Incotel) to the `imbackups` folder on the backup server using a file transfer tool (e.g. WinSCP).

Note: You don’t need to copy the `*.pwds` file. That's just an information file containing the passwords of the users configurted in the Linux image.

7.8.8 Recovery Mode Information

If your device is started in Recovery Mode, than you can use following user to login (Diagnosis Tool uses the same user for ssh connection and it is hardcoded):

- user: `tc`
- pass: `1qwe!QWE`

Root user is disabled, but you can have root permissions with following command: `sudo su`

Note: No root password necessary to change to superuser.

7.8.9 How to Backup an Image

Step by Step

1) Start the Diagnosis Tool

2) Right click on the device youi want to backup and select **Reboot OSX Client device to Recovery Mode**.
3) Wait for the device to boot in Recovery mode, then click on **Update List** button.
4) When the Client is in Recovery Mode, a new option appears in the contect menu in Diagnosis Tool. Select the **Backup OSX Client device** option.
5) In the appearing window enter the folder name where the backup will be saved (**Backup Name** field).
6) After pressing **OK** the image will be saved to the `imbackups/<BackupName>` folder.

   During the backup process a new folder with the MAC Address of the client will be created and it contains the `backup.img` file. This can be restored later to the same device. (The MAC Address is checked during restore.)

7.8.10 How to Restore an Image

Step by Step

1) In Diagnosis Tool (device in Recovery mode) right click on the client you want to restore and select **Restore OSX Client device**.
2) In the window that appears select the formerly created `backup folder` from the list, that needs to be restored.
3) After pressing **OK** the selected image will be restored.

   Note: The MAC address will be checked.

7.8.11 How to Push an Image

Prerequisites

You need to place the factory Linux image in the i`mbackups` folder on the backup server to change the OS from Windows XP to Linux or to refresh the existing Linux image.

Step by Step

1) In Diagnosis Tool (device is in Recovery mode) select **Refresh the image of OSX Client device to a new one** for the client you want to push the image to.
2) In the appearing window select the image you want ot install on the device.
3) After pressing **OK** the selected image will be pushed to the device.

   The existing network settings, hostname and client connection information will be kept, but you'll need to install the OpenScape Xpert Client application.
4) When the push process is ready the device will be rebooted automatically to normal mode.

7.8.12 How to Install the OpenScape Xpert Client Application

Prerequisites

When the installation of the new Linux image on an OpenStage Xpert 6010p device is finished, you can install the OpenScape Xpert Client application using the Diagnosis Tool.

Step by Step

1) In Diagnosis Tool (device in normal mode with the new image installed) right click on the device and select the **Install OSX Client** option.

   A new window is displayed.

2) Enter the IP address/ hostname of System Manager in the corresponding field.

   If the selected devices already has a `TurretGlobalSettings.ini` configuration file with the same IP address/ hostname as the System Manager, then the IP address field is automatically filled in with the common IP address.

3) Optionally, you can configure a HTTP/HTTPS proxy for System Manager.

4) Browse for the `.deb` file to install the OpenScape Xpert Client.

   The **OK** button becomes enabled if the following requirements are fulfilled:

   - There is an IP address or a fully qualified domain name in the textbox,
   - The `turret.deb` file is selected.

5) Click the **OK** button to install the Client application via Diagnosis Tool.

7.9 Devicelock

Overview

Several customers want to prevent their users attaching non-supported USB devices to the OSX Client device. The devicelock is considered to be a security feature in order to prevent any malfunctioning in the system, or spreading viruses from pen-drives, etc..

Sometimes the system administrator needs to attach a non-supported USB device (e.g. a keyboard in order to configure the OSX Client). To by-pass the devicelock an "USB-key-unlock" feature is provided.

- The administrator creates an unique USB key. After plugging in this unique USB key, the Operating System enables attaching any USB devices.
- If the System Administrator would like to create an USB key, he/she will need a public/private key pair.
  - The public key has to be placed on the OSX Client Device. It is used for verifying the USB key.
  - The private key is used for creating the signature file on the USB stick. This is the file which is veryfied by the OSX Client using the public key. The private key must be kept at a safe location because the owner can create a new unlock-key.

NOTICE:

This features are available on linux operating systems only. Both, the devicelock and the USB-key-unlock feature are turned off by default.

7.9.1 How to Turn On Devicelock

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

The devicelock is turned off.

Step by Step

1) In Diagnosis Tool (device in normal mode) right-click on the device.
2) Select the Devicelock -> Enable USB devicelock for selected OSX Client devices option.

7.9.2 How to Turn Off Devicelock

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

The devicelock is turned off.

Step by Step

1) In Diagnosis Tool (device in normal mode) right-click on the device.
2) Select the Devicelock -> Disable USB devicelock for selected OSX Client devices option.

7.9.3 How to Create a Public/Private Key Pair

Prerequisites

A (secure) linux machine is available, with installed gpg.

Step by Step

1) Generate the key: `gpg --full-generate-key"`
   a) Enter the type of key: `1`

   NOTICE:

   `RSA` can be changed to "1" in the list of key types while this value represents `"RSA"` and `"RSA(default)"`.

   b) Enter the size of the key: `2048`
   c) Enter how long is it valid: `0` (0 means that the key doesn't expire at all, a reasonable difference from this can be applied)
   d) Enter the real name and email address.
   e) If necessary, enter a comment.
   f) The passphrase must be empty.

      During the creation of the key, the following error can occurre: "Not enough random bytes available." This problem is caused by the lack of entropy in the system.
   g) In case of an error, run the following command on another terminal: `apt-get install rng-tools`
   h) If the key is still not generated, run the following command too: `rngd -f -r /dev/urandom`
2) Export the public key to a file, to push it later to the OSX Clients: `gpg --output <filename> --export <emailaddress>`

NOTICE:

For further information about GPG please refer to https://www.gnupg.org/gph/en/manual.html

7.9.4 How to Push the Public Key to an OSX Client

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

Step by Step

1) In Diagnosis Tool (device in normal mode) right-click on the device.
2) Select the Devicelock -> Push certificate to selected OSX Client devices option.
3) In the appearing window browse for the public key file.
4) Click **OK**.

7.9.5 How to Create a USB Key

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

A formatted USB stick is available.

A (secure) linux machine is available, with installed gpg.

The private key needs to be imported into your keyring. If the key-pair was generated on this machine, then it is imported already. Otherwise manual import is necessary (`gpg --import <path to your private key>`)

Step by Step

1) Execute this script (the script is in the Tools\DeviceLock directory on the CD): `/createkey.sh <device> <private key id>`.
2) Enter the <device> parameter: The device file for the USB stick, e.g. `/dev/sdb`. can be determined from the output of `dmesg` command after plugging it in and running. Here is an example of the output:
   a) To determine the USB device's file plug in the USB device.
   b) Run `dmesg`. The last row shows the name of the device file.

      Here is an example of the output:

```
[264719.052308] scsi 4:0:0:0: Direct-Access     ADATA    USB Flash Drive  1100 PQ: 0 ANSI: 6
[264719.053422] sd 4:0:0:0: Attached scsi generic sg1 type 0
[264719.055299] sd 4:0:0:0: [sdb] 15425536 512-byte logical blocks: (7.89 GB/7.35 GiB)
[264719.058528] sd 4:0:0:0: [sdb] Write Protect is off
[264719.058543] sd 4:0:0:0: [sdb] Mode Sense: 22 00 00 00
[264719.059932] sd 4:0:0:0: [sdb] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA
[264719.071053]  sdb: sdb1
[264719.076626] sd 4:0:0:0: [sdb] Attached SCSI removable disk
```

      In this example, the needed device file is sdb, so the <device> parameter should be /dev/sdb
3) Enter the <private key id> parameter (optional): The key id for the private key you want to use for signing the USB stick. If no key is provided, the default key will be used.
   a) To get the key id run `gpg --list-keys`.

      The keys are listed.

      Example:

      ```
      pub rsa2048 2018-07-27 [SC]
      E9CEDA3B139762A0FA171B8048E15585C74E0E6E
      uid [ultimate] John Smith <john.smith@unify.com>
      sub rsa2048 2018-07-27 [E]
      ```

      In this example, the needed ID is E9CEDA3B139762A0FA171B8048E15585C74E0E6E.

7.9.6 How to Turn On USB Key Unlock

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

The devicelock public key has been pushed to the OSX Client.

USB Key Unlock feature is turned off.

Step by Step

1) In Diagnosis Tool (device in normal mode) right-click on the device.

2) Select the Devicelock -> Enable USB key unlock for selected OSX Client devices option.

7.9.7 How to Turn Off USB Key Unlock

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

The devicelock public key has been pushed to the OSX Client.

USB Key Unlock feature is turned on.

Step by Step

1) In Diagnosis Tool (device in normal mode) right-click on the device.
2) Select the Devicelock -> Disable USB key unlock for selected OSX Client devices option.

7.10 LLDP-MED

Customers can use OSX Client devices in a VLAN together with LLDP-MED protocol. This feature can be turned off / on from Diagnosis Tool.

NOTICE:

Starting with image version 4.0.6, LLDP-MED is disabled by default.
To enable it, please refer to How to create a bootable USB stick on page 162.

7.10.1 How to turn off LLDP-MED

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

The LLDP-MED is turned on.

