A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

Installation Configuration and Migration V10

Installation Guide
07/2024

A31003-H31A0-J100-18-7620

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 Preparations

1.1 Prerequisites

- Information regarding documentation: All documents that are available on E-Doku are also available on the Unify Partner Portal. If you don't have access to E-Doku please use the Partner Portal.
- No other application is allowed to run co-located on the machine (e.g. virus scan) (see also Section 1.2, "Use of 3rd Party Products").
- Please check Chapter 2, "OpenScape 4000 Deployments" in OpenScape 4000, Feature Description book for information regarding hardware compatibility of OpenScape 4000 software.
- Use the security checklist to adopt / to check the required security settings for each product.

1.2 Use of 3rd Party Products

Use of 3rd Party Software on OpenScape 4000

- It is not allowed to install 3rd Party Software on OpenScape 4000. OpenScape 4000 uses the Appliance Model for the Linux operating system. This means only the necessary operating system components are used, which not only streamlines the system - making it more efficient, but also more secure. Required SUSE Linux operating system updates will be applied as part of our Fix Release/Hot Fix concept.
- Anti-virus scanner or other intrusion detection systems are also not allowed. The following are the reasons for this:
  - The server is already a low-profile target for viruses, worms and other intruders because it is Linux-based and not Windows-based, its firewall configurations and carefully controlled administrative access minimize its susceptibility.
  - Running such scanners can cause a significant increase in server CPU usage, invalidating other capacity calculations. A corporate policy that requires virus scanners on all computers is not appropriate to enforce on this type of specialized server; it is recommended that a waiver be sought from such a policy.

  Instead, it is more appropriate to scan the software prior to installation.

1.3 Connecting a Service PC to the System

If no keyboard, mouse and monitor is available a service PC can be connected via USB to the EcoServer and EcoBranch.

To connect a service PC the following preparations must be performed.

1.3.1 USB drivers and read me

The WHQL USB drivers are needed for USB1 console installation on EcoServer and EcoBranch.

IMPORTANT: Unify takes no responsibility for the use/ installation of these USB drivers and provides the only latest WHQL drivers upon time of image creation from the manufacturer's website.

For console (terminal emulation) access, see `USB_INSTALL_README.png`. This file is part of the ISO and is located in the path `\DriversAndTools \USB_Driver\`.

Actual drivers should be downloaded from the manufacturer's website directly and will not be supplied with the OpenScape 4000 ISO file:

EcoServer/EcoBranch:

http://www.ftdichip.com/Drivers/VCP.htm

Reported Driver Install Issues

Some problems have been reported where the newly installed USB devices show up with a yellow exclamation mark under Windows Device Manager. In those cases, right click the device under Windows Device Manager and under the Features tab assign a previous unused COM Port e.g. COM 10 & COM 11.

1.3.2 BIOS settings

NOTICE: With BIOS version 4 and higher no changes must be performed in the BIOS settings.

There are three possibilities of how the BIOS can be configured in the **BIOS MENU**. Under **Advanced Remote Access > Configuration** and the **Redirection after BIOS POST** must match, if not black text can be displayed on a black background!

Terminal Type=ANSI -Colour Redirection after BIOS POST=Boot Loader Putty Settings Recommendation: The Backspace Key "Control-H" Function Keys and Keypad "ESC)n~"

Terminal Type=VT100 -Black and White only. Redirection after BIOS POST=Always Putty Settings Recommendation: The Backspace Key "Control-H" Function Keys and Keypad "VT100"

Terminal Type=VT-UTF8 -Recommend and will become BIOS default. Redirection after BIOS POST=Boot Loader Putty Settings Recommendation: The Backspace Key "Control-H" Function Keys and Keypad "Linux"

NOTICE: Keyboard/Terminal emulation parameters may need to be adjusted dependent on configuration.

Now you can connect your Service PC to the EcoServer/EcoBranch, as follows:

- Connect a service PC to the USB1 interface of the EcoServer/EcoBranch board.

Figure 1: TAP connection at EcoServer

Figure 2: TAP connection at EcoBranch

- Configure the first new COM port from that. Install with 115200, 8, None, 1.

Important Information

- Terminal Emulation Program
- A terminal emulation program is needed for the installation/configuration via USB console port (e.g. HyperTerminal/Putty/TeraTerm). ComWin is not sufficient because it does not support the required terminal emulation to enter the BIOS. Putty is recommended, because this is most often used also for SSH connections.
- SB drivers are needed the from the manufacturer for USB1 console installation.

  ATOS takes no responsibility for the use/installation of the USB drivers and recommends only latest WHQL drivers.

  Actual drivers should be downloaded from the manufacturer's website directly and will not be supplied with the OpenScape4000 ISO:

  – EcoServer:

    http://www.ftdichip.com/Drivers/VCP.htm
  – EcoBranch:

    http://www.ftdichip.com/Drivers/VCP.htm

1.3.3 Service access over Management port

NOTICE: The purpose of management ethernet is for trouble shooting cases to connect directly to the internal vLAN Switch/

Bridge. A PC can be connected directly and will get an IP address assigned out of the internal IP segment.

WARNING: A permanent connection of the management port to an IT network (e.g. management network) is not allowed, nor connectivity to other EcoServer as it will influence system stability.

- Configuration

  On selected HW platforms (EcoServer and EcoBranch) there is a special ethernet port available on the back of the box, marked with the sign of the wrench, so called management port. This port can be used for service access to the Web Based Management, Comwin, Assistant, Portal, CSTA and SSH of 4k system.

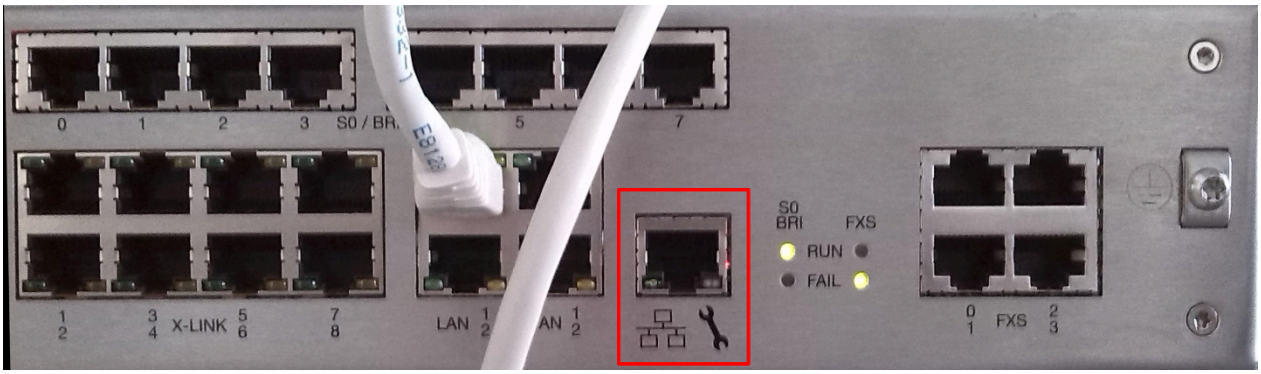


Figure 3: Management port on OpenScape 4000 EcoBranch

By default this service access feature of the management port is enabled. It can be switched on/off in the Portal LAN wizard, section Internal LAN, checkbox "Enable Management Port (eth10)". Please mind that this

checkbox is present only when the hardware EcoServer or EcoBranch is detected.

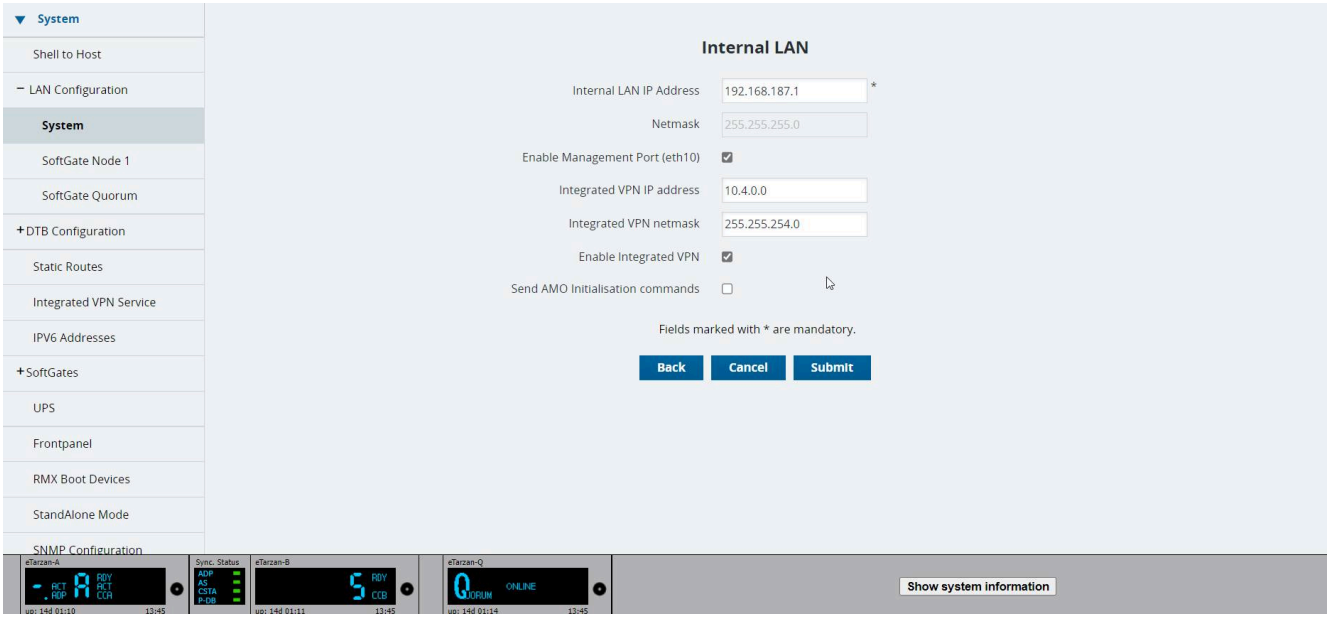


Figure 4: Management port activation checkbox

You can check the status of the management port on the blue LCD display, page "Mgmt Port":

Figure 5: LCD display showing management port status - Enabled / Disabled

NOTICE: After connecting the Service PC to Management port on the LCD display you will see 'Connected' instead of 'Enabled' (Mngt port page from Display is not refreshed automatically).

- Usage

1) Check on the LCD display if the management port is enabled.
2) Using ethernet cable interconnect your laptop and the management port.
3) Set your network card configuration to get the IP address through DHCP.
4) Wait until you are given the IP address from the DHCP server. Management port shares the same address subnet as the Internal LAN. The default ILAN settings is 192.168.187.100-150, netmask 255.255.255.0. You will be leased the IP address from this range.
5) Now you can access the services over the web browser, Comwin or SSH client on the Internal LAN addresses of Portal, Assistant and CSTA. These addresses are displayed on the LCD display.

1.4 Default settings for Logins and Network Configuration

EcoServer and EcoBranch are delivered with a preinstalled appliance software with the following default settings for logins and network configuration.

- Logins:

  NOTICE: The first time you login, you will be requested to change the default password. The password of OpenScape 4000 Assistant is also used for OpenScape 4000 Platform Administration (Portal).

  Table 1: Default settings for Logins

Application	User	Password
Linux / RMX	root	hicom
Linux	linuser	hicom
OpenScape 4000 Platform Administration (Portal) / OpenScape 4000 Assistant	engr	4K-admin
OpenScape 4000 CSTA	root	4K-admin
CSTA CBAdmin	Admin	Admin

- Network configuration:

  Table 2: Default settings for network configuration

Interface LAN 1 - eth0	IP Address
physical IP	192.168.0.2 / 24
OpenScape 4000 Platform Administration (Portal)	192.168.0.3 / 24
Default GW / Router	192.168.0.1

- After the image installation is done, a standard server will start in multi user mode with Networking (init 3).

  IMPORTANT: OpenScape 4000 systems are only allowed to run in Linux run level 3 (init3).

2 First Installation

IMPORTANT: First Installation without XML is no longer supported starting with V10R1.

2.1 Important Information

IMPORTANT: The installation procedure checks the available disk space on the hard disk and determines the possible deployments. For more information regarding the needed hard disk size refer to Section 2.2.3.1, "Possible Deployment depending on the Hard Disk Size".

IMPORTANT: If a physical LAN separation is not possible and infrastructure components are used to connect nodes (e.g. network switches), then traffic from the different interfaces (Customer, IPDA, Corosync, Atlantic LANs) must be separated via VLANs. This can be done either in the infrastructure components themselves or in the OpenScape 4000 network configuration.

Deployment	Options	DSCXL2/DSCXL2+ S30122-K7732-X S30122-X8004-X39	OSA500 S30807-U6649-X100-11 S30807-U6649-X101 S30807-U6649-X101-G1 S30807-U6649-X101-8 S30807-U6649-X300-11 S30807-U6649-X301 S30807-U6649-X301-H1 S30807-U6649-X101-9	VMware®	OS 4000 EcoServer S30122-K7754-X S30122-K7754-X100 S30122-K7754-X200	OS 4000 Branch S30122-K7758-X	OS EcoServer (ECO2) S30122-K7760-X	OS EcoBranch (Branch2) S30122-K7761-X
Simplex	without SoftGate	n/r	n/r	✓	✓ [1]	n/r	✓ [1]	n/r
	with SoftGate	n/r	✓	✓ [2]	✓ [1]	✓ [1]	✓ [1]	✓ [1]
Duplex	Duplex	n/r	n/p	n/p	✓	n/p	✓	n/p
	with SoftGate	n/p	n/p	n/p	✓ [2] [5]	n/p	✓ [2] [5]	n/p
Separated Duplex (GSD)	Node A & B	n/r	n/r	✓	✓	n/r	✓	n/r
	Node A & B with SoftGate	n/p	n/r	n/r	✓ [2] [5]	n/r	✓ [2] [5]	n/r
	Quorum	n/r	✓	✓	✓	✓	✓	✓
	Quorum with SoftGate	n/r	✓	✓ [2]	✓	✓	✓	✓
APE		✓[4]	n/p [3]	n/p [3]	n/p [3]	n/p [3]	n/p [3]	n/p [3]
Survivable	without SoftGate	n/r	✓	✓	✓ [1]	✓ [1]	✓ [1]	✓ [1]
	with SoftGate	n/p	✓	✓ [2]	✓ [1]	✓ [1]	✓ [1]	✓ [1]
Standalone SoftGate	Standalone SoftGate	n/r	✓	✓ [2]	n/r	✓	n/r	✓
Enterprise Gateway	without SoftGate	n/p	n/p	n/p	✓ [1]	n/p	✓ [1]	n/p
	with SoftGate	n/p	n/p	n/p	✓ [1][2]	n/p	✓ [1][2]	n/p
Survivable Enterprise Gateway	without SoftGate	n/p	n/p	n/p	✓ [1]	n/p	✓ [1]	n/p
	with SoftGate	n/p	n/p	n/p	✓ [1][2]	n/p	✓ [1][2]	n/p
Manager		n/p	n/p	✓	n/p	n/p	✓	n/p

✓ = possible

n/p = not possible; The firstinst-netw.sh blocks the installation. Portal LAN Wizard configuration not possible .

n/r = not released; The firstinst-netw.sh allows the installation, but a warning is displayed. Portal LAN Wizard configuration is allowed, but a warning is displayed.

[1] Installation/Activation of Hosted OpenScape Session Border Controller (hSBC) is supported

[2] Xlink connectivity to Access modules is not supported for VMware deployments, or hosted SoftGates (meaning iSG on Enterprise Gateways and node A or B of Duplex/GSD)

[3] For APE select Survivable deployment and don't configure the SoftGate.

[4] The DSCXL HW will be discontinued starting with SW version V10R1.

[5] Starting with V10R1

Figure 6: OpenScape 4000 V10 Deployment Matrix

2.2 Installation and Configuration Steps

With Remote Major Update process a central host system running HiPath 4000 V7R2 can be updated to OpenScape 4000 V10 from remote.

This process involves using a second system of the same hardware type as the remote system for preparing and creating a Recovery ISO Image containing the OpenScape 4000 V10 R1 Software plus complete system configuration.

This ISO Image will be then transferred to the remote host system and used for the remote major update process.

NOTICE: Starting with V10R1, Remote Major Update (RMU) is no longer supported.

2.2.1 Planning of IP Addresses/Deployment

First the configuration of the infrastructure has to be planned. It depends on the network structure and includes the IP addresses of the OpenScape 4000 system.

2.2.1.1 Host Name

Prepare a valid unique host name (the hostname must start with a letter, can include a letter, a digit or a hyphen, and must not end with a hyphen):

In case of duplex/separated duplex scenarios separate host names are necessary for all nodes.

Please note that in case of simplex the system hostname will be set by the hostname assigned to the customer interface and in case of Duplex deployments by the corosync hostname.

IMPORTANT: Please note that if the hostname begins with a digit it causes failure to the loading of the pre-configured node.

2.2.1.2 Corosync LAN

IMPORTANT: Corosync LAN must not be configured for Single node deployment!

Choose the host name(s) for the Corosync LAN (must be the same as the machine's host name).

Host name for the Corosync LAN must be different to the host name of the Customer LAN.

e.g. soco2-sys1, soco2-sys2 and soco2-quorum

There is no requirement for the Domain name to differ though.

2.2.1.3 Customer and IPDA LAN are located in the same Subnet or in Different Subnets

Check if Customer LAN and IPDA LAN are located in the same subnet or in different subnets.

Customer LAN and IPDA LAN are located in the same subnet

IMPORTANT: If Customer LAN and IPDA LAN are located in the same subnet (e.g. 218.1.17.0 /24), then the same physical interface (e.g. eth0) must be used for both. It is strictly forbidden to use different interfaces as it would lead to routing problems.

- Customer LAN and IPDA LAN

  Choose the host name(s) for the Customer LAN/IPDA LAN.

  For Duplex deployments, hostname for the Customer LAN/IPDA LAN must be different to the host name of the Corosync LAN.

  e.g. soco2-sys1-cust, soco2-sys2-cust and soco2-quorum-adm

  Customer LAN and IPDA LAN are located in different subnets

  IMPORTANT: If Customer LAN and IPDA LAN are located in different subnets (e.g. customer LAN 218.1.17.0 /24 and IPDA LAN 172.16.2.0 /24), then two separate physical interfaces (e.g. eth0 and eth2) have to be used.

- Customer LAN

  Choose the host name(s) for the Customer LAN.

  For Duplex deployments, hostname for the Customer LAN must be different to the host name of the Corosync LAN.

  e.g. soco2-sys1-cust, soco2-sys2-cust and soco2-quorum-adm
- IPDA LAN

  Choose the host name(s) for the IPDA LAN.

  e.g. soco2-sys1-ipda and soco2-sys2-ipda

  For Duplex deployments, hostname for the IPDA LAN must be different to the hostname of the Corosync LAN.

2.2.1.4 IP Addresses

- Every IP address has to be unique.
- The physical network cards of Customer and IPDA LAN need unique IP addresses.
- It is not allowed to use any other IP address as physical address, e.g. CCA/CCB.
- Supernetting is not supported for the IPDA interfaces.

2.2.1.5 Atlantic LAN

Previously adjacent pairs e.g. 6&7 were used for Atlantic LAN interface, but this was not aligned with our recommandation for bonding in case the customer wants to configure bonds later on.

2.2.1.6 Planning Tables

Empty planning tables for your infrastructure planning can be found in Chapter 9, "Appendix A: Tables for Infrastructure Planning".

An example for each deployment can be found in the following sections:

- Simplex
- Simplex with Integrated SoftGate
- Duplex
- Separated Duplex
- Separated Duplex with Integrated SoftGate
- APE
- Standalone SoftGate
- Survivable
- Enterprise GW
- Survivable Enterprise Gateway

Simplex

IMPORTANT: The following examples are valid for OpenScape 4000 software running on EcoServer and EcoBranch.

Example: Customer LAN and IPDA LAN are located in one subnet

Table 3: Simplex: Infrastructure planning - Customer and IPDA LAN in one subnet

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1
OpenScape 4000 Platform Administration (Portal)	218.1.17.102		

OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
CCA	218.1.17.105		
Default Gateway/Router	218.1.17.254		
NGS	218.1.17.107		
ETH5 & ETH6LAN	Atlantic		

Example: Customer LAN and IPDA LAN are located in separate subnets

Table 4: Simplex: Infrastructure planning - Customer and IPDA LAN in separate subnets

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust
OpenScape 4000 Platform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
Default Gateway/Router	218.1.17.254		
ETH2	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda
CCA	172.16.2.105		
Default Router	172.16.2.254		
NGS	172.16.2.107		
ETH5 & ETH6	Atlantic LAN		

Simplex with Integrated SoftGate

IMPORTANT: Only "direct link" OpenScape 4000 Softgate can be integrated in Simplex server deployments.

Example: Customer LAN and IPDA LAN are located in one subnet

Table 5: Simplex with integrated OpenScape 4000 SoftGate: Infrastructure planning - Customer and IPDA LAN in one subnet

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname

phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1
OpenScape 4000 Platform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
CCA	218.1.17.105		
NGS	218.1.17.107		
Default Gateway/Router	218.1.17.254		
	SoftGate Configuration Data		
NCUI	218.1.17.123		
AP internal IP (DL)	192.168.1.23	255.255.255.0	
ETH5 & ETH6	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in separate subnets

Table 6: Simplex with integrated OpenScape 4000 SoftGate: Infrastructure planning - Customer and IPDA LAN in separate subnets

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1
OpenScape 4000 Platform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
Default Gateway/Router	218.1.17.254		
ETH2	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda
CCA	172.16.2.105		
NGS	172.16.2.107		
Default Router	172.16.2.254		
	SoftGate Configuration Data		
vNCUI	172.16.2.108		
AP internal IP (DL)	192.168.1.23	255.255.255.0	

ETH5 & ETH6	Atlantic LAN

Duplex

Example: Customer LAN and IPDA LAN are located in one subnet

Table 7: Duplex: Infrastructure planning - Customer and IPDA LAN in one subnet

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP Node 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust
phys. IP Node 2 (YaST)	218.1.17.101		soco2-sys2-cust
OpenScape 4000 Platform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
CCA	218.1.17.105		
CCB	218.1.17.106		
NGS	218.1.17.107		
Default Gateway/Router	218.1.17.254		
ETH4	Corosync LAN		
	IP Address	Netmask	Hostname
phys. IP Node 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1
phys. IP Node 2 (YaST)	10.1.187.2		soco2-sys2
ETH5 & ETH6	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in separate subnets

Table 8: Duplex: Infrastructure planning - Customer and IPDA LAN in separate subnets

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP Node 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust
phys. IP Node 2 (YaST)	218.1.17.101		soco2-sys2-cust
OpenScape 4000 Platform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		

Default Gateway/Router	218.1.17.254		
ETH2	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP Node 1 (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda
phys. IP Node 2 (YaST)	172.16.2.101		soco2-sys2-ipda
CCA	172.16.2.105		
CCB	172.16.2.106		
NGS	172.16.2.107		
Default Router	172.16.2.254		
ETH4	Corosync LAN		
	IP Address	Netmask	Hostname
Interface			
phys. IP Node 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1
phys. IP Node 2 (YaST)	10.1.187.2		soco2-sys2
ETH5 & ETH6	Atlantic LAN		

Separated Duplex

Example: Customer LAN and IPDA LAN are located in one subnet

Table 9: Separated Duplex: Infrastructure planning - Customer and IPDA LAN in one subnet

Customer & IPDA LAN				
	IP Address	Netmask	Hostname	Interface
OpenScape 4000 Platform Administration (Portal)	218.1.17.102			
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
CCA	218.1.17.105			
CCB	218.1.17.106			
NGS	218.1.17.107			
Default Gateway/ Router	218.1.17.254			

phys. IP Node 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/ VLAN100
phys. IP Node 2 (YaST)	218.1.17.101		soco2-sys2-cust	
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
Corosync LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/ VLAN300
phys. IP Node 2 (YaST)	10.1.187.2		soco2-sys2	
phys. IP Quorum (YaST) [1]	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				
				Interface
Interface				ETH5/ BOND3
Interface				ETH6/ BOND3

Example: Customer LAN and IPDA LAN are located in separate subnets

Table 10: Separated Duplex: Infrastructure planning - Customer and IPDA LAN in separate subnets

Customer LAN				
	IP Address	Netmask	Hostname	Interface
OpenScape 4000 Platform Administration (Portal)	218.1.17.102			
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
Default Gateway/ Router	218.1.17.254			

[1] For Quorum a suitable interface can be chosen, e.g. eth0

phys. IP Node 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/ VLAN100
phys. IP Node 2 (YaST)	218.1.17.101		soco2-sys2-cust	
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
IPDA LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda	ETH2/ BOND1/ VLAN200
phys. IP Node 2 (YaST)	172.16.2.101		soco2-sys2-ipda	
CCA	172.16.2.105			
CCB	172.16.2.106			
NGS	172.16.2.107			
Default Router	172.16.2.254			
Corosync LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/ VLAN300
phys. IP Node 2 (YaST)	10.1.187.2		soco2-sys2	
phys. IP Quorum (YaST) [2]	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				
				Interface
Interface				ETH5/BOND3
Interface				ETH5/BOND3

Separated Duplex with Integrated SoftGate

NOTICE: The SoftGate feature "SIP Load Balancer" is not supported for this scenario. (The "SIP Load Balancer" feature can be used only in a "SoftGate Standalone" deployment).

Example: Customer LAN and IPDA LAN are located in one subnet

[2] For Quorum a suitable interface can be chosen, e.g. eth0

Table 11: Separated Duplex: Infrastructure planning - Customer and IPDA LAN in one subnet

Customer & IPDA LAN				
	IP Address	Netmask	Hostname	Interface
OpenScape 4000 Platform Administration (Portal)	218.1.17.102			
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
CCA	218.1.17.105			
CCB	218.1.17.106			
NGS	218.1.17.107			
Default Gateway/ Router	218.1.17.254			
phys. IP Node 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/ VLAN100
phys. IP Node 2 (YaST)	218.1.17.101		soco2-sys2-cust	
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
	SoftGate Configuration Data			
vNCUI	218.1.17.108			
AP internal IP (DL)	192.168.1.23	255.255.255.0		
Corosync LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/ VLAN300
phys. IP Node 2 (YaST)	10.1.187.2		soco2-sys2	
phys. IP Quorum (YaST) [3]	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				
				Interface

[3] For Quorum a suitable interface can be chosen, e.g. eth0

Interface		ETH5/BOND3
Interface		ETH6/BOND3

Example: Customer LAN and IPDA LAN are located in separate subnets

Table 12: Separated Duplex: Infrastructure planning - Customer and IPDA LAN in separate subnets

Customer LAN				
	IP Address	Netmask	Hostname	Interface
OpenScape 4000 Platform Administration (Portal)	218.1.17.102			
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
Default Gateway/ Router	218.1.17.254			
phys. IP Node 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/ VLAN100
phys. IP Node 2 (YaST)	218.1.17.101		soco2-sys2-cust	
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
IPDA LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda	ETH2/ BOND1/ VLAN200
phys. IP Node 2 (YaST)	172.16.2.101		soco2-sys2-ipda	
CCA	172.16.2.105			
CCB	172.16.2.106			
NGS	172.16.2.107			
Default Router	172.16.2.254			
	SoftGate Configuration Data			
vNCUI	172.16.2.108			
AP internal IP (DL)	192.168.1.23	255.255.255.0		

Corosync LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/ VLAN300
phys. IP Node 2 (YaST)	10.1.187.2		soco2-sys2	
phys. IP Quorum (YaST) [4]	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				
				Interface
Interface				ETH5/BOND3
Interface				ETH5/BOND3

APE

Example: Customer LAN and IPDA LAN are located in one subnet

IMPORTANT: The NGS IP address entered for the APE must be the same IP address the one entered on the host system.

Table 13: APE: Infrastructure planning - Customer and IPDA LAN in one subnet

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	APE-23
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCAP (APESU of host system)	218.1.17.115		
NGS (of the host)	218.1.17.117		
Default Gateway/Router	218.1.17.254		
	IP address of the host system		
CCA	218.1.17.105		
ETH5 & ETH6	Atlantic LAN		

[4] For Quorum a suitable interface can be chosen, e.g. eth0

Example: Customer LAN and IPDA LAN are located in separate subnets

Table 14: APE : Infrastructure planning - Customer and IPDA LAN in separate subnets

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	APE-23
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
Default Gateway/Router	218.1.17.254		
ETH2	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	172.16.2.110	255.255.255.0	APE-23-ipda
CCAP (APESU of host system)	172.16.2.115		
NGS (of the host)	172.16.2.117		
Default Gateway/Router	172.16.2.254		
	IP address of the host system		
CCA	172.16.2.105		
ETH5 & ETH6	Atlantic LAN		

Standalone SoftGate

NOTICE: On OpenScape 4000 EcoBranch there are two redundant LAN/WAN ports. All settings and functions are the same as OpenScape Access.

NOTICE: OpenScape 4000 Platform Administration (Portal) configuration is optional in some deployments. If the IP address for OpenScape 4000 Platform Administration (Portal) is not configured it can be reach on the NCUI IP address: **https://<ncui_ip_address>:8443)**

Example: Customer LAN and IPDA LAN are located in one subnet -direct link

Table 15: Standalone SoftGate: Infrastructure planning - Customer and IPDA LAN in one subnet -direct link

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	SoftGate Configuration Data		
vNCUI	218.1.17.123		
AP internal IP (DL)	198.168.1.23	255.255.255.0	
	IP address of the host system		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in one subnet - network link

Table 16: Standalone SoftGate: Infrastructure planning - Customer and IPDA LAN in one subnet - network link

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	SoftGate Configuration Data		
vNCUI	218.1.17.123	255.255.255.0	
	IP address of the host system		
CCA	172.16.2.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in separate subnets - direct link

Table 17: Standalone SoftGate: Infrastructure planning - Customer and IPDA LAN in separate subnets - direct link

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	172.16.2.110	255.255.255.0	OpenScapeAccess-ipda
Default Gateway/Router	172.16.2.254		
	SoftGate Configuration Data		
vNCUI	172.16.2.123		
AP internal IP (DL)	198.168.1.23	255.255.255.0	
	IP address of the host system		
CCA	172.16.2.105		

Example: Customer LAN and IPDA LAN are located in separate subnets - network link

Table 18: Standalone SoftGate: Infrastructure planning - Customer and IPDA LAN in separate subnets - network link

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	172.168.2.110	255.255.255.0	OpenScapeAccess-ipda
Default Gateway/Router	172.168.2.254		
	SoftGate Configuration Data		

vNCUI	172.168.2.123	255.255.255.0	
	IP address of the host system		
CCA	172.16.2.105		

Survivable

NOTICE: On OpenScape 4000 EcoBranch there are two redundant LAN/WAN ports. All settings and functions are the same as OpenScape Access.

IMPORTANT: Some conditions require a new installation of the software on the OSA500. If the OSA500 is planned to be used as Survivable SoftGate, then the installed system (Platform) must have the same basic version (MinorRelease/ FixRelease version) as the OpenScape 4000, e.g. if switch is R0.6.0 then the OSA500 has to be installed with R0.6.0. Else the OpenScape Backup & Restore from Assistant (HBR) for AP-Emergency will fail. This is normal behaviour and not an error (known from APE and Backup & Restore). The opposite is also possible i.e. when the switch has a lower version than the delivered OSA500 preinstalled software. In this case the switch has to be upgraded, before activating the synchronization over HBR.