Step by Step

1) In Diagnosis Tool (device in normal mode) right-click in the device.
2) Select the **LLDP-MED configuration**.
3) Select the **Disable LLDP-MED** option.

NOTICE:

After deploying a new OpenStage Xpert Client image the LLDP-MED feature will be turned on. Use the procedure above to turn it off again.

7.10.2 How to turn on LLDP-MED

Prerequisites

The new Linux image is present on an OpenStage Xpert 6010p device.

The LLDP-MED is turned off.

Step by Step

1) In Diagnosis Tool (device in normal mode) right-click on the device.
2) Select the **LLDP-MED configuration**.
3) Select the **Enable LLDP-MED** option.

7.11 Mass deployment of HTEMS certificates for OSX Devices

7.11.1 Generate the certificates with a MS CA

This section describes how to auto generate and deploy certificates for OSX Devices (MLCs and Linux Turrets with software installed). This certificate will be used for secure HTEMS communication between devices, respectively for securing the API communication on Turrets, and securing the SIP and CSTA communication on MLCs.

Prerequisites

A CA with a certificate template that can be used to generate the certificates. The certificate template should have have configured the following parameters:

1) Key Usage: Digital Signature, Key Encipherment
2) Enhanced Key Usage: Client Authentication, Server Authentication
3) For auto enrollment: CA certificate manager approval must not be checked
4) Subject Name must be configured to "Supply in request"
5) The user must have Read and Enroll the rights for this template
6) Cryptography:
   - The minimum key size must be set to 2048
   - Requests can use any provider available

     or

     Requests must use one of the following providers: select **Microsoft RSA Channel Cryptographic Provider**

Step by Step

1) From the **Client** list select the OSX Devices for which you want to generate and deploy certificates.
2) Select the **Certificates** menu and then click on **Generate and deploy machine certificate** sub menu.
3) Enter the configuration address of the CA you want to use it in the **Certificate Authority** text box. If you do not know this address press **Browse** and select the CA you want to use. In this case the CA configuration string is automatically filled.

4) In the **Certificate Template Name** text box enter the certificate template name you want to use for certificate generation.

   NOTICE:

   The **Certificate Template Name** is not the same as the **Certificate Template Display Name.**

5) In the **Trusted CA certificate handling** section, select:
   - **Do not change**, if you want to leave the Trusted CA certificates file (ca-cert.pem) untouched
   - **Append to existing,** if you want the certificate of the used CA to be appended to the `ca-cert.pem` file on the client
   - **Replace all Existing,** if you want it to be overwritten.
6) Press **OK** to start the certificate deployment. The MLCs for the successful deployment is automatically restarted. The OSX clients must be restarted in an additional step using the context menu.

   NOTICE:

   In case of Windows Soft Clients it is mandatory the user has Local Administrator rights on Windows workstations.

7.11.2 Use pregenerated HTEMS certificates

Step by Step

1) Select the OSX devices for which you want to deploy certificates from the client list.
2) Select the **Certificates** menu.
3) Select the **Deploy pre-created machine certificates** sub menu.
4) On the opening dialog, press the **Browse** button and select the data/csv file which contains the information about the machine certificates.

   The file must contain:

   a) • the IP address of the client
      • the path to the PFX file containing the certificates (absolute or relative to the data file)
      • the password to the PFX file

      NOTICE:

      All fields are mandatory and separated by a comma.

   Example:

   a) • 192.168.1.1, C:\temp\client1.pfx,pwd

- 192.168.1.2,client2.pfx,pwd

After selecting the data/csv file, a prevalidation check will be performed (e.g.the selected clients have corresponding records in the data file).

If there are any prevalidation errors, they will be displayed in a separate dialogue and the deployment will stop. Otherwise, the **OK** button will be enabled.

In the Trusted CA certificate handling section, select:

- **a)** **Do not Change** if you want to leave the Trusted CA certificates file (ca-cert.pem) untouched.
  b) **Append to existing** if you want the certificate of the used CA to be appended to the **ca-cert.pem** file on the client
  c) **Replace all Existing** if you want it overwritten.

  Select **OK** to start the certificates deployment.The MLCs will be restarted automatically and the OSX clients have to be restarted in an additional step using the context menu.

NOTICE:

In case of Windows Soft Clients it is mandatory the user has local administrator rights on Windows workstations.

7.12 Mass replacement of Trusted CA certificates for OSX Devices

To replace the Trusted CA certificates file (`ca-cert.pem`) used for secure communication (HTEMS, API, SIP, CSTA) please follow the steps below.

Prerequisites

The following devices are currently available for this feature:

1) MLCs
2) Linux Turrets with client software installed

Step by Step

1) Select the **Certificates** menu and then click on the **Replace Trusted CA certificates** sub menu.

2) On the opening dialog select the Trusted CA certificates file you want to use and click **OK.**

Fastpath:

The MLCs for the successful deployment is automatically restarted and the OSX clients must be restarted in an additional step using the context menu.

The Trusted CA certificates file must be in PEM format. All the trusted CAs certificates should be copied on it in PEM format.

To convert a certificate from DER to PEM format you can use the openssl command (available in the Diagnosis Tool INSTALL_DIR):

```
openssl x509 -inform der -in certificate.cer
-out certificate.pem
```

NOTICE: The certificate update will not work, if you delete manually any installed certificate files on Linux Turrets.

---

8 Fault Management with CAP FM — Overview

This chapter describes the installation and configuration of the Microsoft Windows SNMP service and the CAP FM at the OpenScape Xpert System manager server and the configuration of the related components.

Functional Overview

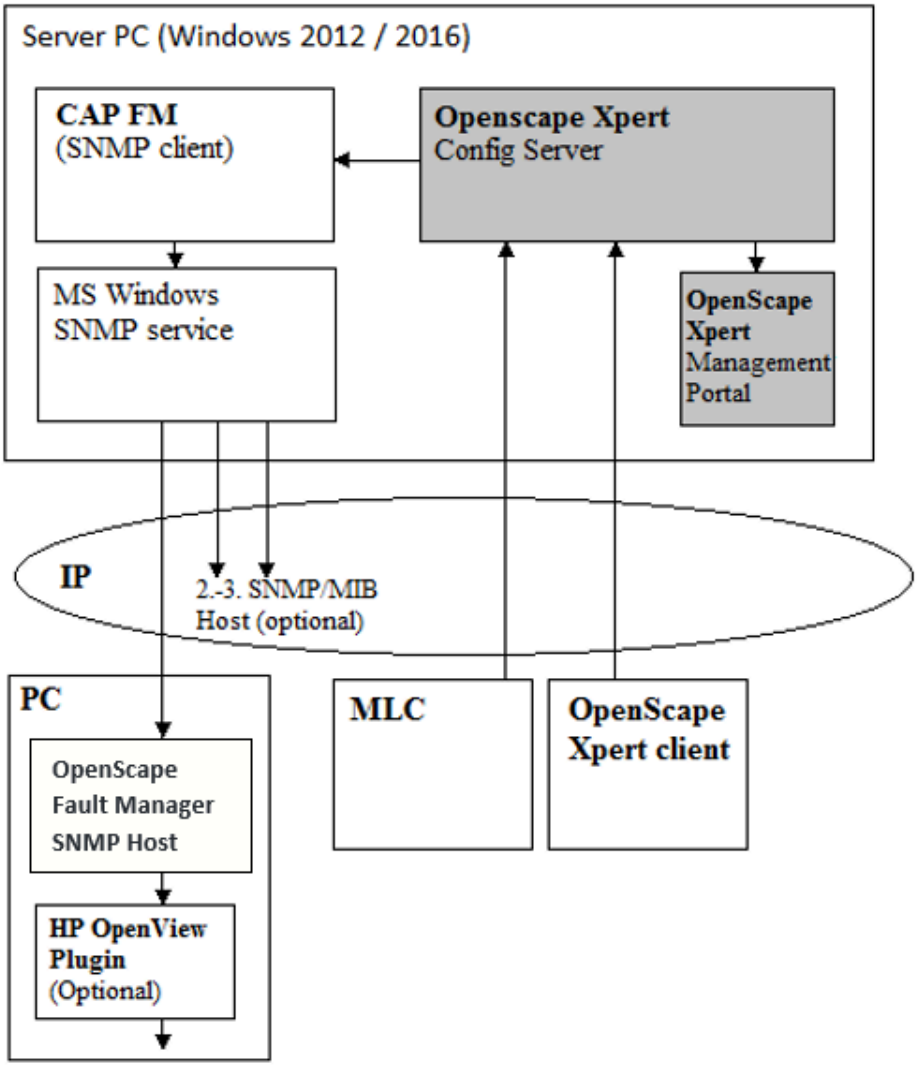
The condition of the OpenScape Xpert system components is displayed on the user interface at the System Manager client. The OpenScape Xpert has the possibility to send errors and warnings from OpenScape Xpert System Manager to a SNMP/MIB Host (OpenScape Fault Manager) via the Simple Network. Management Protocol SNMP by using a particular Management Information Base Definition MIB. With this feature, states of OpenScape Xpert hardware components can be monitored through an SNMP/MIB Host e.g. OpenScape Fault Manager.