Example: Customer LAN and IPDA LAN are located in one subnet -direct link

Table 19: Survivable: Infrastructure planning -Customer and IPDA LAN in one subnet -direct link

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU of host system)	218.1.17.115		
NGS (of the host)	218.1.17.117		
	SoftGate Configuration Data		
vNCUI	172.16.2.123		
AP internal IP (DL)	192.168.1.23	255.255.255.240	

	IP address of the host system		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in one subnet - network link

Table 20: Survivable: Infrastructure planning -Customer and IPDA LAN in one subnet -network link

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU of host system)	218.1.17.115		
NGS (of the host)	172.16.2.117.117		
	IP address of the host system		
CCA	172.16.2.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in separate subnets - direct link

Table 21: Survivable: Infrastructure planning - Customer and IPDA LAN in separate subnets -direct link

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		

phys. IP (YaST)	172.16.2.110	255.255.255.0	Surv-OpenScapeAccess-ipda
CCA (APESU of host system)	172.16.2.115		
NGS (of the host)	172.16.2.112		
Default Gateway/Router	172.16.2.254		
	IP address of the host system		
CCA	172.16.2.105		

Example: Customer LAN and IPDA LAN are located in separate subnets - network link

Table 22: Survivable: Infrastructure planning - Customer and IPDA LAN in separate subnets -network link

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		
phys. IP (YaST)	172.16.2.110	255.255.255.0	Surv-OpenScapeAccess-ipda
CCA (APESU of host system)	172.16.2.115		
NGS (of the host)	192.168.20.112		
Default Gateway/Router	172.16.2.254		
	IP address of the host system		
CCA	172.16.2.105		

Enterprise GW

Example: Customer LAN and IPDA LAN are located in one subnet -direct link

Table 23: Enterprise GW: Infrastructure planning - Customer and IPDA LAN in one subnet -direct link

ETH0	Customer & IPDA LAN

	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	Enterprise GW Configuration Data		
Enterprise GW (synonymous with vNCUI)	218.1.17.123		
AP internal IP (DL)	198.168.1.23	255.255.255.0	
	IP address of the host system		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in one subnet - network link

Table 24: Enterprise GW: Infrastructure planning - Customer and IPDA LAN in one subnet -network link

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	Enterprise GW Configuration Data		
Enterprise GW (synonymous with vNCUI)	218.1.17.123	255.255.255.0	
	IP address of the host system		
CCA	172.16.2.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in separate subnets - direct link

Table 25: Enterprise GW: Infrastructure planning - Customer and IPDA LAN in separate subnets -direct link

ETH0	Customer LAN

	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	172.16.2.110	255.255.255.0	EnterpriseGWipda
Default Gateway/Router	172.16.2.254		
	SoftGate Configuration Data		
Enterprise GW (synonymous with vNCUI)	172.16.2.123		
AP internal IP (DL)	198.168.1.23	255.255.255.0	
	IP address of the host system		
CCA	172.16.2.105		

Example: Customer LAN and IPDA LAN are located in separate subnets - network link

Table 26: Enterprise GW: Infrastructure planning - Customer and IPDA LAN in separate subnets - network link

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Platform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	172.168.2.110	255.255.255.0	EnterpriseGWipda
Default Gateway/Router	172.168.2.254		
	OpenScape 4000 SoftGate Configuration Data		
Enterprise GW (synonymous with vNCUI)	172.168.2.123	255.255.255.0	

	IP address of the host system		
CCA	172.16.2.105		

Survivable Enterprise GW

Example: Customer LAN and IPDA LAN are located in one subnet -direct link

Table 27: Survivable Enterprise GW: Infrastructure planning -Customer and IPDA LAN in one subnet - direct link

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU of host system)	218.1.17.115		
NGS (of the host)	218.1.17.117		
	Enterprise GW Configuration Data		
Enterprise GW (synonymous with vNCUI)	172.16.2.123		
AP internal IP (DL)	192.168.1.23	255.255.255.240	
	IP address of the host system		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in one subnet - network link

Table 28: Survivable Enterprise GW: Infrastructure planning -Customer and IPDA LAN in one subnet - network link

ETH0	Customer & IPDA LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		

OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU of host system)	218.1.17.115		
NGS (of the host)	172.16.2.117.117		
	IP address of the host system		
CCA	172.16.2.105		
ETH1	Atlantic LAN		

Example: Customer LAN and IPDA LAN are located in separate subnets - direct link

Table 29: Survivable Enterprise GW: Infrastructure planning - Customer and IPDA LAN in separate subnets -direct link

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW
OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		
phys. IP (YaST)	172.16.2.110	255.255.255.0	SurvEnterpriseGWipda
CCA (APESU of host system)	172.16.2.115		
NGS (of the host)	172.16.2.112		
Default Gateway/Router	172.16.2.254		
	IP address of the host system		
CCA	172.16.2.105		

Example: Customer LAN and IPDA LAN are located in separate subnets - network link

Table 30: Survivable Enterprise GW: Infrastructure planning - Customer and IPDA LAN in separate subnets -network link

ETH0	Customer LAN		
	IP Address	Netmask	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW

OpenScape 4000 Platform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		
phys. IP (YaST)	172.16.2.110	255.255.255.0	SurvEnterpriseGWipda
CCA (APESU of host system)	172.16.2.115		
NGS (of the host)	192.168.20.112		
Default Gateway/Router	172.16.2.254		
	IP address of the host system		
CCA	172.16.2.105		

2.2.2 HowTo write bootable 4K ISO Image on USB Stick

Prerequisites: 8GB Stick or bigger, but not bigger than 32GB.

For USB stick handling users can choose their preferred handling, whereby both unetbootin and rufus tools have been successfully verified.

- Unetbootin should use a minimum version of unetbootin-windows-585.exe, because checksum issues were noted with earlier versions.
- HPUSBDisk no longer works from Windows 10 and can no longer be delivered due to licensing reasons. A "how to" for Windows formatting can be found on the ISO under the following path: `<ISO_Root_Dir>\DriversAndTools\USB_Flash_Tools \HowTo_write_bootable_4K_ISO_Image_on_USB_Stick.txt`
- Rufus tool (not delivered on the installation ISO) offers both formatting and ISO burning functionalities. Minimum lab verified version was V2.11.

> **IMPORTANT:** Make sure to select "FAT32" as Filesystem. If the USB Stick is already formatted with NTFS please reformat with FAT32. For USB stick handling users can choose their preferred handling, whereby both unetbootin and rufus have been successfully verified.

Example:

1) Start the unetbootin-windows-625.exe program and
   - select the DiskImage option
   - leave the "ISO" option selected
   - use the "..." button to browse and select the 4K Installation ISO
   - under "Type" leave selected the "USB Drive" option
   - under "Drive" make sure you select the USB Stick Drive

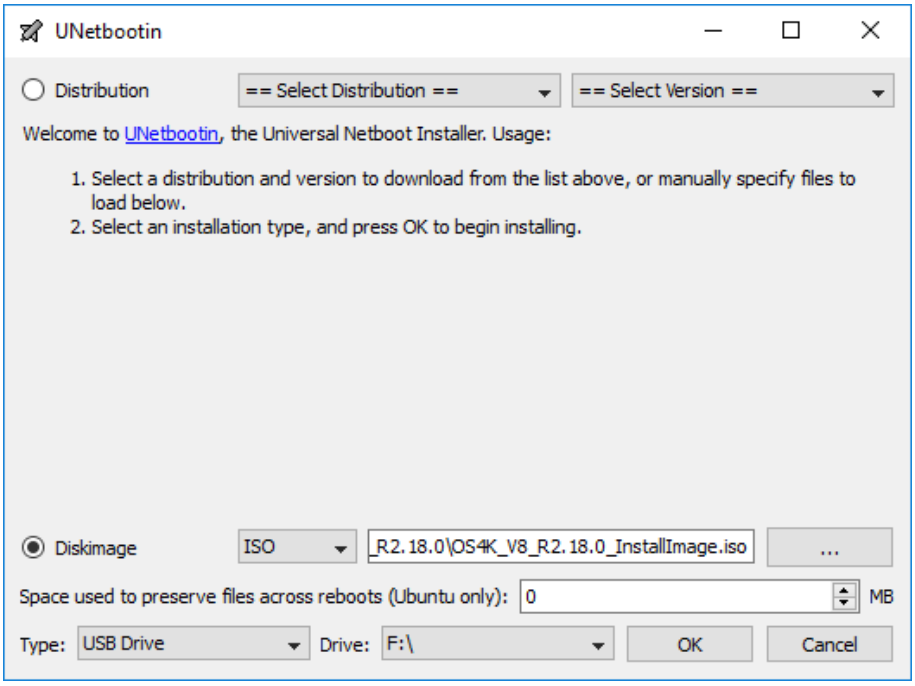


Figure 7: Universal Netboot Installer (UNetbootin)

   - press OK
   - wait until the process is finished
   - press Exit
2) Use the "Safely Remove Hardware" to remove the stick
3) Remove the stick after you get the message that you can remove it safely

2.2.3 Installation and OpenScape 4000 Configuration

This section contains the description of the

1) installation and
2) configuration of OpenScape 4000.

All these steps are configured in a XML file and then started and performed automatically.

NOTICE: In order to migrate from the old hardware to the new hardware, the XML from the existing system must be generated and the old MAC must be replaced with the MAC from the new hardware.

2.2.3.1 Possible Deployment depending on the Hard Disk Size

Table 31: Possible deployment depending on the hard disk size

Possible Deployment	Hard Disk Size [GB]		
	>= 250	75 - 250	30 - 75 (*)
All deployments	x	---	---
Standalone SoftGate[5]	x	x	---
Quorum	x	x	x

NOTICE: (*) No longer supported in V10R1.

2.2.3.2 Preparation

1) Collect one MAC address of any LAN interface from the hardware which is to be installed.
2) Fill in the XML configuration file.

   Please refer to Section 10.3, "XML Configuration File" for information on the XML file.

   Templates and examples of different XML configuration files for all deployment types are included in XML Config File Generator (under File > Load Examples), available with the latest ComWin release.
3) Copy the completely filled in XML file(s) into the folder **config** on the installation media.

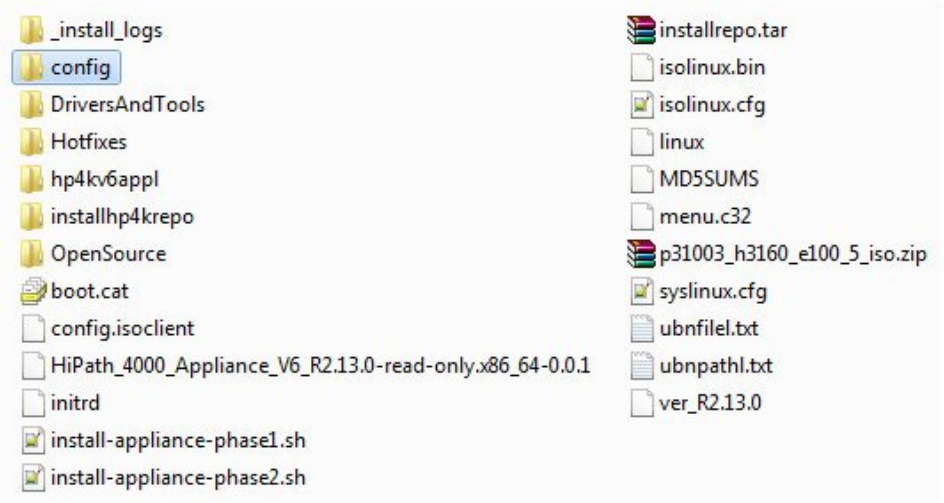


Figure 8: XML file location on installation media

This is the case for the following deployments:

[5] applies also for SoftGate on Quorum

- Standalone OpenScape 4000 SoftGate
- Simplex with integrated OpenScape 4000 SoftGate (can be installed on OSA500, ESX-VMware, EcoServer and EcoBranch)
- OpenScape Access 500/OpenScape 4000 EcoBranch
- Survivable OpenScape 4000 SoftGate
- OpenScape Access 500/OpenScape 4000 EcoBranch with Survivable OpenScape 4000 SoftGate

NOTICE: For manual OpenScape 4000 SoftGate configuration (no intialcfg file/softGateInitialConfiguration section in the configuration XML file) please refer to Section 2.3, "Manual OpenScape 4000 SoftGate Configuration".

2.2.3.3 Preparations for HotFix Installations

It is possible to transfer and or activate one or more Hotfixes as part of the first installation process.

Here are the types of HotFixes and the supported actions for each of them:

Table 32: Types of HotFixes and their supported actions

HotFix Type	Supported Actions
Assistant HotFix	Automatic activation (default), manual activation
CSTA HotFix	Automatic activation (default), manual activation
Loadware HotFix	Automatic activation
RMX HotFix	Automatic activation (default), manual activation
Platform HotFix	Automatic activation

In order to include one or more HotFixes in the installation process, these must be copied into the HotFixes folder on the installation media. The ZIP/TAR HotFix files must not be extracted. They have to be copied to /Hotfixes onto the installation media as downloaded from SWS. Make sure that the following line is included in the *.xml installation file:

<hfActivationFlags>assistantHF=auto, cstaHF=auto, rmxHF=auto</hfActivationFlags>

For Assistant and CSTA HotFixes it is possible to chose that they will be just transferred to the System without automatic activation (referred to in above table as "manual activation").

In case of manual activation, the HotFix(es) will appear in the Assistant Software Activation GUI after the OpenScape4000 Installation process and all other automatic HotFix activations have finished.

2.2.3.4 First installation with Auto GENDB

Starting V8 R1 it is possible to use a RMX REGEN file to automatically generate the RMX DB during the FI process.

The format of the REGEN File is same as the System outputs when AMO STA-REGEN is used.

A CODEW can be present in the REGEN File, otherwise the Grace Period CODEW generated by Assistant will be used.

The RMX generation will be started only after the Assistant Installation. The status and progress can be checked in the Platform Portal UI in the menu Status -> "Installation Status"

USB Installations:

The RMX REGEN File must be copied to the USB Stick in the "config" directory next to the first installation XML and it must contain in the name a MAC address matching one LAN interface of the System and the extension ".samtxt", i.e. like this:

<MAC-address>.samtxt

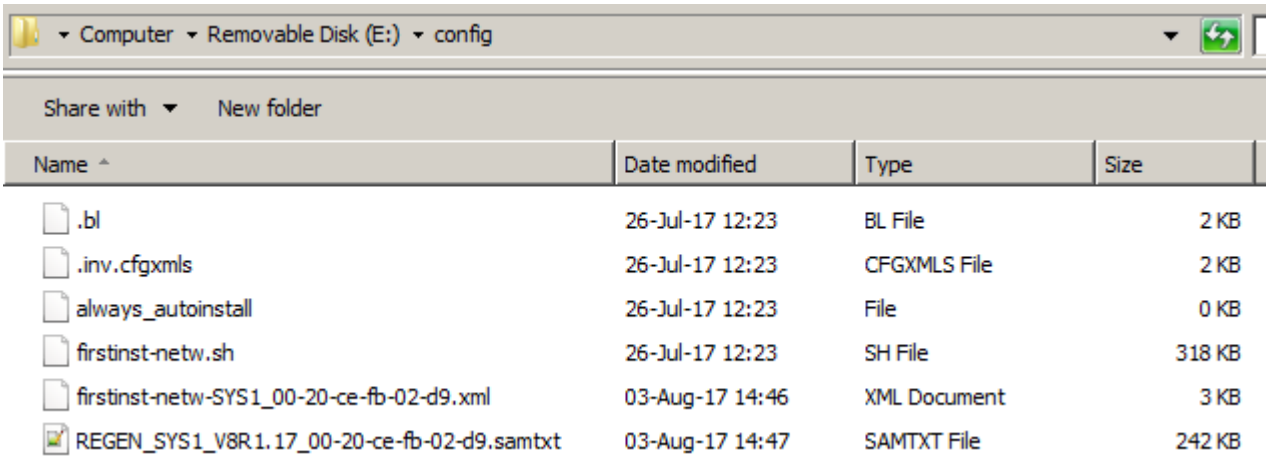


Figure 9: RMX REGEN File - "config" directory

First installation XML and REGEN file names must not contain spaces.

VMware ESXi installations:

In case of virtual machine installations, the RMX REGEN file must be placed inside the floppy image.

NOTICE: Because of the floppy image size restrictions the REGEN file must be additionally compressed in ZIP format and must have the extension ".samtxt.zip", i.e. file name must be like this: *<MAC-address>*.samtxt.zip

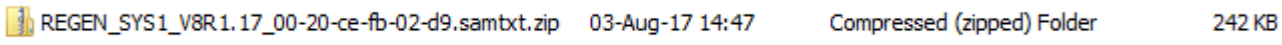


Figure 10: RMX REGEN File - floppy image

NOTICE: For floppy usage, please see the following chapters: Service PC on page 81 and Preparations on the Service PC on page 89.

2.2.3.5 Installation procedure using monitor/keyboard

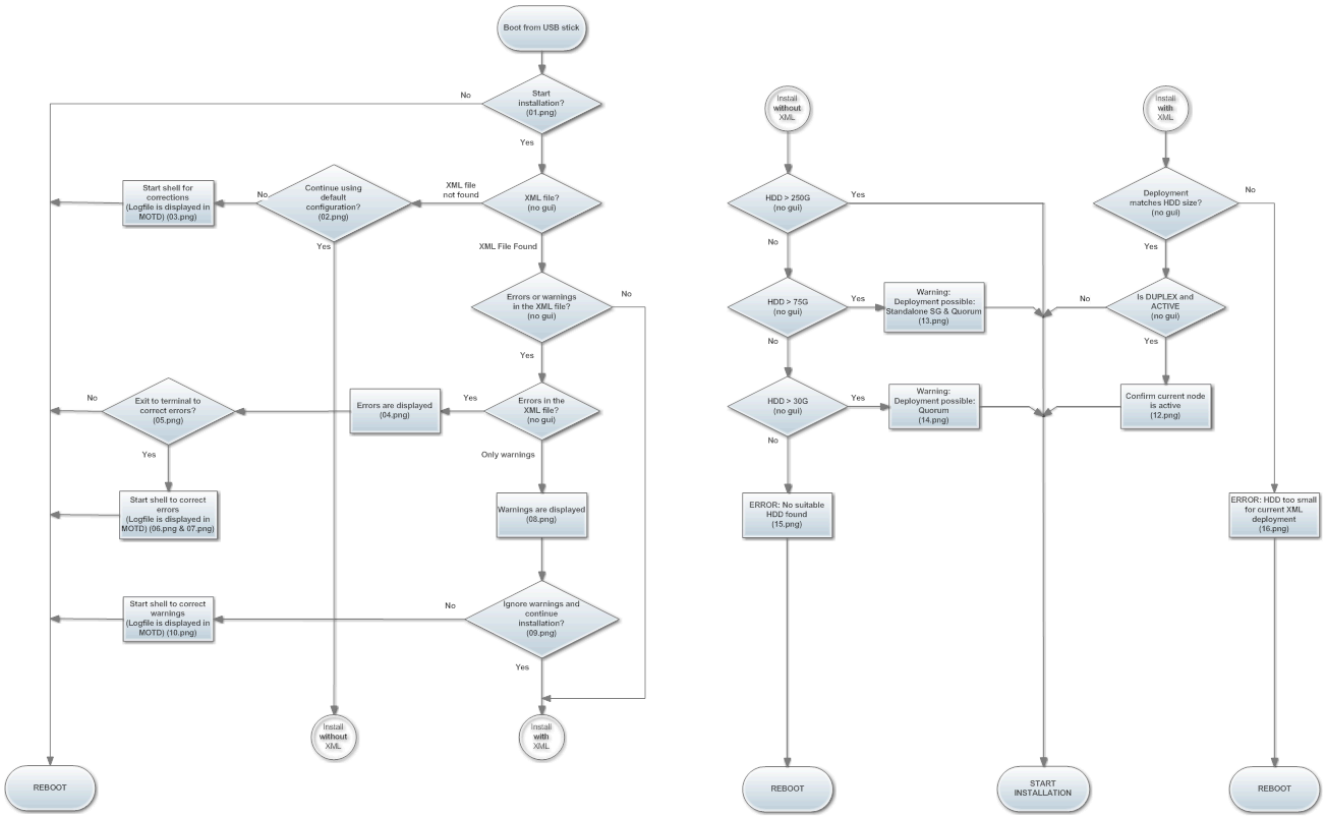


Figure 11: Installation procedure overview

1) Enter the boot menu to select the boot device.

- EcoServer / EcoBranch: F11 direct, F11 console

2) Please be aware when using F11 to choose the boot device from BIOS that the used USB device can be presented twice i.e. once with UEFI prefix and once without. The boot device without UEFI prefix should be selected.

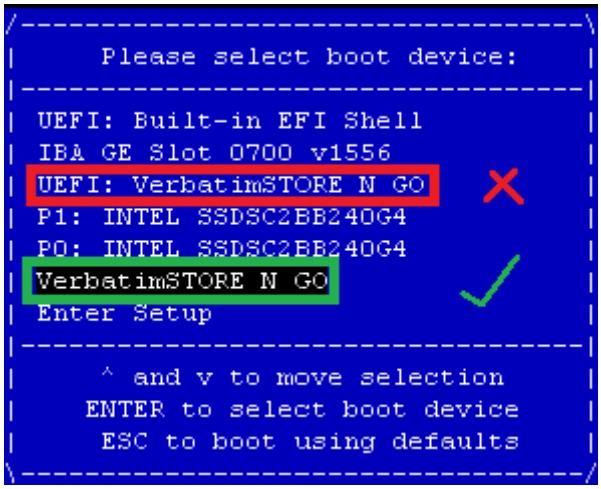


Figure 12: BIOS Boot device selection

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

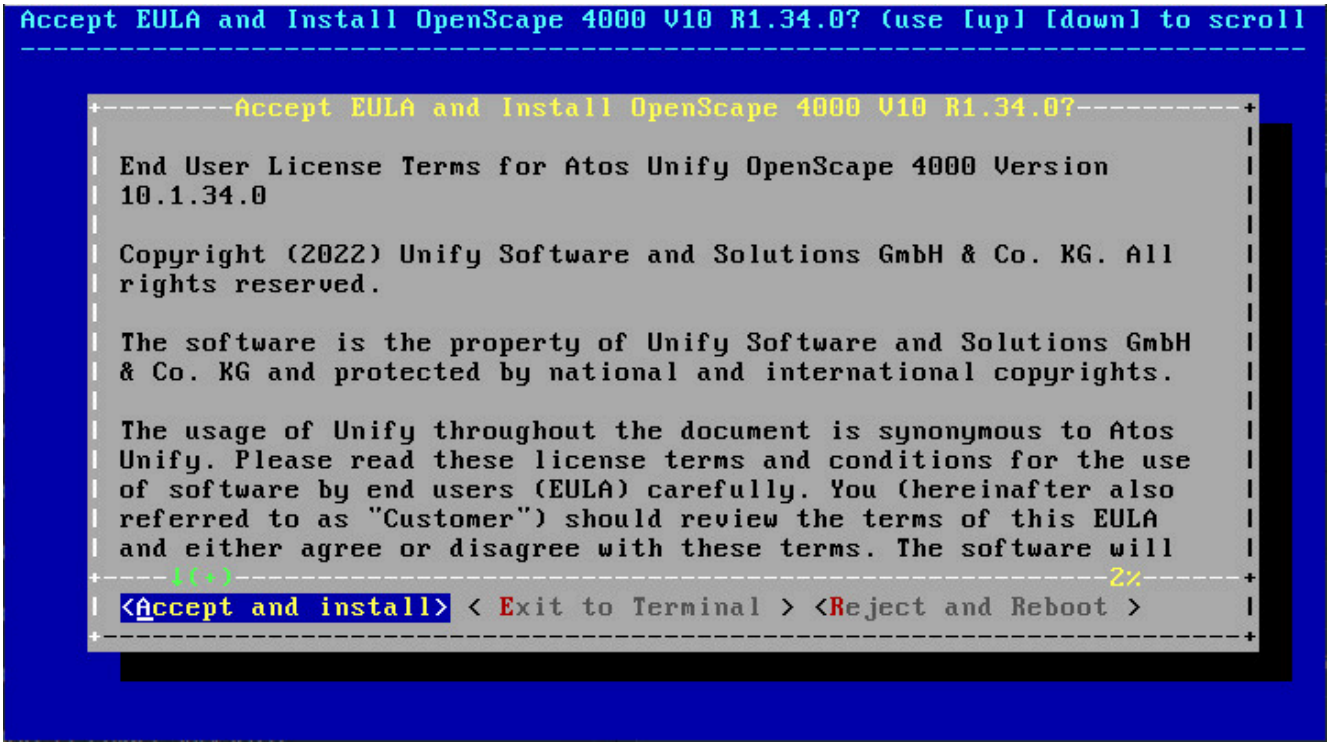


Figure 13: Boot from the installation media (USB stick)

4) Check if a compatible XML configuration file is available

If you choose **Yes** (start the installation) a check on the installation media in the folder **config** is executed in order to check if a compatible XML configuration file for the hardware is found.

Case 1: XML configuration file found

If a XML configuration file is found containing a MAC address from one of the systems interface that XML file will be checked for errors regarding Linux configuration data.

Case 1-1: XML configuration file contains no errors/warnings

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

For more information please refer to 5.

Case 1-2: XML configuration file contains errors

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

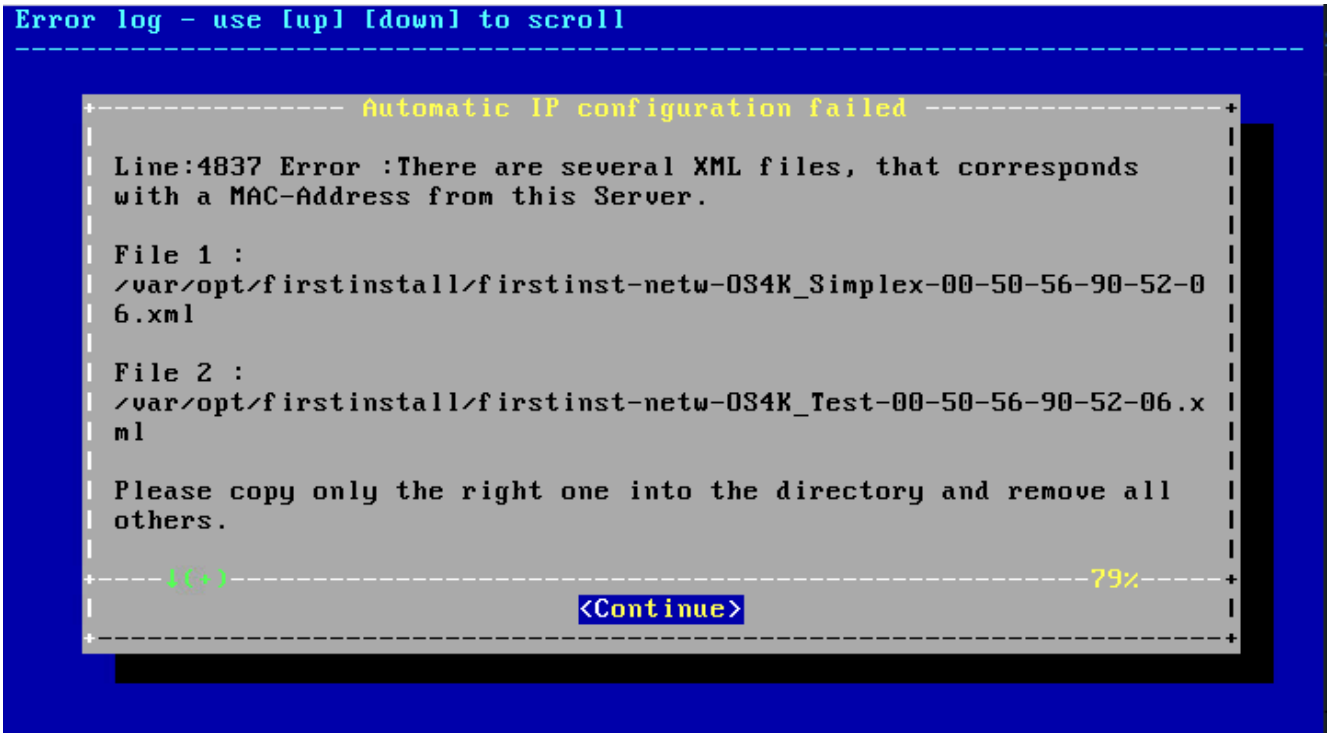


Figure 14: First installation - XML configuration file with errors

Press **Continue**.

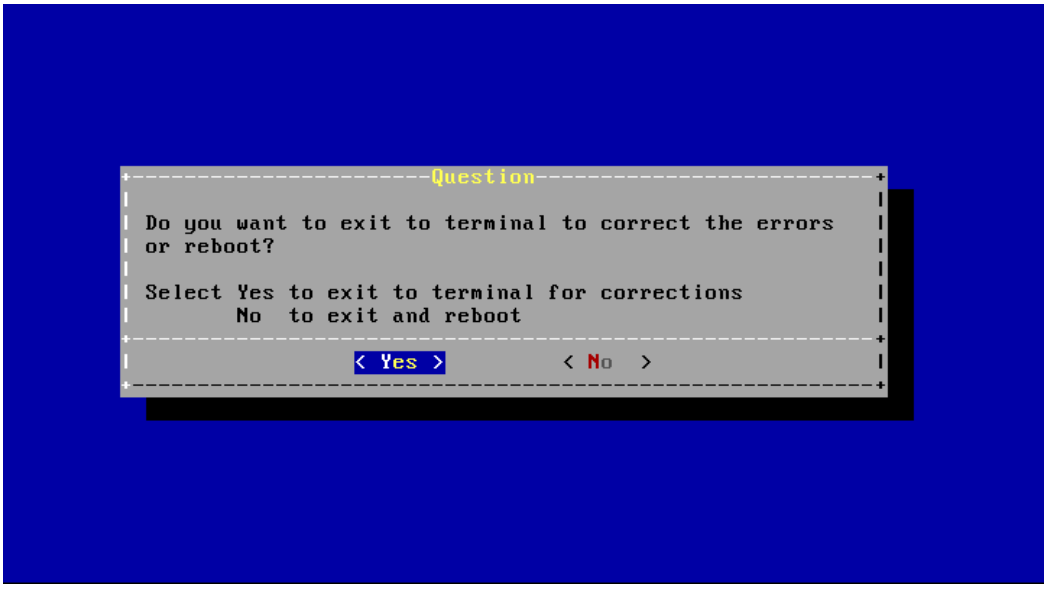


Figure 15: First installation - XML configuration file with errors

Select **Yes** to exit to the terminal for doing the corresponding corrections and then perform a reboot or **No** to exit the installation and reboot.

In case of **Yes** the log file is displayed.

Examples:

1. More than one XML configuration file that corresponds with a MAC address from this server:

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

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

File 1 : /var/opt/firstinstall/firstinst-netw-OS4K_Simplex.xml

File 2 : /var/opt/firstinstall/firstinst-netw-OS4K_Test.xml

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

Line:4935  Warning : Softgate Initial Config file is missing in
/var/opt/firstinstall/.