The following OpenScape Xpert object can be monitored

- MLC
- IP Turret

NOTICE:

The Operating System and PC/Server Hardware can also be monitored by the SNMP protocol, but it is not the part of the OpenScape Xpert Feature.



NOTICE:

No events will be accumulated and for example, collectively sent after a time via SNMP/MIB Interface. There is a unidirectional data transfer from the System Manger Server (Reporting Client) to the SNMP/MIB Hosts e.g. OpenScape Fault Manager.

Definitions

- **SNMP**: Simple Network Management Protocol, Standard: RFC 1157 IP Network Ports: 161/UDP, 162/UDP (Trap).
- **Trap**: The managed agent sends an event notification, called "trap" to the management system to identify the occurrence of conditions such as threshold that exceeds a predetermined value.

8.1 OpenScape Xpert System Manager Administration

This section describes the handling of the alarms and reports using the OpenScape Xpert System Manager.

Operational States

The condition of the OpenScape Xpert system components is displayed on the user interface at the OpenScape Xpert Management Portal.

State	Node Address	Alias Name	Location	Group Name	Assigned IP
●	1.1.1.0		Default Location	Trading Group (Q) 2	192.168.9.132
●	1.1.2.0		Default Location	Trading Group (Q) 2	192.168.9.147
○	1.1.3.0		Default Location	Trading Group (Q) 2	Unassigned
○	1.1.4.0		Default Location	Trading Group (Q) 3	Unassigned
○	1.1.5.0		Default Location	Trading Group (Q) 3	Unassigned
○	1.1.6.0		Default Location	Trading Group (Q) 3	Unassigned
○	1.1.7.0		Default Location	Trading Group (Q) 3	Unassigned
○	1.1.8.0		Default Location	Trading Group (Q) 3	Unassigned
○	1.1.10.0		Default Location	Trading Group (Q) 3	Unassigned
●	1.1.9.0	MyLittleTT	Default Location	Trading Group (Q) 3	192.168.9.56
○	1.1.11.0	MyLittleTT (1)	Default Location	Trading Group (Q) 3	Unassigned
○	1.1.12.0	MyLittleTT (2)	Default Location	Trading Group (Q) 3	Unassigned

The operational states will be shown in the OSX Client list and MLC list in the OSX Management Portal.

State	Node Address	Alias Name	Location	Group Name	Num. of Lines	Assigned IP
○	1.100.2.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.3.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.4.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.5.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.7.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.8.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.9.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.10.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
○	1.100.11.0		Default Location	Trading Group (Q) 1	0 / 241	Unassigned
●	1.100.1.0	MLC 1	Default Location	Trading Group (Q) 1	10 / 241	192.168.12.31
○	1.100.6.0	MyLittleMLC	Default Location	Trading Group (Q) 1	0 / 241	Unassigned

The following “Operational States” are possible for the OpenScape Xpert components:

	Operational States		
	OK	New	Error
MLC (DPC)	●	○	●
IP Turret	●	○	●

- OK

  The connection between the Turret/MLC and the SM is OK.
- NEW

  The topology object has the New state if the object is not assigned to an IP address.

- ERROR

  The Turret/MLC is assigned but the connection between the Turret/MLC is disconnected. This state is displayed if the Turret/MLC is not running or crashed.

Functional Description

The settings for the optional information via SNMP/MIB are carried out at the System Manager client and can only be done with the Administrator authorization. With the Maintenance and Customer authorizations, the setting can be displayed but cannot be modified. A Signaling via SNMP/MIB is generated when the error or warning events occur as well as when they are resolved.

8.1.1 How to Configure Error Reporting for a MLC/Client

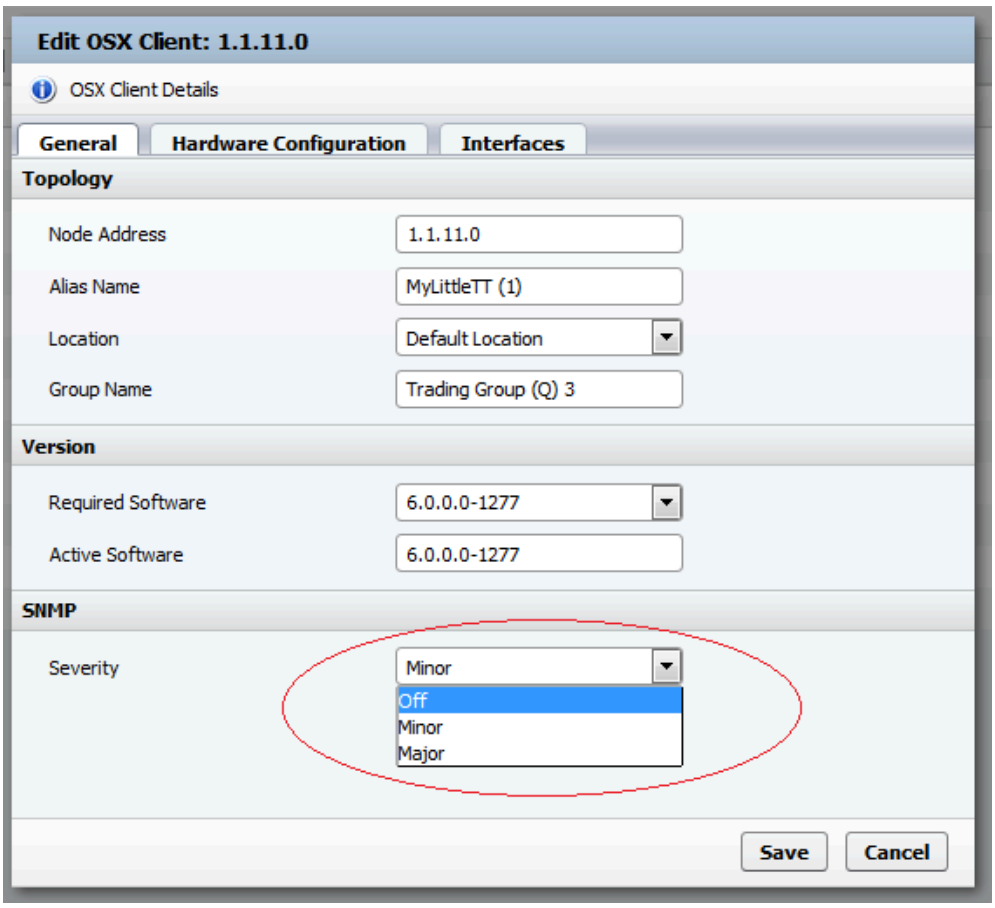
Proceed as follows to configure the error reporting settings for a specific OSX Client/MLC (hereinafter clients).

Step by Step

1) Within the Management Portal, select the **OSX Clients** (or MLCs) menu entry on the side menu.

2) Click on the node address of the client.

3) In the property window, below the SNMP label you can select the desired severity of the SNMP traps. The available options are:



4) In order to receive SNMP traps about the client, select either Minor or Major. The feature can be disabled by selecting Off. The following char summarizes the severities of the traps sent about this client:

	Events				
Selected SNMP severity	Config Server Start	Client assigned	Client unassigned	Client connected	Client disconnected
Off	N/A	N/A	N/A	N/A	N/A
Minor	Minor	Minor	Unmanaged	Normal	Minor
Major	Major	Major	Unmanaged	Normal	Major

5) Click **Save** to confirm the settings.

8.2 Microsoft® Windows SNMP Service

This section describes how to check the Microsoft Windows SNMP service installation and how to install it.

The Windows SNMP Service provides an own GUI for the administration of the SNMP properties, including the trap destinations.

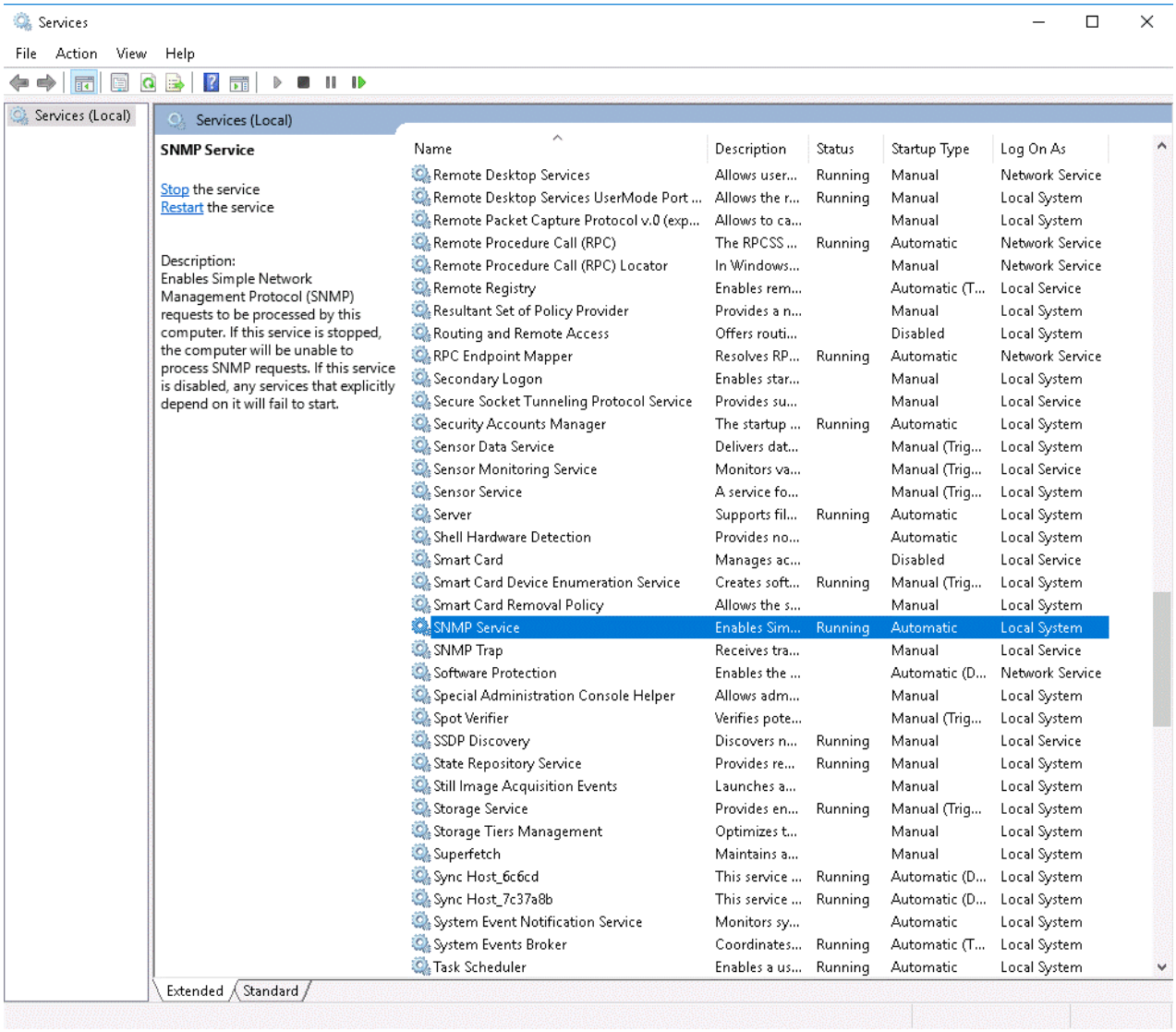
8.2.1 How to Check the SNMP Service

For a successful installation the SNMP Service has to be installed on the computer where TRAP messages will be sent.

Step by Step

1) To check whether SNMP is installed on the computer, open **Settings** > **Control Panel** > **Administrative Tools** > **Component services** > **Services (Local)**.

A list of programs installed on the computer appears.



2) Please check for **SNMP service**. If it is not present, then it must be installed.

8.2.2 How to Install Windows SNMP Service (Windows 2016/2019)

If Windows SNMP is not installed on the computer, then proceed as follows to install it.

Step by Step

1) Start the Server Manager.
2) On Dashboard click on **Add roles and features**.

   The wizard appears.
3) Click on **Server Selection**.
4) Click on **Features**.
5) Select **SNMP Services** from the list of Features.

   A dialog appears.
6) Click on **Add Features**.
7) Click **Next** and then **Install** to perform the installation.

   You do not have to reboot the computer.

The Microsoft Windows SNMP Service is installed on the system.

8.2.3 How to Configure the SNMP Service

Proceed as follows to configure the Windows SNMP Service, including the trap destinations.

Prerequisites

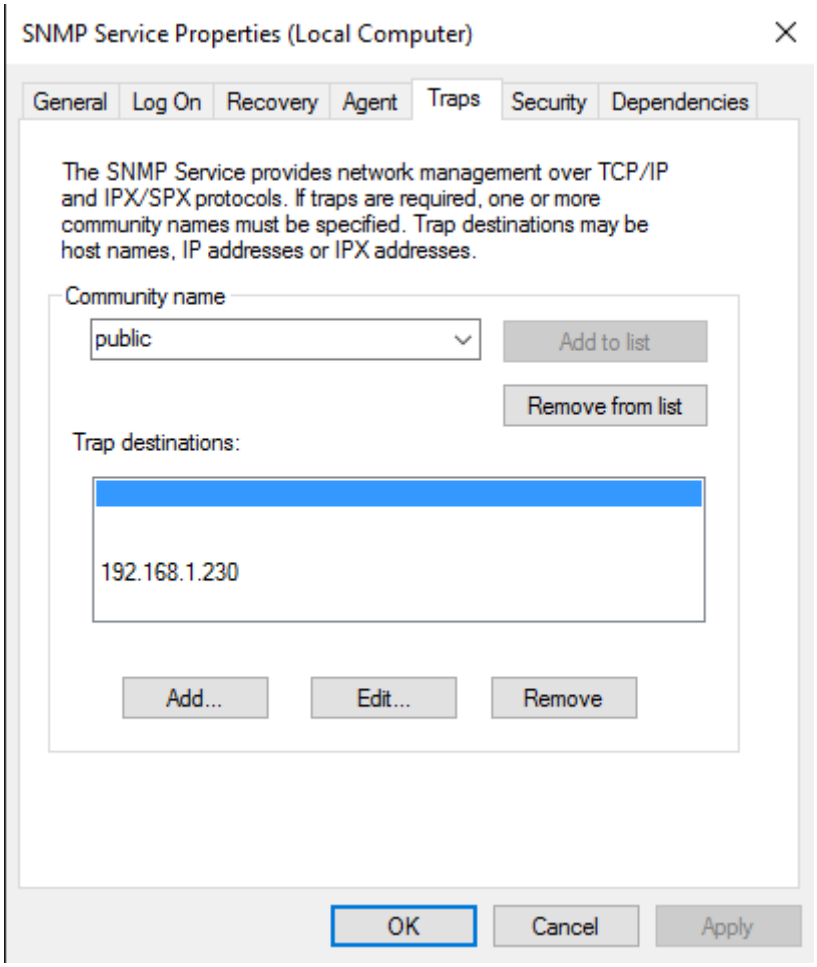
The SNMP Service is installed on the system.

Step by Step

1) To open the SNMP service navigate to **Administrative Tools** > **Server Manager**.
2) In the Server Manager open **Configuration** and got to **Services**.

3) Within the list of local services, double-click the **SNMP Service** entry or right-click the **SNMP Service** entry and a select **Properties**.

   The **SNMP Service Properties** dialog appears.



4) Select the **Traps** tab.
   a) The **Community name** here must be the same as on the OSFM (here “public”).
   b) Use the **Add**, **Edit** or **Remove** buttons to configure the **Trap destinations** for this community according to the requirements.

8.3 CAP FM at Openscape Xpert System Manager Server

This section describes the installation procedure of the Common Application Platform Fault Management at the OpenScape Voice Xpert System Manager Server.

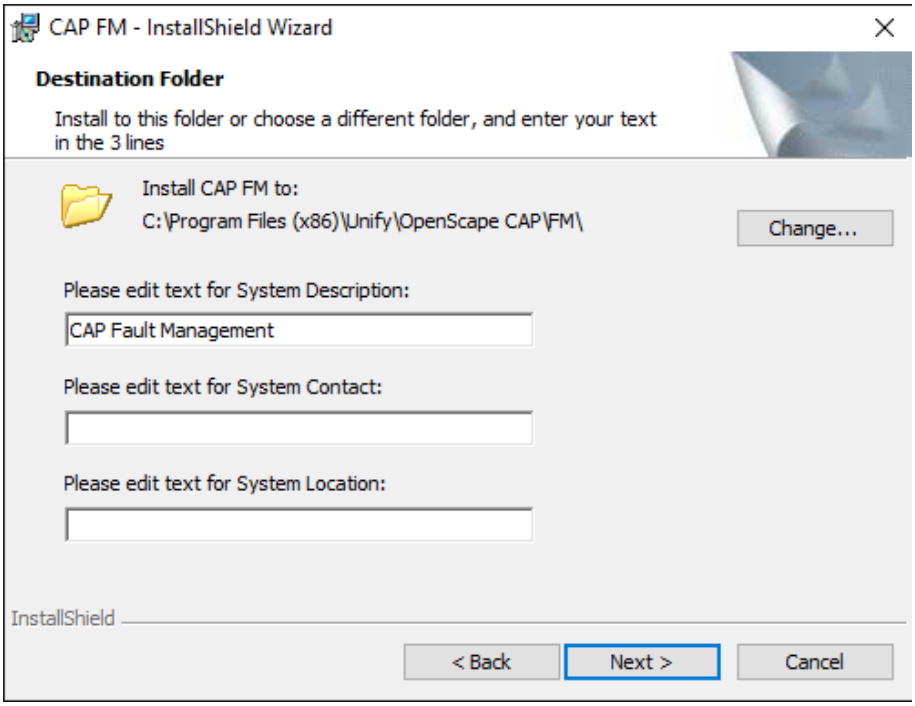
8.3.1 How to Install and Configure CAP FM at the System Manager

Proceed as follows to install the Common Application Platform Fault Management Software on the OpenScape Xpert System Manager Server.