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

/dev/null
linux-openscape-v10:/livecd/config # _
```

Figure 16: First installation - log file for a XML configuration file with error messages

2. Wrong deployment in XML configuration file

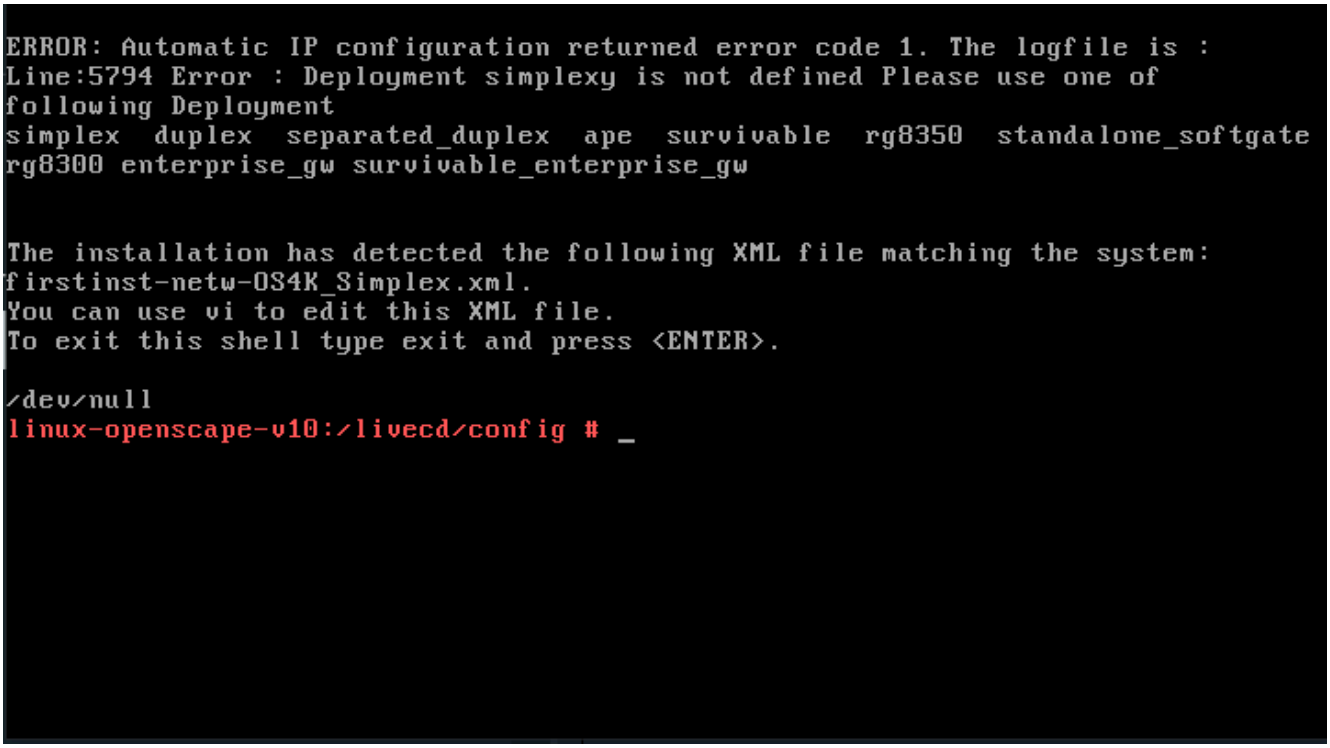


Figure 17: First installation - log file for a XML configuration file with error messages

Case 1-3: XML configuration file contains warnings

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

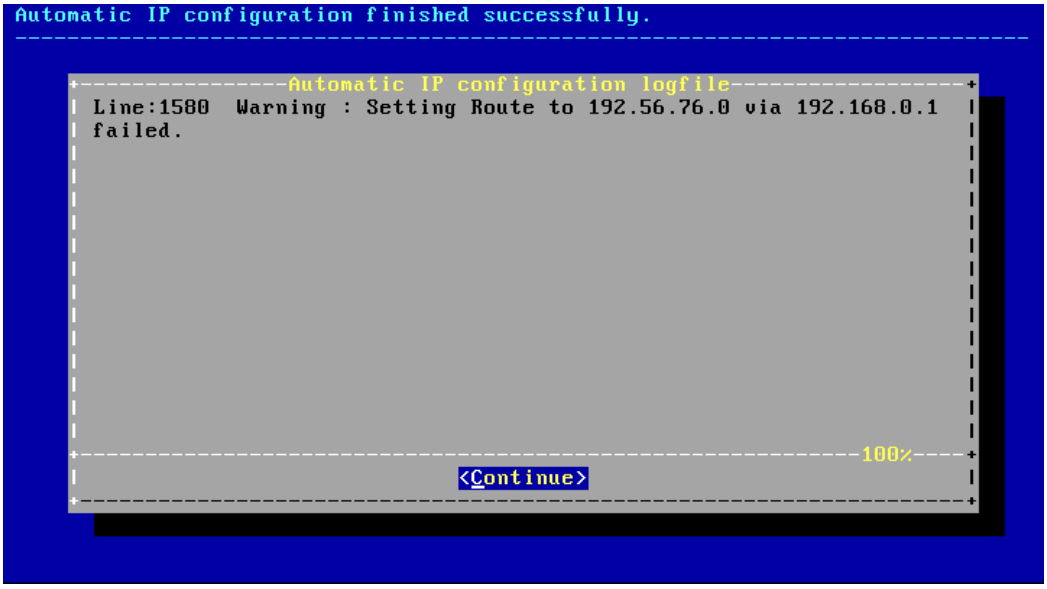


Figure 18: First installation - XML configuration file with warnings

After pressing **Continue** the following screen appears:

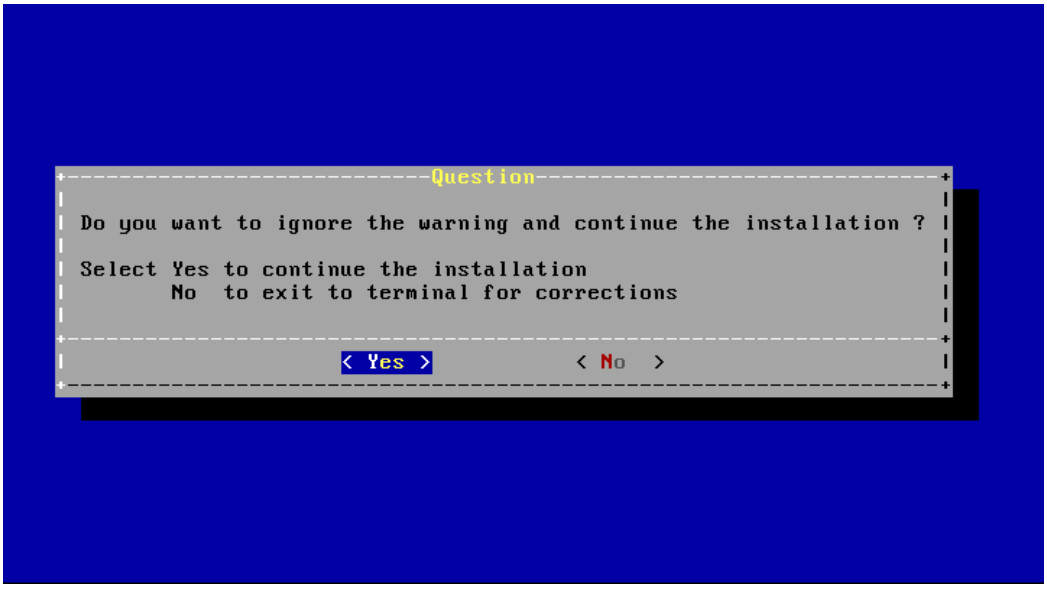


Figure 19: First installation - XML configuration file with warnings

You can select **Yes** for ignoring the warning and continuing the installation or select **No** to exit the installation and open a terminal session for doing the corresponding corrections.

If you select **Yes** the installation procedure now checks the available disk space on the hard disk and determines if the deployment matches the hard disk space.

For more information please refer to 5.

If you choose **No** the following screen appears:

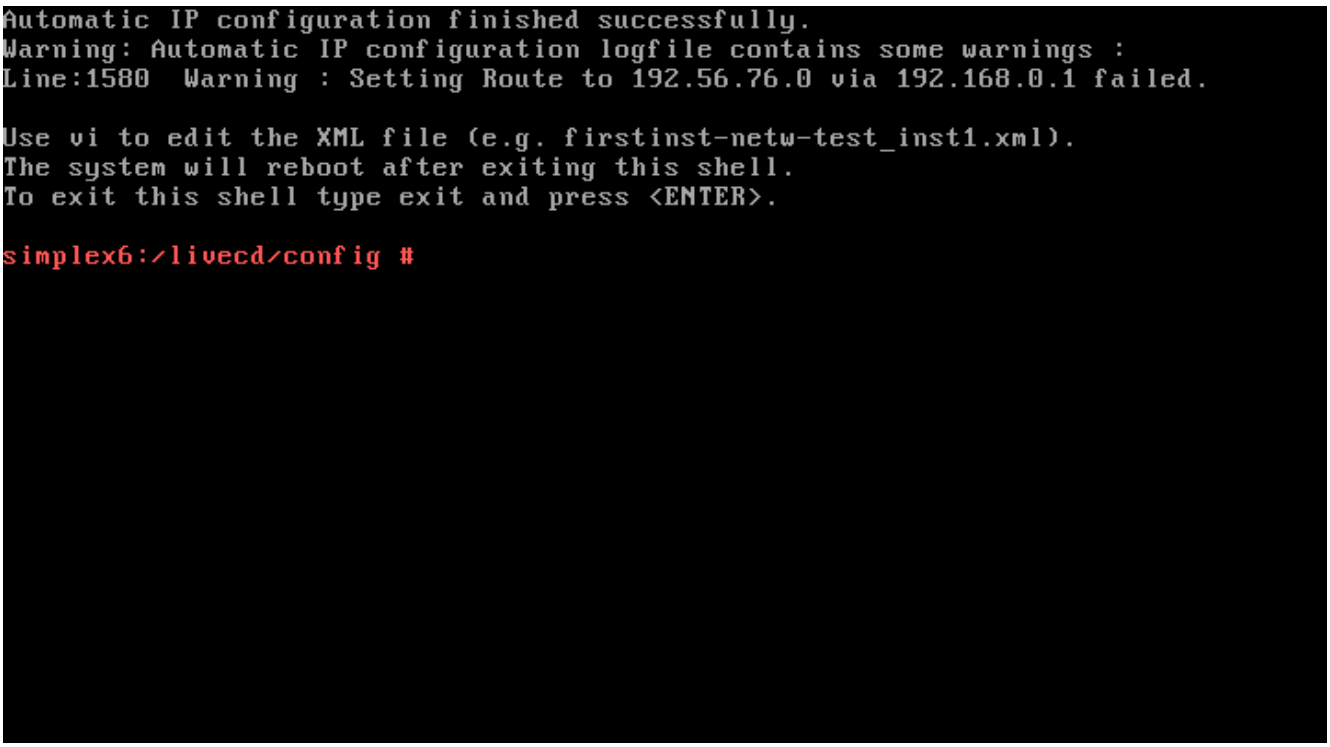


Figure 20: First installation - Log file for a XML configuration file with warnings

Case 2: No XML configuration file found

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

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

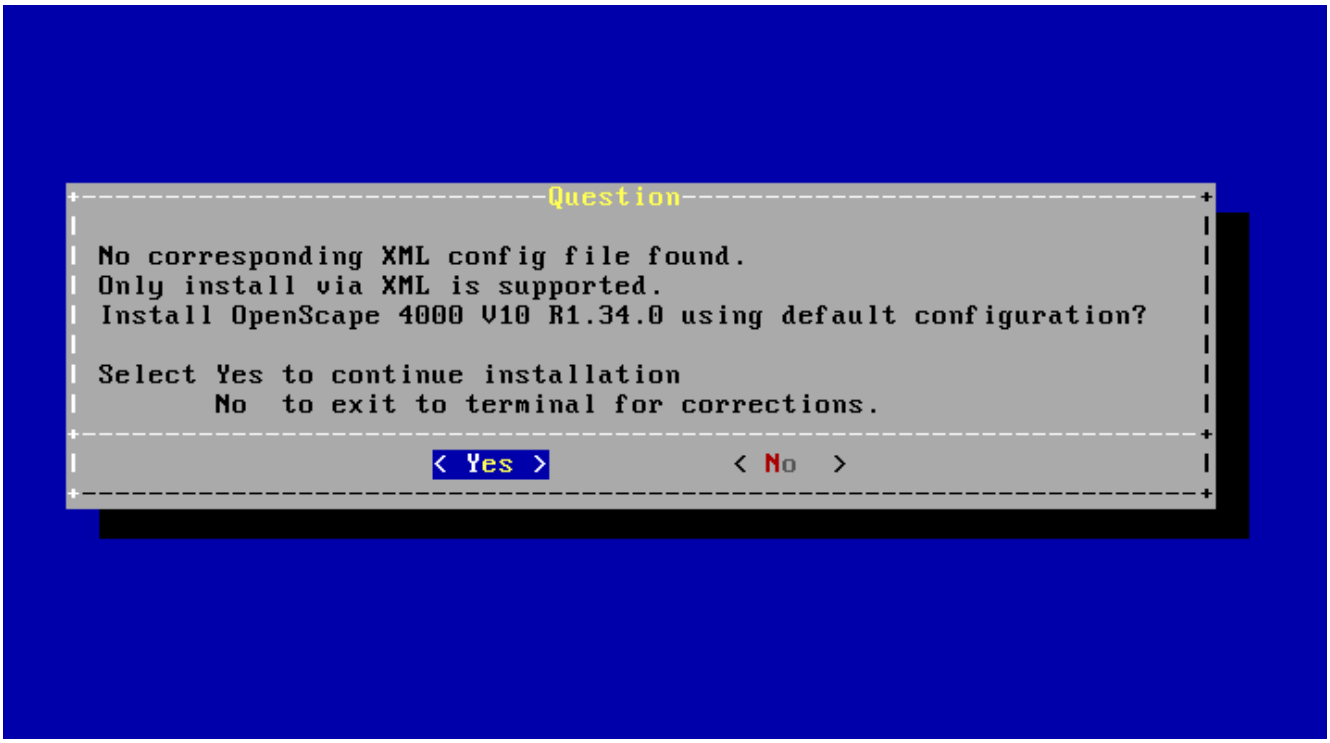


Figure 21: First installation - XML configuration file not found

Starting with V10, installation without xml is no longer supported.

NOTICE: Check if the .xml file exists in the right path and if yes then if it contains the correct MAC address of the node. To edit the .xml file you can use the vi editor.

5) Checking of available disk space

Case 1: Installation with XML configuration file: Deployment matches hard disk size?

Case 1-1: Deployment matches hard disk size

If the hard disk is suitable for the deployment of the XML configuration file then it will be checked if the current deployment is a Duplex or Separated Duplex deployment (see 6).

Case 1-2: Deployment doesn't matches hard disk size

If the hard disk is too small for the deployment of the XML configuration file then the following error message appears and a reboot will be performed.

Figure 22: First installation - Hard disk size doesn't match deployment

Case 2: Installation without XML configuration file: Hard disk size?

Case 2-1: Hard disk size is at least 250 GB

All deployments are possible and the installation will be started.

Case 2-2: Hard disk size between 75 GB and 250 GB

Only the deployments Standalone SoftGate, SoftGate on Quorum and Quorum are possible and the following warning appears.

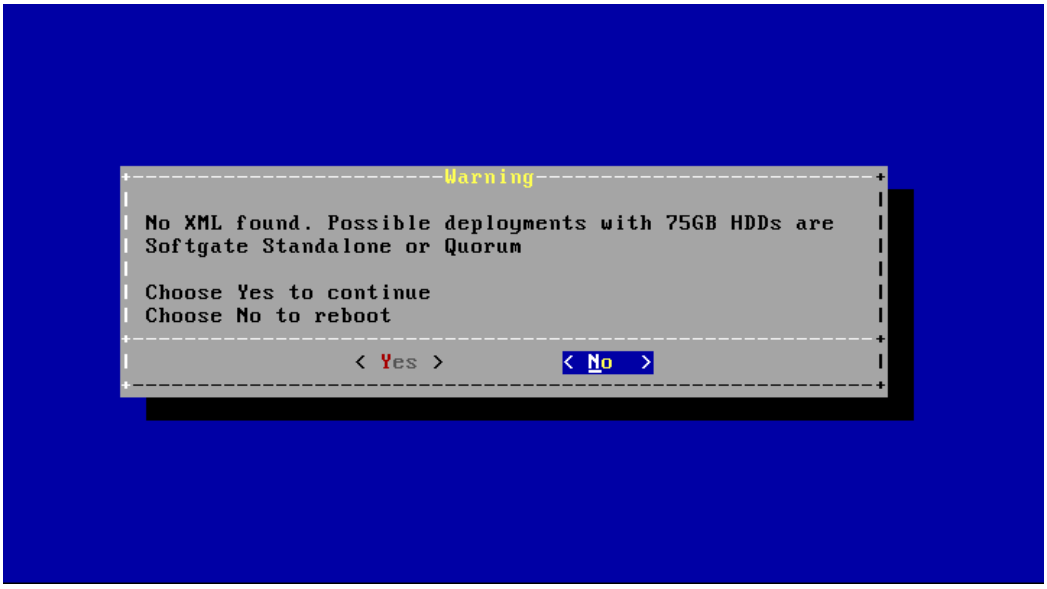


Figure 23: First installation - Deployments with hard disk between 75 GB and 250 GB

If the deployment of the XML configuration file matches the determined hard disk size then select **Yes** and the installation will be started. Otherwise choose **No** and a reboot will be performed.

Case 2-3: Hard disk size between 30 GB and 75 GB

The only possible deployment is Quorum.

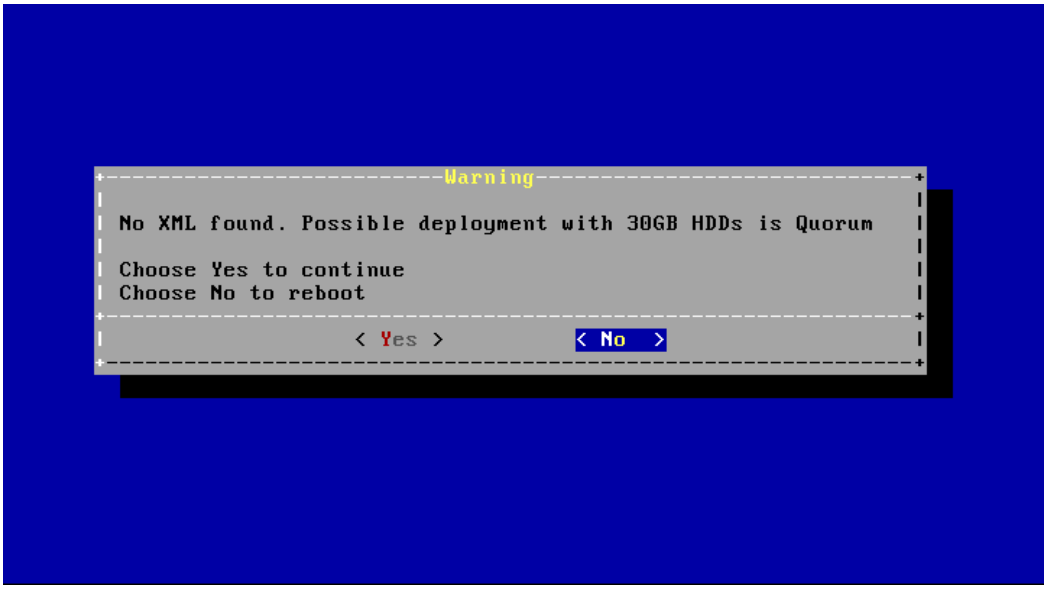


Figure 24: First installation - Deployment with hard disk size between 30 GB and 75 GB

If the deployment of the XML configuration file is a Quorum node then select **Yes** and the installation will be started. Otherwise choose **No** and a reboot will be performed.

Case 2-4: No suitable hard disk found

If no suitable hard disk is found the following message appears and a reboot will be performed.

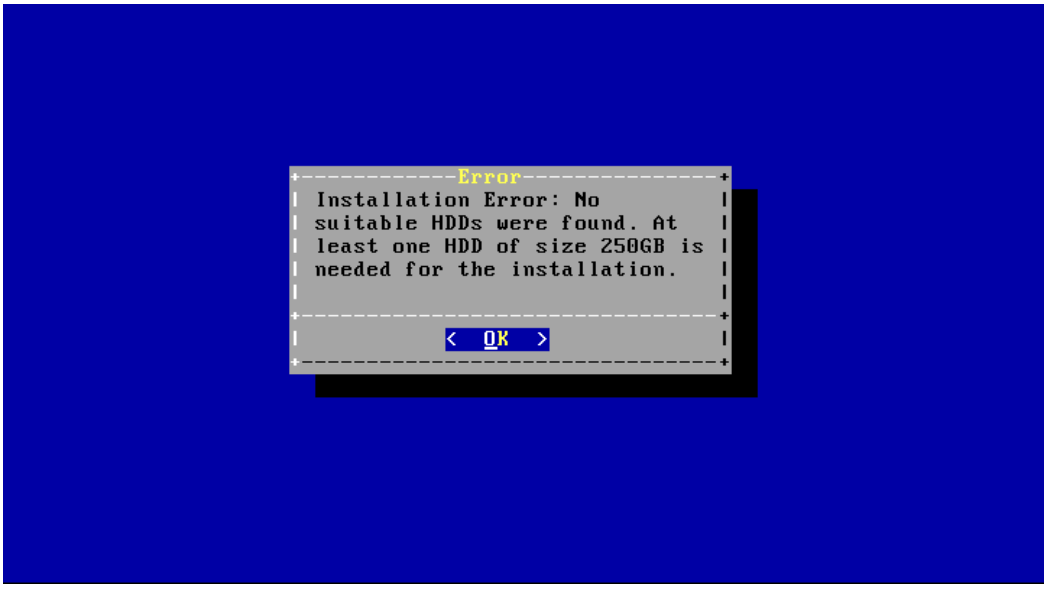


Figure 25: First installation - No suitable hard disk found

6) Duplex/Separated Duplex deployment:

In case of a Duplex or Separate Duplex deployment the following screen appears:

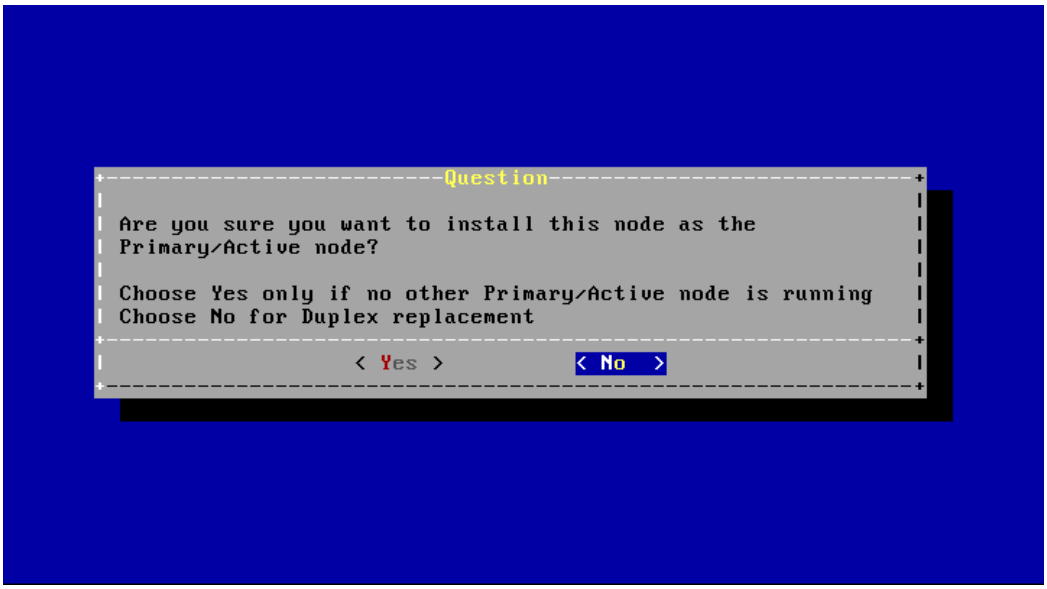


Figure 26: First installation - Duplex/Separated Duplex deployment

If you choose **Yes** the current node will be the active node after system startup.

IMPORTANT: Only choose **Yes**, if no other primary/active node is running.

For a Duplex replacement you have to select **No**.

7) When the installation has finished successfully a message will be displayed and you will be asked to remove the installation media and press OK to restart the system.

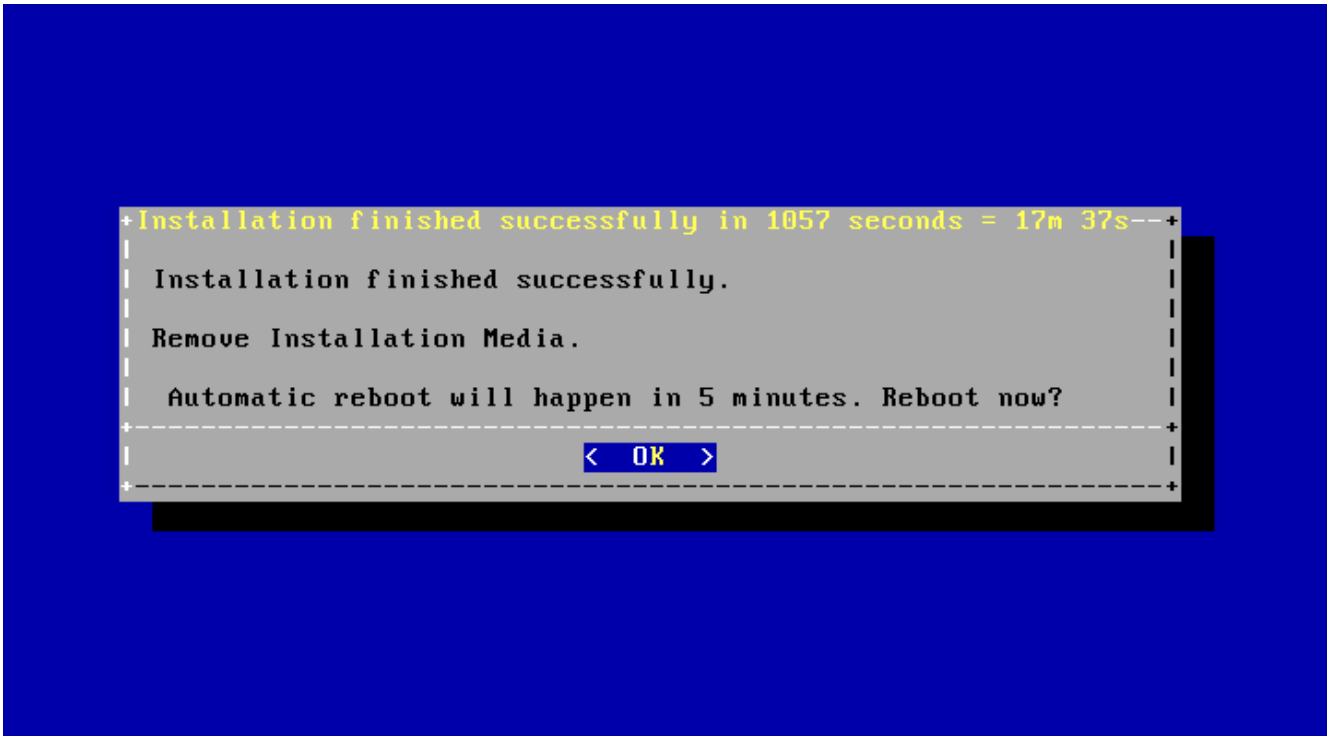


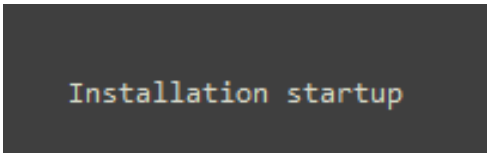
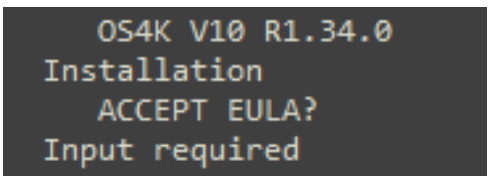
Figure 27: Installation completed successfully

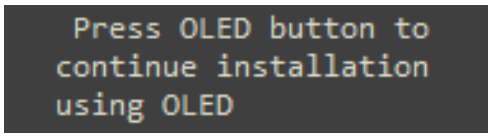
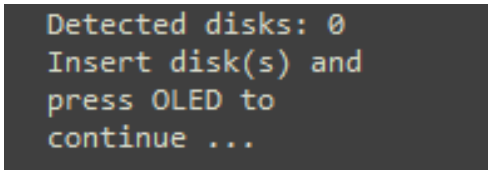
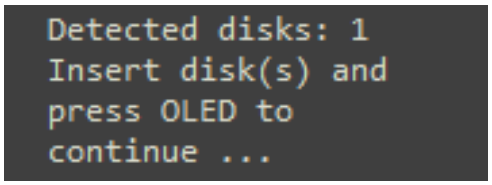
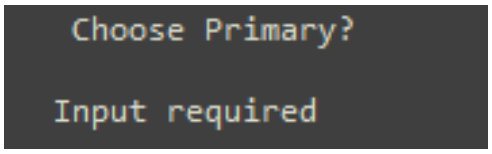
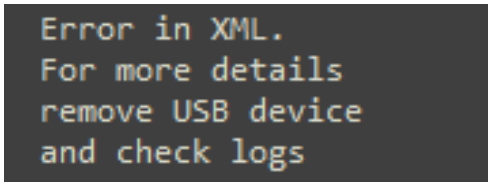
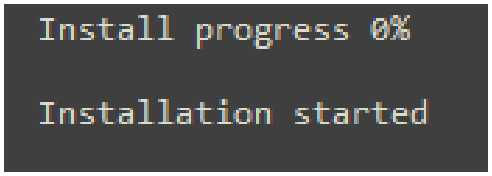
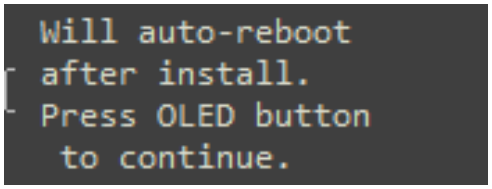
8) After rebooting, the system will start from the installed software on the hard disk and it can be accessed over any configured IP address for the connected LAN interfaces.

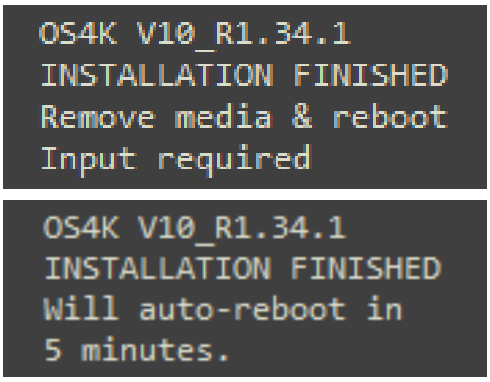
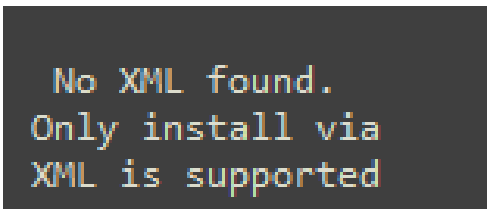
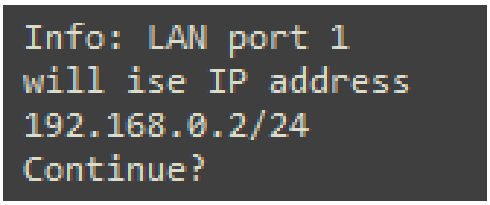
2.2.3.6 Installation using only the OLED display and the "ON" button