Step by Step

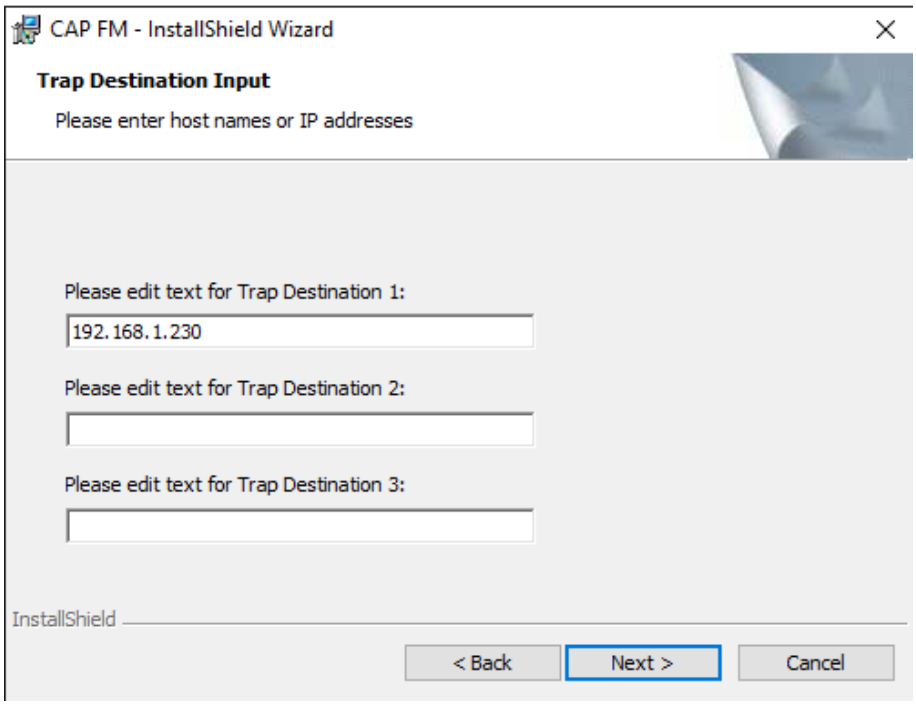
1) Insert the OpenScape Xpert System software installation CD in the disk drive of the System Manager server.
2) Run the CAP FM setup program under Tools\CAPFM. The Installation Welcome dialog appears indicating that the basic checks have been successfully passed and the installation process can be continued. This dialog shows the actual version and build of OpenScape CAP FM provided with the MSI-package.
3) Click the **Next** button in the Installation Welcome dialog.

   The Destination folder and system description dialog appears. The Destination folder and system description dialog provides the GUI to change the default installation directory and shows the default value for the system description parameter.



4) Click the **Next** button in the Destination folder and system description dialog.

The Trap destination input dialog appears. Enter the IP address of the OSFM.



5) The Trap destination input dialog provides the GUI to enable the input of up to three trap destinations into the trap destinations table of the Windows SNMP Service.

NOTICE: Any trap notification of OpenScape CAP FM will be sent to every trap destination listed in the trap destination table of the Windows SNMP Service. OpenScape FM or any other network management system that wants to receive trap notifications from OpenScape CAP FM is required to enter its host name or IP address into the trap destination table

---

6) Click the **Next** button and follow the instructions of the setup wizard to finish the installation.

8.4 Installation Checklist for Fault Manager

The OpenScape Fault Manager is the standard SNMP/MIB host system for the OpenScape Xpert System. Only this SNMP/MIB host is tested and released with OpenScape Xpert.

Prerequisites

- Running OpenScape Xpert System with System Manager and MLCs and IP Turrets.
- All concerned PC’s have to be in the same network.
- PC for FM Server and CAP FM. For more information, see OpenScape Fault Management documentation.

- License for FM Server.

Installation

(Example – Could be different in each FM Software)

- Install Java on the FM Server.
- Install FM Server Software.
- Register license for FM Server.
- Start the FM Server (e.g. services…)
- Install at the OpenScape Xpert System Manager the CAP FM.
- Configure OpenScape Xpert System Manager as described before.
- Check if at the OpenScape Xpert System Manager the Service SNMP is started.
- Log in to the FM Server.
- Configure the FM Server for the OpenScape Xpert System.

8.5 OpenScape Fault Manager Tool

The OpenScape Fault Manager Tool is a small tool for OpenScape Xpert which enables the Xpert system's topology to be displayed in a tree view in OpenScape Fault Management.

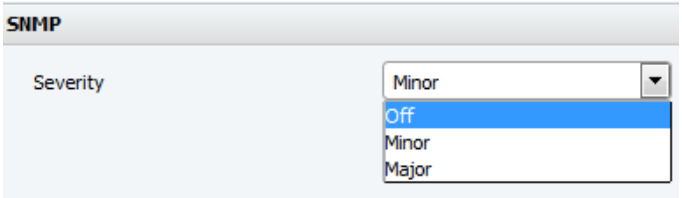
General Information

NOTICE:

The Fault Management server can collect information from the OS Xpert System Manager even if this tool is not installed, but it won't show the System Topology and won't display the events separately for the different Xpert components.

- Status information is sent from local MLCs and Turrets.
- Status information is sent from connected SMs in Cluster.
- If the status tool has any exception during running, the tree will contain an „OpenScape Xpert Script Error" node.

  In the current value of this node, a detailed error text is displayed. If necessary contact OpenScape Xpert support and report the problem.
- Status information will only be sent to OpenScape FM if the Turret or MLC is set to send reports in SMAdmin.

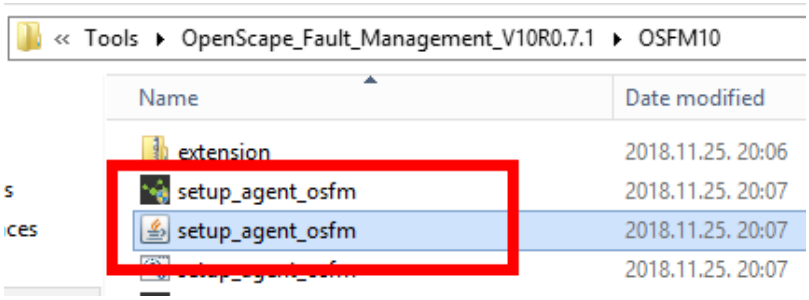


- This setting also affects the Error Severity (if in error case minor or major errors are reported).

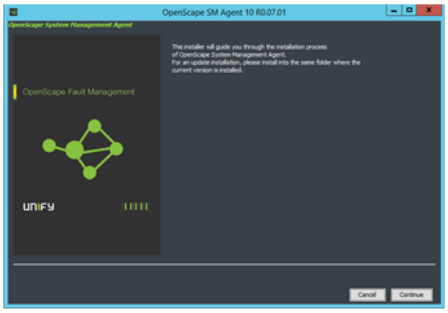
8.5.1 How to Setup the OpenScape Fault Manager Tool

Step by Step

1) Install the OpenScape FM SM Agent on the OpenScape Xpert System Manager (This Software is part of the OpenScape FM Software) .

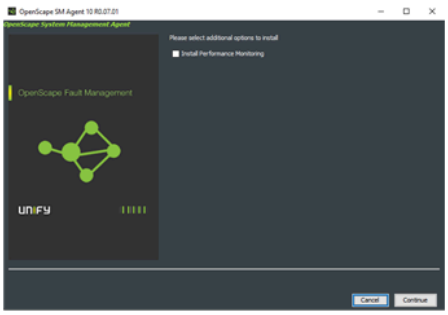


(E.g. from OpenScape FM Software V10)



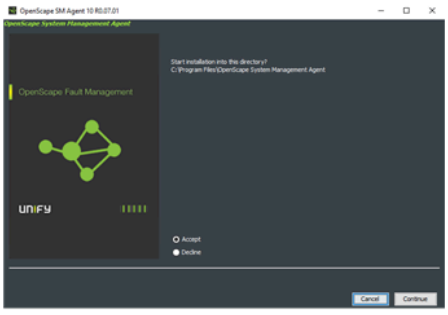
Click Continue

Accept the License and click Continue

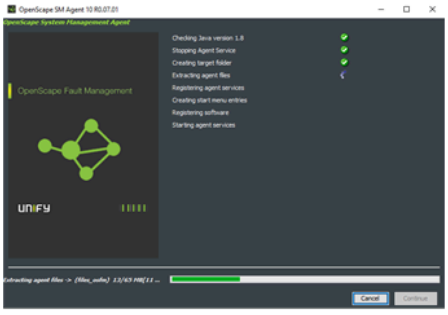


Click Continue

Choose or change the Folder and click Continue



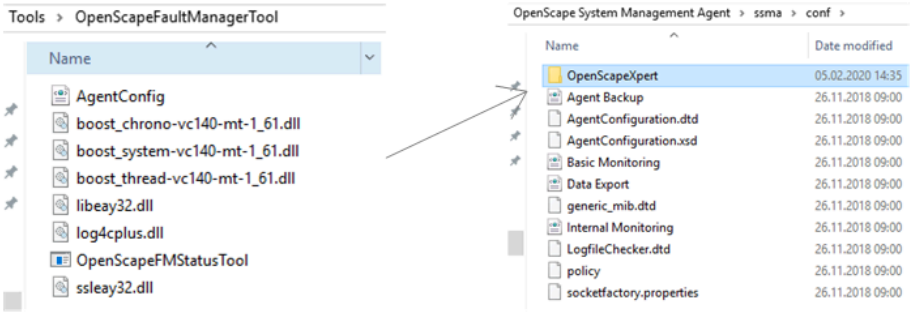
Accept the folder and press Continue



End the installation with Finished

2) Add the OpenScape Xpert SM as „SSMAP” to the OpenScape FM as IP node, if not yet available. For detailed steps please see the OpenScape Fault Management manual.