OpenScape 4000 Installation on EcoServer/EcoBranch can be performed using only the OLED display and the "ON" button which is placed left from it. There is no need to connect either monitor or keyboard, as the necessary installation steps are confirmed by a sole button.

Steps for installation using OLED:

1. Plug in the USB stick, remove all HGs/SSDs and Power on the EcoServer/EcoBranch. Wait for about 2-3 minutes during which the system displays "Installation Startup".	
2. The OLED display should show the message "ACCEPT EULA?". Press the "ON" button.	

3. Wait for the next prompt which asks the user to continue the installation using OLED.	
Press the "ON" button and wait until the following message is shown on the OLED:	
4. At this point insert one or two HDs/SSDs depending on your deployment. Wait for the correct number of disks to be displayed on the OLED. Press "ON" button to continue the installation **Note:** The display will refresh automatically every 30 seconds.	
Note: In case of Duplex or GSD systems the node configured as primary in the XML must be confirmed. Press "ON" button to confirm.	
Note: In case an error has been detected in the XML file (e. g. missing mandatory parameters) the following will be displayed:	
While OpenScape 4000 installation is in progress, the OLED displays the following message:	 

5. After the installation is finished, remove the USB drive and press the "ON" button once more in order to reboot and start the OpenScape4000 system for the first time.	
In case of installation without XML is performed, the OLED will show the following message. Press "ON" button to continue the installation without XML.	
In case of installation without XML (*), the OLED will show the IP Address which will be assigned to the first physical LAN interface of the Eco Server/EcoBranch. You can connect the first physical LAN interface to a network which has DHCP Server running and then the Eco server/EcoBranch will try to obtain an IP address. This will be shown on the OLED for verification purposes. Continue by pressing again the "ON" button. At the end of the installation the OpenScape 4000 Platform Portal will be accessible over that IP address. In case no DHCP answer is received the default IP address/netmask will be 192.168.0.2/255.255.255.0.	

NOTICE: in case of any error remove the USB Stick, check the logs inside the directory "<usb_stick_root>/_install_logs", then correct the issue(s) and start again from Step 1. It is recommended to Power OFF the ECO Server/EcoBranch before the Step 1).

2.2.3.7 Recommended GSD Installation Sequence

Recommended and most efficient first installation sequence for Separated Duplex:

- Install Quorum Node
- Install Node B

- Install Node A as active node.

2.2.3.8 Recommended Duplex Installation Sequence

Recommended and most efficient first installation sequence for Duplex:

- Install Node B
- Install Node A as active node.

NOTICE: In case of multi node, it is recommended to use a common xml for all nodes and have all the cables connected (including cross-connect) prior to installation.

2.2.3.9 Administrative Data Processor (ADP)

The ADP is the primary internal server and is a mandatory component of all systems. Its main function is administration and maintenance of the system.

The standard functions of the ADP are:

- System startup
- Direct AMO dialog (DAD) access for configuration administration
- Remote maintenance administration (RMA)
- Local maintenance terminal interface
- Call Detail Recording
- Traffic metering and statistics

2.2.3.9.1 System Startup

The ADP is responsible for commissioning (placing into service) the system.

The commissioning sequence occurs after powering on a system and after a software- or hardware-initiated system restart (reload or hard restart only).

The ADP also reloads flashware and loadware on a subsystem level (ADP, SWU, and ACD secondary server) and an individual module level (after deactivation and activation of boards).

The commissioning sequence is as follows:

- Startup of ADP:
  - Loading ADP common control unit flashware
  - Loading ADP common control unit software
  - Starting basic operation of ADP common control unit
  - Initializing the ADP interface ports
  - Loading the ADP interface ports
  - Starting the ADP interface ports

- Startup of switching unit:
  - Loading SWU flashware
  - Loading SWU software
  - Starting basic operation of the SWU
  - Copying Linux command file for database
  - Generating the database
  - Loading the loadware on telephony boards
  - Starting telephony boards
  - Starting the call processing operation

2.2.3.9.2 Direct AMO Dialog (DAD) Access

The OpenScape 4000 Manager provides direct command line access for administration and troubleshooting configuration and system problems.

2.2.3.9.3 Remote Maintenance and Administration

The Linux-based RMA application provides information and status reports for major and minor alarms.

RMA requires a CCA II (asynchronous) modem to support the following:

2.2.3.9.4 Local Maintenance Terminal Interface

This interface provides for the physical connection of a maintenance terminal to the ADP and access to Linux applications.

2.2.3.9.5 Call Detail Recording

CDR provides traffic statistics for monitoring system activity and evaluating system performance. CDR statistics can also be used by the traffic metering and statistics application.

2.2.3.9.6 Traffic Metering and Statistics Application

This program is a Linux-based application that analyzes system performance and generates tabular data for evaluating and optimizing system resources.

2.2.3.9.7 System Security

Application software in the ADP provides for system security. The system administrator uses the software to assign user passwords and control the access level of those passwords. This prevents unauthorized access to the system and to critical system files, databases, and administration or maintenance facilities.

2.2.3.9.8 RDS

Realtime Diagnostics System (RDS), formerly trunk diagnostics system (TDS), is a diagnostic tool that provides telephony fault localization for station and data lines and limited trunk fault reporting capabilities for trunk facility problems. It provides tools and features that allow you to solve line and trunk problems more efficiently

2.2.3.9.9 HSD

The hardware and symptom diagnosis (HSD) tool is a browser-based application that resides on the Primergy server. HSD functionality consists of menu choices within the OpenScape 4000 Manager client application. HSD can be used either remotely or locally. It is designed to improve usability, reduce service time, reduce cost, and enhance serviceability.

2.3 Manual OpenScape 4000 SoftGate Configuration

In case at the time of system installation no intialcfg file/ softGateInitialConfiguration section in the configuration XML file was available on the installation media you can now configure the OpenScape 4000 SoftGate manually with the OpenScape 4000 Platform Administration (Portal).

NOTICE: Please use XML to configure bonds during the installation then assign the bond instead of the eth as the interface to be used. If the SG is already installed then please use the recover-H4K.sh Tool to configure the bond then assign the bond in the WBM. For more details please see Using Recovery/Reconfiguration Tool.

Start the OpenScape 4000 Platform Administration (Portal) and open the LAN Wizard:

System > LAN Configuration > LAN Wizard:

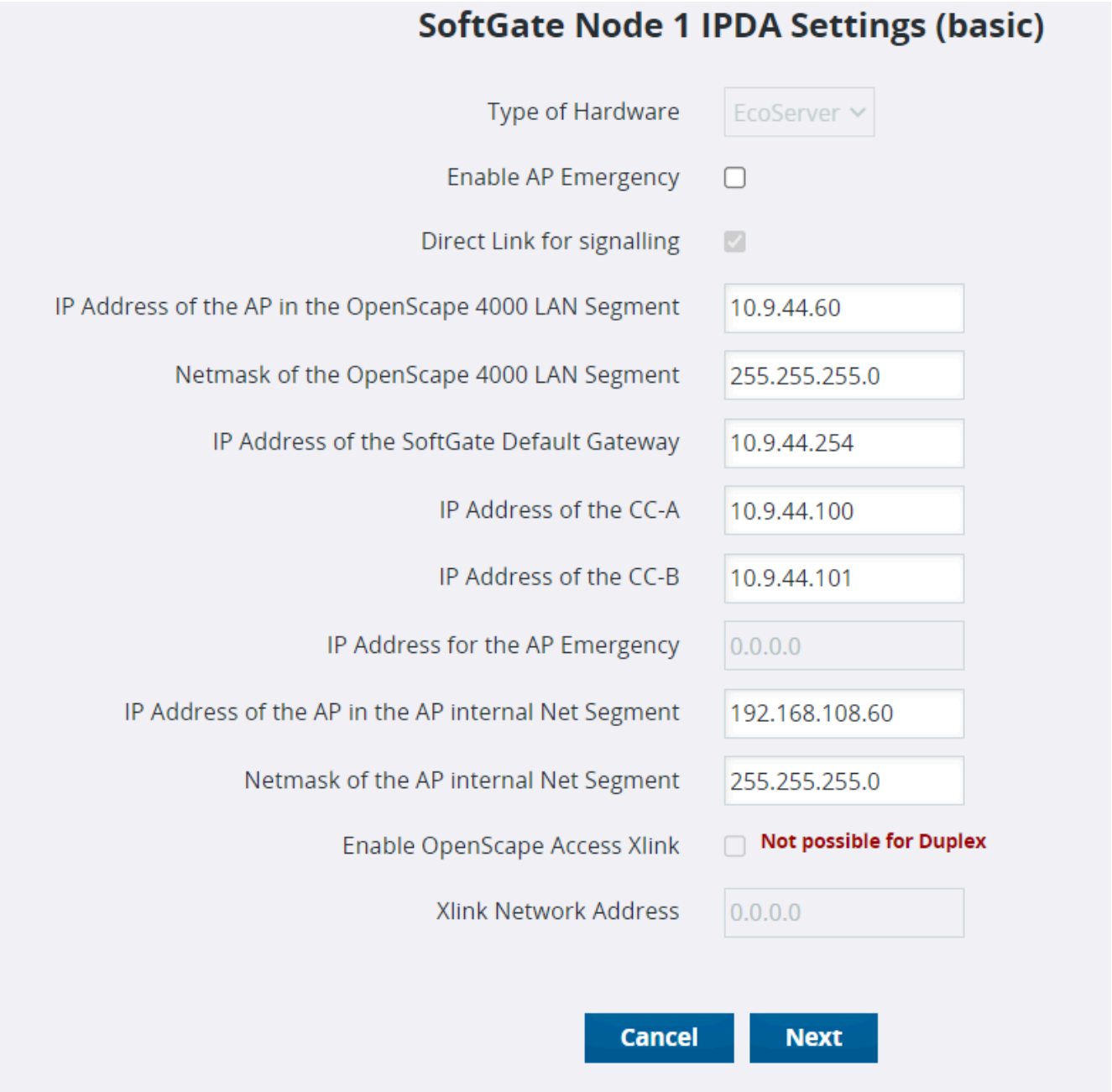


Figure 28: OpenScape 4000 SoftGate configuration - Basic IPDA settings

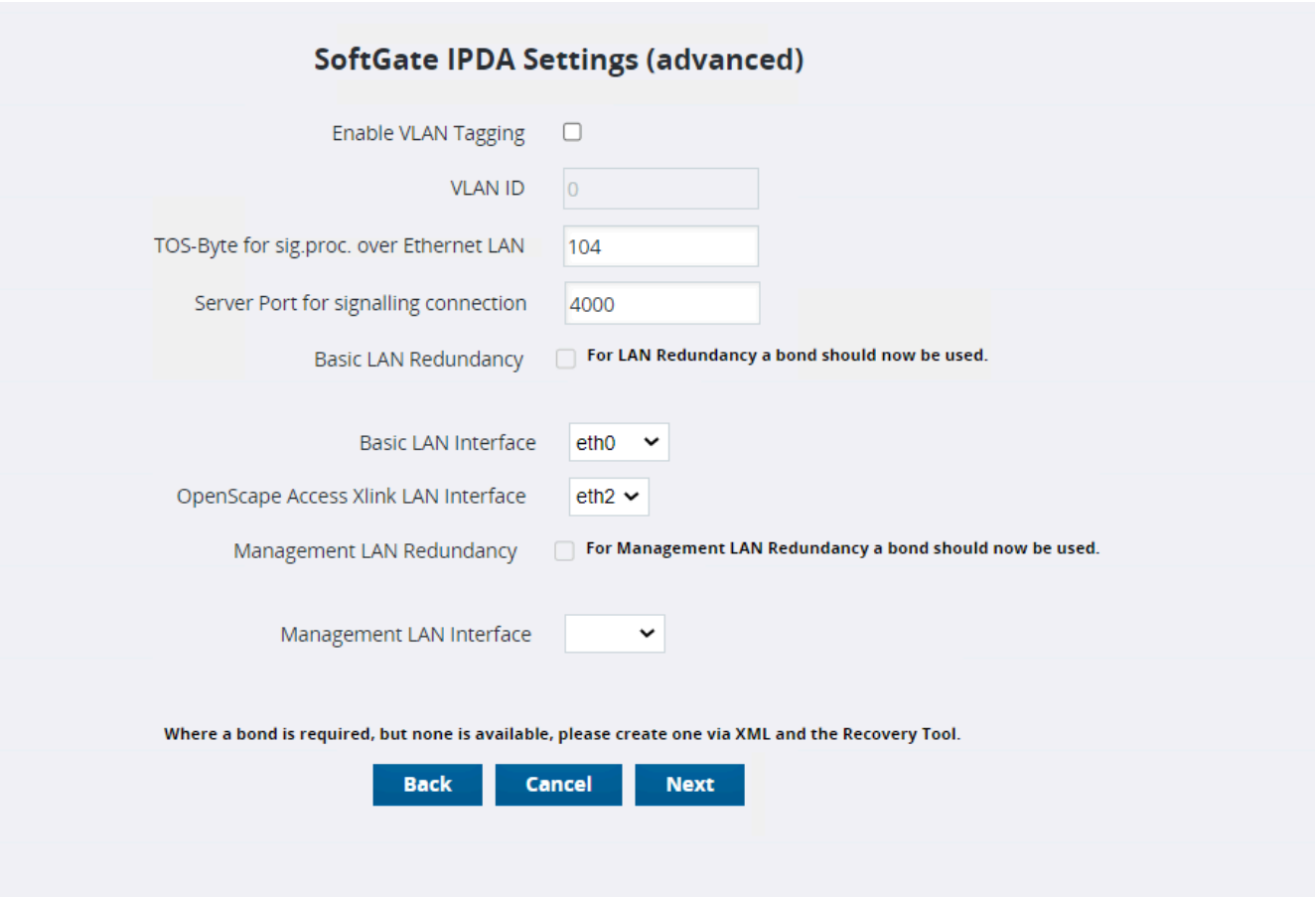


Figure 29: OpenScape 4000 SoftGate configuration - Advanced IPDA settings

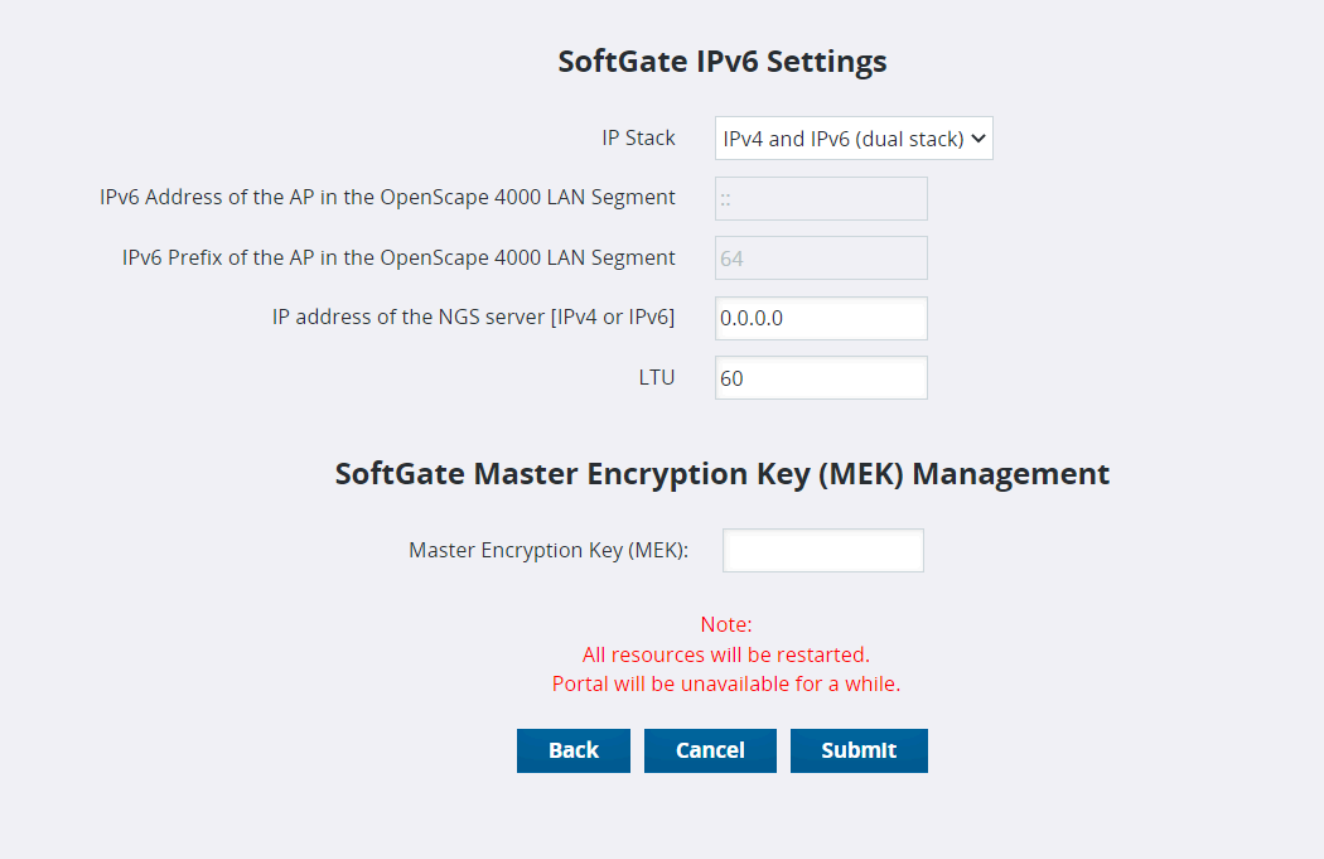


Figure 30: OpenScape 4000 SoftGate configuration - Basic IPDA settings

NOTICE:

With OpenScape 4000 V8 R2 or higher, the procedure from above applies also for configuring an Integrated SoftGate on Enterprise GW after enabling it under System > LAN Configuration > System.

With OpenScape 4000 V10 R1 or higher, the procedure from above applies also for configuring an Integrated SoftGate on a Duplex System after enabling it under System > LAN Configuration > System.

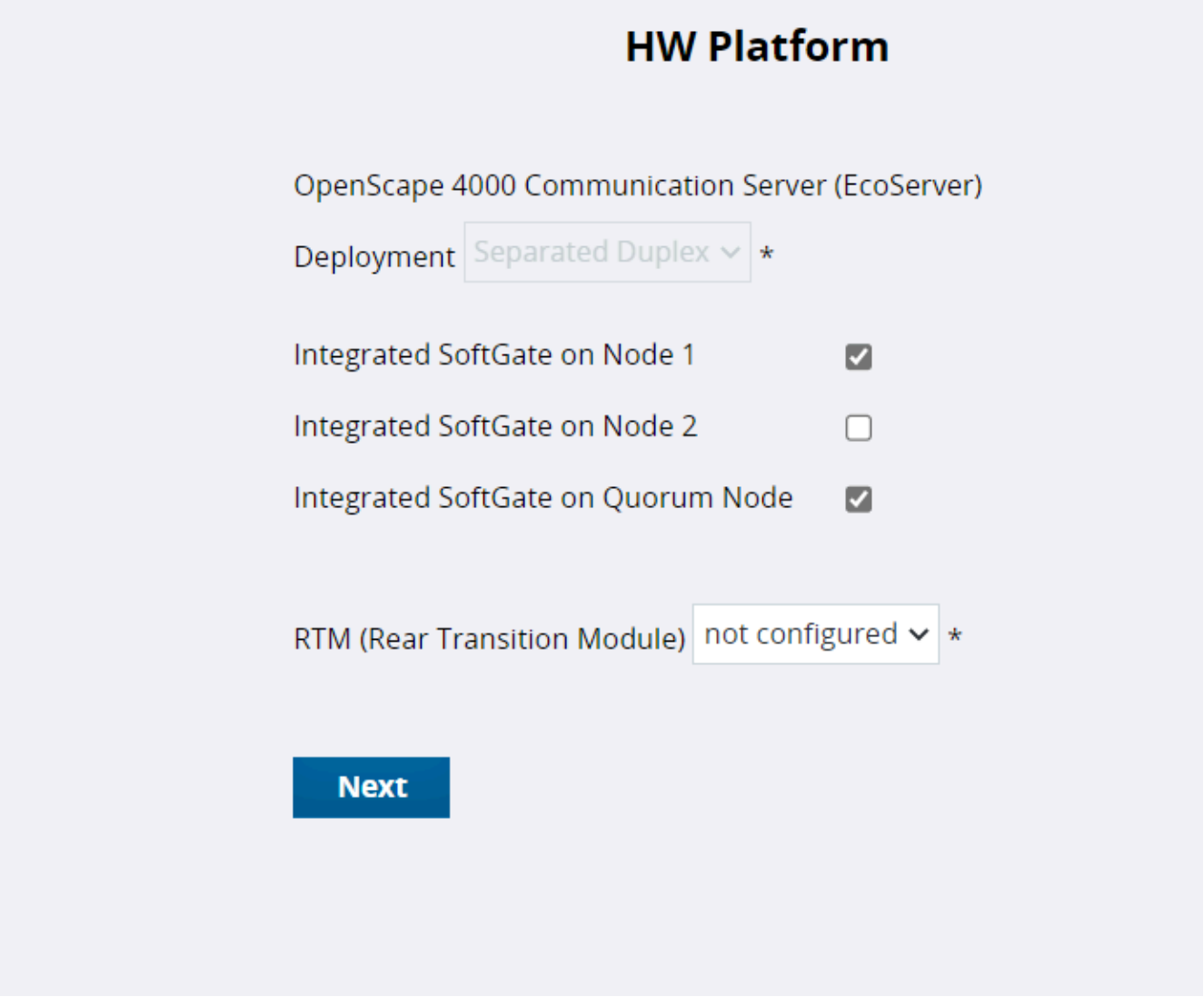


Figure 31: OpenScape 4000 SoftGate configuration - Integrated SoftGate

2.4 Zero Local Configuration for Stand-Alone OpenScape 4000 SoftGate

2.4.1 Feature Description

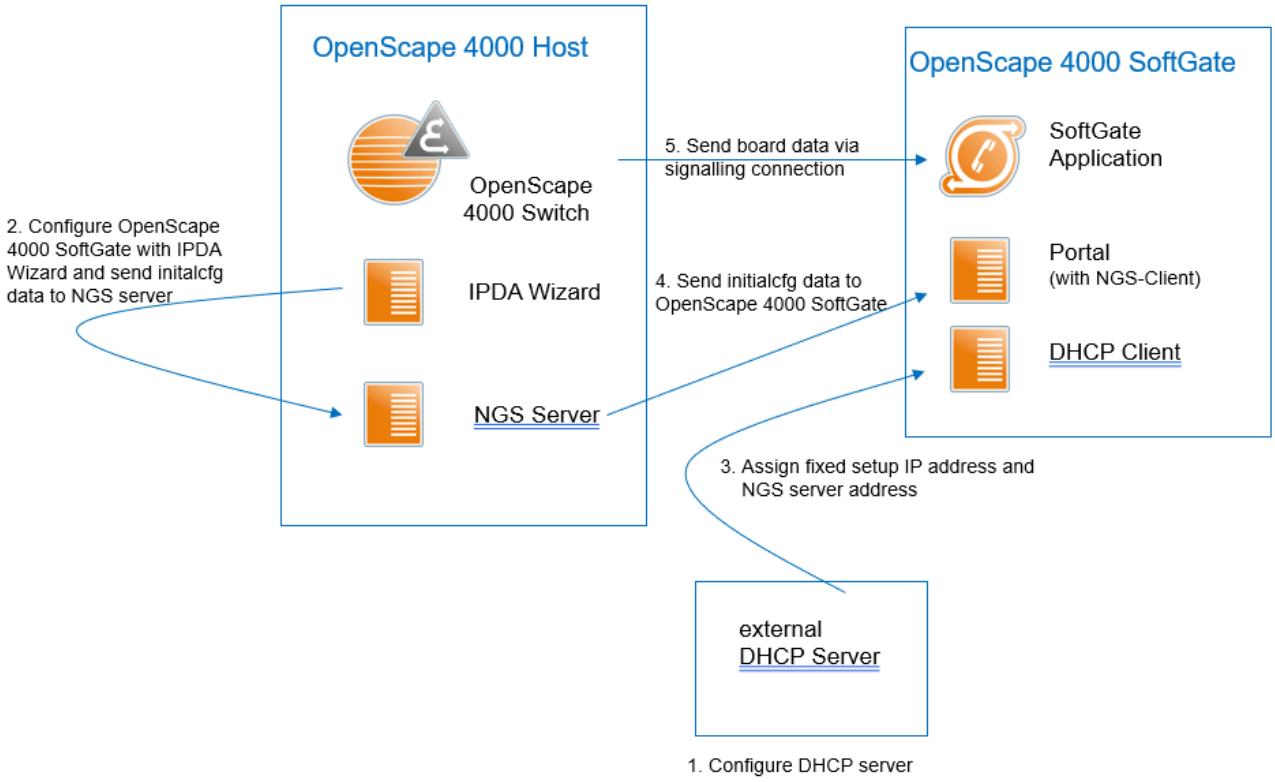


Figure 32: Configuration overview for Zero Local Configuration

The Zero Local Configuration feature allows the first installation of a stand-alone OpenScape 4000 SoftGate without any local configuration. The OpenScape 4000 SoftGate can be connected to an existing system. It is then installed and configured automatically without further manual intervention as soon as the connection to the host system has been established.

An external DHCP server is one of the prerequisites for this. The NGS has also been extended so as to now also provide support for the Zero Local Configuration feature in addition to data distribution of IPv6 addresses.

Prerequisites:

- DHCP server

  An external DHCP server must be provided for this purpose. The MAC address of the OpenScape 4000 SoftGate must be known to this server as it is used by the server to provide a fixed IPv4 address for the OpenScape 4000 SoftGate. This IPv4 address is the setup IP address used for the OpenScape 4000 SoftGate, in other words the IP address that is also used subsequently to access the OpenScape 4000 Platform Administration (Portal).

  Please refer to Section 2.4.3, "Configuration (Example)" for correctly configuring the DHCP server.

- The OpenScape 4000 SoftGate must be configured using the IPDA Wizard. The IPDA Wizard saves the data for the first installation (initialcfg.xml) with the setup IP address in the NGS server database on the OpenScape 4000 host.

First installation sequence

When the OpenScape 4000 SoftGate is starting up, it sends a DHCP request (DHCP discover message with option 60) to retrieve the IP address of the OpenScape 4000 Platform Administration (Portal) of the OpenScape 4000 SoftGate. If an IP address with vendor option 43, which contains the NGS IP address, is delivered by the DHCP server, the OpenScape 4000 SoftGate contacts the NGS server and retrieves its first installation data (initialcfg.xml) with the help of the setup IP address. If the first installation startup fails, the OpenScape 4000 SoftGate tries to retrieve updated first installation data, if available.

If the NGS server cannot be contacted, further retries are attempted until the NGS server is available or the first installation data is provided/created manually on the system.