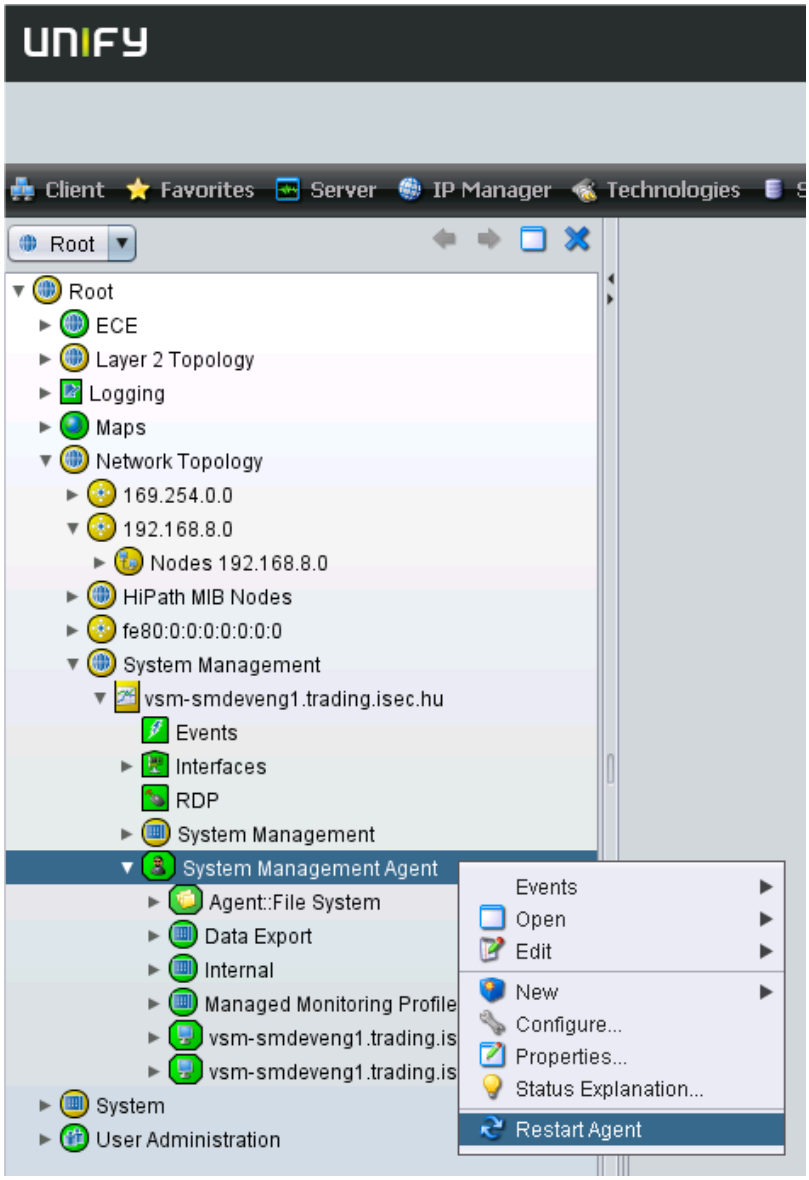
3) Create a new folder in <OSFM install dir>\ssma\conf called “OpenScapeXpert”. (The folder name under ssma will be displayed in the OSFM tree. You can use any other name too.)
4) Copy all files from \Tools\OpenScapeFaultManagerTool of the OpenScape Xpert Software to this folder.



5) Modify the AgentConfig.xml for your needs. (Not necessary)
   a) Setup the execution interval. By default the status will be queried every 180 seconds.
   b) To change the value configure the following line „`<interval interval="180"/>`”.
6) Restart the SMAgent on the OpenScape FM System.
   a) Look for the node in the OSFM tree where the SMAgent was installed.
   b) Open the node and right clock on Internal System Management Agent.
   c) Select **Restart Agent**.

   After the restart the OpenScape Xpert status information are displayed in the tree under the „System Management/OpenScape Xpert/OpenScape Xpert” node.

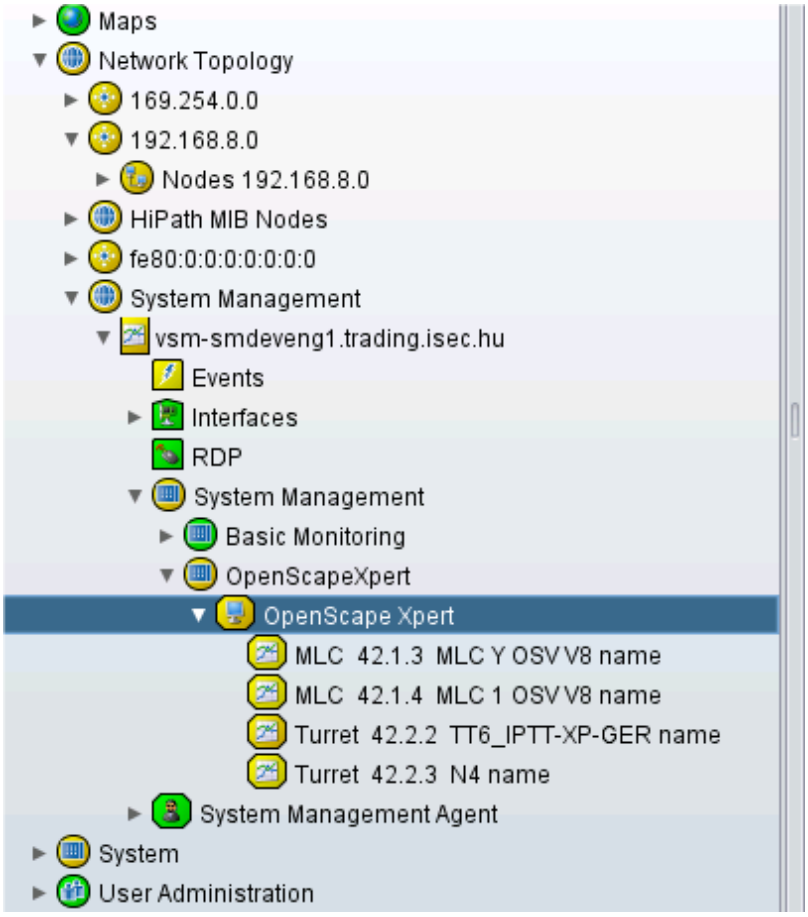
7) If the new node is not displayed, right click on the Internal System Management node and select Execute All Monitors. Or setup a new IP Node manually.



NOTICE:

The "System Management" and "System Management Agent" node is called "Internal System Management" or

"Internal System Management Agent" if it is running on the local server.



The status items have names of the format "<Type> <Node Address> <Alias Name>".See Picture E.g.: "Turret 42.2.3 N4 name". Unlike in the picture, the labeling is with OSX V6 and V7 as follows "Turret 1.1.5 N4 name".

8.5.2 HP OpenView Plugin for OpenScape Fault Manager

Management Platform

MATERNA MANAGEMENT PLATFORM Gateway for OpenScape and HP OpenView/IBM Tivoli NetView, called the MMP GATEWAY, provides for an efficient and innovative solution for interconnecting complementary IT management platforms with OpenScape Fault Management from Unify:

- Hewlett Packard’s OpenView Network Node Manager.
- IBM’s Tivoli NetView.

By employing the MMP GATEWAY, any object, which is managed by HiPath FM, can be visualized in HP OpenView/IBM Tivoli NetView.

NOTICE:

For further Informations on OpenScape Fault Mananger and HP OpenView Plugin please contact Your next level of Unify Support.

9 Reference Information OpenScape Xpert V7

This chapter contains reference information on the OpenScape Xpert V7 system components.

9.1 Firewall Ports OpenScape Xpert V7

OpenScape Xpert V7Rx
Firewall basic requirements
Standard ports

Device A		Device B	Protocol	Port	Designation	Comments
Xpert Windows Soft Client	⇆	Active Directory Server	TCP / UDP	53	dns	Name Resolution
Xpert Windows Soft Client	⇆	Active Directory Server	UDP	88	kerberos	Kerberos authentication
Xpert Windows Soft Client	⇆	Active Directory Server	UDP	123	ntp	time synchronization
Xpert Windows Soft Client	⇆	Active Directory Server	TCP	135	rpc	RPC Service
Xpert Windows Soft Client	⇆	Active Directory Server	UDP	137	netbios-ns	NetBIOS - Naming Service
Xpert Windows Soft Client	⇆	Active Directory Server	UDP	138	netbios-dgm	NetBIOS - Datagram Service
Xpert Windows Soft Client	⇆	Active Directory Server	TCP	139	netbios-ssn	NetBIOS - Session Service
Xpert Windows Soft Client	⇆	Active Directory Server	TCP	445	smb	SMB client for database backups
Xpert Windows Soft Client	⇆	Active Directory Server	TCP	464	kpasswd	Kerberos Password Change
Xpert Windows Soft Client	⇆	Active Directory Server	ICMP	Type 8 / Type 0	ping	Network Service
Xpert Windows Soft Client	⇆	Active Directory Server / LDAP Server	TCP	389	ldap	LDAP authentication of OSX client users
Xpert Windows Soft Client	⇆	Active Directory Server / LDAP Server	TCP	636	ldaps	Secured LDAPS authentication of OSX client users
Xpert Windows Soft Client	→	DHCP Server	UDP	67	bootps	DHCP Discover / DHCP Request
Xpert Windows Soft Client	←	DHCP Server	UDP	68	bootpc	DHCP offer DHCP acknowledgement
Xpert Windows Soft Client	⇆	System Manager	UDP	137	netbios-ns	NetBIOS - Naming Service
Xpert Windows Soft Client	⇆	System Manager	UDP	138	netbios-dgm	NetBIOS - Datagram Service
Xpert Windows Soft Client	⇆	System Manager	TCP	139	netbios-ssn	NetBIOS - Session Service
Xpert Windows Soft Client	⇆	System Manager	TCP	443	https	MLC & Client SW update via HTTPS
Xpert Windows Soft Client	⇆	System Manager	TCP	445	smb	Versions check and 6010p Turret & Xpert Soft Client Upgrade
Xpert Windows Soft Client	⇆	System Manager	ICMP	Type 8 / Type 0	ping	A ping may be performed on the Server when starting a terminal
6010p Turret & Linux Soft Client	⇆	Active Directory Server	TCP / UDP	53	dns	Name Resolution
6010p Turret & Linux Soft Client	⇆	Active Directory Server	UDP	137	netbios-ns	NetBIOS - Naming Service
6010p Turret & Linux Soft Client	⇆	Active Directory Server	UDP	138	netbios-dgm	NetBIOS - Datagram Service
6010p Turret & Linux Soft Client	⇆	Active Directory Server	TCP	139	netbios-ssn	NetBIOS - Session Service
6010p Turret & Linux Soft Client	⇆	Active Directory Server	TCP	445	smb	SMB client for database backups
6010p Turret & Linux Soft Client	⇆	Active Directory Server	ICMP	Type 8 / Type 0	ping	Network Service
6010p Turret & Linux Soft Client	⇆	Active Directory Server / LDAP Server	TCP	389	ldap	LDAP authentication of OSX client users
6010p Turret & Linux Soft Client	⇆	Active Directory Server / LDAP Server	TCP	636	ldaps	Secured LDAPS authentication of OSX client users
6010p Turret & Linux Soft Client	→	DHCP Server	UDP	67	bootps	DHCP Discover / DHCP Request
6010p Turret & Linux Soft Client	←	DHCP Server	UDP	68	bootpc	DHCP offer DHCP acknowledgement
6010p Turret & Linux Soft Client	⇆	NTP Server	UDP	123	ntp	time synchronization
6010p Turret & Linux Soft Client	⇆	System Manager	UDP	137	netbios-ns	NetBIOS - Naming Service
6010p Turret & Linux Soft Client	⇆	System Manager	UDP	138	netbios-dgm	NetBIOS - Datagram Service
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	139	netbios-ssn	NetBIOS - Session Service
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	445	smb	Versions check and 6010p Turret & Xpert Soft Client Upgrade
6010p Turret & Linux Soft Client	⇆	System Manager	ICMP	Type 8 / Type 0	ping	A ping may be performed on the Server when starting a terminal
System Manager	⇆	Active Directory Server	TCP / UDP	53	dns	Name Resolution
System Manager	⇆	Active Directory Server	UDP	88	kerberos	Protocol (Kerberos V5) for authentication/user login
System Manager	⇆	Active Directory Server	UDP	123	ntp	time synchronization
System Manager	⇆	Active Directory Server	TCP	135	rpc	RPC Service
System Manager	⇆	Active Directory Server	UDP	137	netbios-ns	NetBIOS - Naming Service
System Manager	⇆	Active Directory Server	UDP	138	netbios-dgm	NetBIOS - Datagram Service
System Manager	⇆	Active Directory Server	TCP	139	netbios-ssn	NetBIOS - Session Service
System Manager	⇆	Active Directory Server	TCP	445	smb	SMB client for database backups
System Manager	⇆	Active Directory Server	TCP	464	kpasswd	Kerberos Password Change
System Manager	⇆	Active Directory Server / LDAP Server	TCP / UDP	389	ldap	LDAP authentication of OSXMP users
System Manager	⇆	Active Directory Server / LDAP Server	TCP	636	ldaps	Secured LDAPS authentication of OSXMP users
System Manager	→	OpenScape FaultManagement	UDP	162	snmp	SNMP messaging and transport
Multi Line Controller	⇆	Active Directory Server	UDP	123	ntp	time synchronization
Multi Line Controller	⇆	Active Directory Server	UDP	53	dns	Name Resolution
Multi Line Controller	⇆	System Manager	TCP	514	rsh	Remote Shell
OpenScape FaultManagement	→	System Manager	UDP	161	snmp	SNMP messaging and transport

Xpert Ports

Device A		Device B	Protocol	Port	Designation	Comments
Xpert Windows Soft Client	⇆	CTI Applications (e.g. Reichert/Häger & Busch)	TCP	9000	hte	OpenScape Xpert HTE / CTI Communication (optional)
Xpert Windows Soft Client	⇆	Multi Line Controller	TCP	9003	htems	HTEMS proprietary Protocol for Xpert Communication
Xpert Windows Soft Client	⇆	Multi Line Controller	TCP	9004	htems	HTEMS proprietary Protocol for Xpert Communication
Xpert Windows Soft Client	→	Multi Line Controller	UDP	8002 - 8021	rtp	Voice Stream to MLC
Xpert Windows Soft Client	←	Multi Line Controller	UDP	2048 - 65535	rtp	Voice Stream from MLC
Xpert Windows Soft Client	⇆	OCSP	TCP	80	http	access the URL which can be found in the certificate provided by CA
Xpert Windows Soft Client	⇆	System Manager	TCP	80	http	Client SW update via HTTP
Xpert Windows Soft Client	⇆	System Manager	TCP	443	https	Client SW update via HTTPS
Xpert Windows Soft Client	⇆	System Manager	TCP	8080	http	Client SW update via HTTP
Xpert Windows Soft Client	→	System Manager	TCP	8443	https	Client SW update via HTTPS - Request
Xpert Windows Soft Client	⇆	System Manager	TCP	9003	htems	HTEMS proprietary Protocol for Xpert Communication
Xpert Windows Soft Client	⇆	System Manager	TCP	9004	htems	HTEMS proprietary Protocol for Xpert Communication
Xpert Windows Soft Client	→	System Manager	TCP	9006	application	Java JBOSS (J2EE) Communication Port
Xpert Windows Soft Client	⇆	System Manager / Service PC	TCP / UDP	3389	rdp	Remote Desktop
Xpert Windows Soft Client	→	Thrift Applications (e.g. Reichert/Häger & Busch)	TCP	9007	thrift	new Xpert Thrift API
Xpert Windows Soft Client	←	Thrift Applications (e.g. Reichert/Häger & Busch)	TCP	10052	thrift	new Xpert Thrift API
Xpert Windows Soft Client	⇆	Voice Recorder ASC	TCP	443	https	ASC Xpert Replay
Xpert Windows Soft Client	⇆	Voice Recorder ASC	UDP	16900 - 16901	rtp	Voice Stream HTE Recording ASC - Port Assignment
Xpert Windows Soft Client	⇆	Voice Recorder Nice	UDP	10000 - 11001	rtp	Voice Stream HTE Recording Nice - Port Assignment
6010p Turret & Linux Soft Client	⇆	CTI Applications (e.g. Reichert/Häger & Busch)	TCP	9000	hte	OpenScape Xpert HTE / CTI Communication (optional)
6010p Turret & Linux Soft Client	⇆	Multi Line Controller	TCP	9003	htems	HTEMS proprietary Protocol for Xpert Communication
6010p Turret & Linux Soft Client	⇆	Multi Line Controller	TCP	9004	htems	HTEMS proprietary Protocol for Xpert Communication
6010p Turret & Linux Soft Client	→	Multi Line Controller	UDP	8002 - 8021	rtp	Voice Stream to MLC
6010p Turret & Linux Soft Client	←	Multi Line Controller	UDP	2048 - 65535	rtp	Voice Stream from MLC
6010p Turret & Linux Soft Client	⇆	OCSP	TCP	80	http	access the URL which can be found in the certificate provided by CA
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	80	http	Client SW update via HTTP
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	443	https	Client SW update via HTTPS
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	5800	vnc	Virtual network for VNC
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	5900	vnc	Virtual network for VNC
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	8080	http	Client SW update via HTTP
6010p Turret & Linux Soft Client	→	System Manager	TCP	8443	https	Client SW update via HTTPS - Request
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	9003	htems	HTEMS proprietary Protocol for Xpert Communication
6010p Turret & Linux Soft Client	⇆	System Manager	TCP	9004	htems	HTEMS proprietary Protocol for Xpert Communication
6010p Turret & Linux Soft Client	→	System Manager	TCP	9006	application	Java JBOSS (J2EE) Communication Port
6010p Turret & Linux Soft Client	←	System Manager / Service PC	TCP	22	ssh	SSH - Putty / Winscp
6010p Turret & Linux Soft Client	→	Thrift Applications (e.g. Reichert/Häger & Busch)	TCP	9007	thrift	new Xpert Thrift API
6010p Turret & Linux Soft Client	←	Thrift Applications (e.g. Reichert/Häger & Busch)	TCP	10052	thrift	new Xpert Thrift API
6010p Turret & Linux Soft Client	⇆	Voice Recorder ASC	TCP	443	https	ASC Xpert Replay
6010p Turret & Linux Soft Client	⇆	Voice Recorder ASC	UDP	16900 - 16901	rtp	Voice Stream HTE Recording ASC - Port Assignment
6010p Turret & Linux Soft Client	⇆	Voice Recorder Nice	UDP	10000 - 11001	rtp	Voice Stream HTE Recording Nice - Port Assignment
Master Tradeboard (CTI)	⇆	**all Ports of Turrets and Soft Clients +**				
Master Tradeboard (CTI)	⇆	Voice Recorder (e.g. ASC)	TCP	9000	hte	OpenScape Xpert HTE / CTI Communication
Master Tradeboard (CTI)	⇆	CTI Applications (e.g. Reichert/Häger & Busch)	TCP	9000	hte	OpenScape Xpert HTE / CTI Communication
Multi Line Controller	⇆	Multi Line Controller	UDP	2048 - 65535	rtp / srtp	Voice Stream between MLC's
Multi Line Controller	⇆	OCSP	TCP	80	http	access the URL which can be found in the certificate provided by CA
Multi Line Controller	⇆	OS4000 CSTA	UDP	32768 - 61000	csta xml	Busy Signalling of OS4000 Phones
Multi Line Controller	→	OS4000 STMIX / Softgate	TCP	5060	sip	SIP Communication with PBX
Multi Line Controller	→	OS4000 STMIX / Softgate	TCP / TLS	5061	sip	SIP TLS Communication with PBX
Multi Line Controller	←	OS4000 STMIX / Softgate	TCP	1024-65535	sip	SIP via TCP connectivity Xpert PBX - outbound proxy
Multi Line Controller	←	OS4000 STMIX / Softgate	TCP TLS	1024-65535	sip	SIP via TLS connectivity Xpert PBX - outbound proxy
Multi Line Controller	⇆	OS4000 STMIX / Softgate	UDP	16384-32764	rtp / srtp	MLC - PBX / Gateway Payload
Multi Line Controller	→	OSV / OSB	TCP	5060	sip	SIP Communication with PBX
Multi Line Controller	→	OSV / OSB	TCP / TLS	5061	sip	SIP TLS Communication with PBX
Multi Line Controller	←	OSV / OSB	TCP	1024-65535	sip	SIP via TCP connectivity Xpert PBX - outbound proxy
Multi Line Controller	←	OSV / OSB	TCP TLS	1024-65535	sip	SIP via TLS connectivity Xpert PBX - outbound proxy
Multi Line Controller	⇆	OSV / OSB	UDP	16384-32764	rtp / srtp	MLC - PBX / Gateway Payload
Multi Line Controller	→	other PBX's (Alcatel/Avaya)	TCP	5060	sip	SIP Communication with PBX
Multi Line Controller	→	other PBX's (Alcatel/Avaya)	TCP / TLS	5061	sip	SIP TLS Communication with PBX
Multi Line Controller	←	other PBX's (Alcatel/Avaya)	TCP	1024-65535	sip	SIP via TCP connectivity Xpert PBX - outbound proxy
Multi Line Controller	←	other PBX's (Alcatel/Avaya)	TCP TLS	1024-65535	sip	SIP via TLS connectivity Xpert PBX - outbound proxy
Multi Line Controller	⇆	other PBX's (Alcatel/Avaya)	UDP	16384-32764	rtp / srtp	MLC - PBX / Gateway Payload
Multi Line Controller	⇆	System Manager	TCP	80	http	MLC SW update via HTTP
Multi Line Controller	⇆	System Manager	TCP	443	https	MLC SW update via HTTPS
Multi Line Controller	⇆	System Manager	TCP	8080	http	MLC SW update via HTTP
Multi Line Controller	⇆	System Manager	TCP	9003	htems	HTEMS proprietary Protocol for Xpert Communication
Multi Line Controller	⇆	System Manager	TCP	9004	htems	HTEMS proprietary Protocol for Xpert Communication
Multi Line Controller	←	System Manager / Service PC	TCP	22	ssh	SSH - Putty / Winscp
Multi Line Controller	←	Turrets and Soft Clients	UDP	8002 - 8021	rtp / srtp	Voice Stream from Turrets and Soft Clients
Multi Line Controller	→	Turrets and Soft Clients	UDP	2048 - 65535	rtp / srtp	Voice Stream to Turrets and Soft Clients
Multi Line Controller	→	Voice Recorder	UDP	2048 - 65535	rtp / srtp	Voice Stream Payload
Multi Line Controller	→	Voice Recorder ASC	TCP	5060	sip	SIP Communication with Voice Recorder
Multi Line Controller	→	Voice Recorder ASC	TCP / TLS	5061	sip	SIP TLS Communication with Voice Recorder
Multi Line Controller	←	Voice Recorder ASC	TCP	1024-65535	sip	SIP via TCP Communication with Voice Recorder SIPRec - outbound proxy
Multi Line Controller	←	Voice Recorder ASC	TCP / TLS	1024-65535	sip	SIP via TLS Communication with Voice Recorder SIPRec - outbound proxy
Multi Line Controller	→	Voice Recorder ASC	UDP	16900 >	rtp	Voice Stream HTE Recording ASC
Multi Line Controller	→	Voice Recorder Nice	UDP	10000 >	rtp	Voice Stream HTE Recording Nice
Multi Line Controller	→	Voice Recorder Verint	UDP	16900 >	rtp	Voice Stream HTE Recording Verint
System Manager	⇆	6010p Turret & Linux Soft Client	TCP	5800	vnc	Virtual network for VNC
System Manager	⇆	6010p Turret & Linux Soft Client	TCP	5900	vnc	Virtual network for VNC
System Manager	⇆	System Manager	TCP	3306	mysql	MYSQL DB Cluster Replication
System Manager	⇆	System Manager	TCP	8443	https	OpenScape Xpert Management Portal access via HTTPS
System Manager	⇆	System Manager / Turrets and Soft Clients	TCP	9003	htems	HTEMS proprietary Protocol for Xpert Communication - Cluster Failover
System Manager	⇆	System Manager / Turrets and Soft Clients	TCP	9004	htems	HTEMS proprietary Protocol for Xpert Communication - Cluster Failover
System Manager	⇆	System Manager	TCP	9010	thrift	Communication to Remote License Server (SM-SM, usually primary SM)
System Manager	←	Turrets and Soft Clients	TCP	9006	application	Java JBOSS (J2EE) Communication Port
System Manager	⇆	Unify SWS	TCP	447	https	V7R1 Query from SWS server - it is based on that if software download required or not
Xpert Image Server	→	6010p Turret & Linux Soft Client	TCP	22	ssh	Xpert Linux Image Transfer
Xpert Image Server	←	System Manager	TCP	22	ssh	SSH - Putty / Winscp
Xpert Image Server	⇆	System Manager	TCP	80	http	SW update via HTTP
Xpert Image Server	⇆	System Manager	TCP	443	https	SW update via HTTPS
Xpert Image Server	⇆	System Manager	TCP	8080	http	SW update via HTTP
MediaStar Evolution	⇆	Turrets and Soft Clients	TCP	554	rtsp	Real Time Streaming Protocol for MediaStar Evolution IPTV
MediaStar Evolution	→	Turrets and Soft Clients	UDP	4444	IPTV	Video Stream Standard Port for MediaStar Evolution IPTV
MediaStar Evolution	⇆	Turrets and Soft Clients	UDP	15947	rtsp	Real Time Streaming Protocol for MediaStar Evolution IPTV
MediaStar Evolution	⇆	Turrets and Soft Clients	IGMP		igmp	IGMP Multicast Groups
OSX Management PC	⇆	System Manager OSXMP	TCP	8443	https	OpenScape Xpert Management Portal access via HTTPS
CTI Application e.g. Häger & Busch	⇆	Turrets and Soft Clients	TCP	9000	hte	OpenScape Xpert HTE / CTI Communication
CTI Application e.g. Häger & Busch	⇆	Turrets and Soft Clients	TCP	443	https	OpenScape Xpert Management Portal access via HTTPS
CTI Application e.g. Häger & Busch	←	Turrets and Soft Clients	TCP	9007	thrift	new Xpert Thrift API
CTI Application e.g. Häger & Busch	→	Turrets and Soft Clients	TCP	10052	thrift	new Xpert Thrift API
Reichert Radio Gateway	⇆	Turrets and Soft Clients	TCP	8081	http	Reichert Web GUI (changeable)
Reichert Radio Gateway	⇆	Turrets and Soft Clients	TCP	9003	hte	OpenScape Xpert HTE / CTI Communication
LDAP Server	⇆	System Manager / Turrets and Soft Clients	TCP	389	ldap	LDAP authentication of OSXMP users
LDAP Server	⇆	System Manager / Turrets and Soft Clients	TCP	636	ldaps	Secured LDAPS authentication of OSXMP users

Index

M

N

O

P

Q

R

S

T

U

V

W