Afterwards the OpenScape 4000 SoftGate startup proceeds as normal. The OpenScape 4000 SoftGate retrieves the current board data via the signaling connection.

Other scenarios

Beside the first installation, other scenarios are possible with this feature, since when configuration changes are made that impact the initialcfg file, these are not only updated as per usual on the OpenScape 4000 SoftGate but also on the NGS server.

- Replacing hardware

  In case of a hardware replacement the latest first installation data for the OpenScape 4000 SoftGate can be provided.

  If replacement of the OpenScape 4000 SoftGate hardware is necessary, the NGS server will provide the latest first installation data. Note here however that the DHCP server also has to be adapted to the new MAC address of the OpenScape 4000 SoftGate.
- Misconfiguring a OpenScape 4000 SoftGate

  The first installation data can be reset in the case of a misconfigured OpenScape 4000 SoftGate.

  In case of a misconfigured OpenScape 4000 SoftGate, the initialcfg file can be overwritten. This process is initiated by the IPDA Wizard.

2.4.2 Service Information

- This feature is released for stand-alone OpenScape 4000 SoftGates (OpenScape Access 500 or OpenScape 4000 EcoBranch).
- This feature is only released for IPv4 addresses.

- An external DHCP server must be provided that fulfills the following requirements:
  - It must be able to provide a fixed IPv4 address with the vendor-specific option 43.
  - It must provide an IPv4 address (setup IP address for the OpenScape 4000 SoftGate) **and** a host name for the OpenScape 4000 SoftGate to the OpenScape 4000 SoftGate.
  - The NGS IP address must be delivered as a vendor-specific option 43 by the DHCP server. If the vendor option is not configured on the DHCP server, the first installation data cannot be retrieved automatically. The OpenScape 4000 SoftGate must then be configured manually with the OpenScape 4000 Platform Administration (Portal) or by means of an XML file.
- For using this feature, the OpenScape 4000 SoftGate must be configured with the IPDA Wizard.

  The setup IP address assigned to the OpenScape 4000 SoftGate in the DHCP server must be entered as additional information in the IPDA Wizard.
- The NGS IP address must be configured in the LAN Wizard of the OpenScape 4000 Platform Administration (Portal) on the central OpenScape 4000 host. The IP address of the NGS server must be accessible from the IPDA network.
- All OpenScape 4000 SoftGates registered in the OpenScape 4000 SoftGate configuration table of the NGS server are displayed in the OpenScape 4000 Platform Administration (Portal) and can be deleted here. Deletion means that the corresponding OpenScape 4000 SoftGate is deleted from the NGS server database.

  System > SoftGates > Delete button

  IMPORTANT: Only delete those OpenScape 4000 SoftGates that are no longer in use/available, in other words for example have previously been deleted in the IPDA Wizard.

- In case of configuration changes that affect the first installation file, the initialcfg file is not only saved locally on the OpenScape 4000 SoftGate but also updated on the NGS server.
- If the OpenScape 4000 SoftGate is to be installed in a network environment with a separate customer LAN and IPDA LAN, remember that the NGS server is only accessible in the IPDA LAN. A DHCP server has to be made available in this case both in the customer LAN and in the IPDA LAN. The DHCP server in the customer LAN assigns the IP address for accessing the OpenScape 4000 Platform Administration (Portal). The DHCP server in the IPDA LAN has to fulfill the necessary requirements for this feature. For configuration details, refer to Section 2.4.3.2, "Zero Local Configuration in case of separate Customer and IPDA LAN".

2.4.3 Configuration (Example)

2.4.3.1 DHCP Server Configuration

The DHCP **option 60** is the **Vendor Class Identifier** (**VCI**). It is used to identify a client on the server. The DHCP server responds to these requests with **option 43** in order to deliver vendor-specific information to the client. A detailed description of these options can be found in RFC 2132.

In the case of the Zero Local Configuration feature, the OpenScape 4000 SoftGate sends the **VCI** (**Vendor Class Identifier**) string **SEN.Softgate** in the DHCP discovery request. The DHCP server has to transmit the **NGS IP address** as content for **option 43** in the DHCP offer.

The DHCP server has to provide the following options (mandatory parameters):

- host-name
- vendor-encapsulated-options
- IP and subnet-mask
- routers

The DHCP client also accepts the following options if they are available (optional parameters):

- broadcast-address
- domain-name
- domain-name-servers
- time-offset
- ntp-servers

Sample configuration of a Linux DHCP server (ISC)

option space SEN-SG;

option SEN-SG.ngs-ip-address code 1 = ip-address;

default-lease-time 14400;

ddns-update-style none;

log the vendor-id into the lease file

set vendor-string = option vendor-class-identifier;

vendor specific information: these parameters are valid only for clients

belonging to a particular vendor class. The vendor class is identified by

the value that the client sends with the vendor class identifier option.

class "SEN-Softgate" {

option SEN-SG.ngs-ip-address 172.15.3.13;

match if **option vendor-class-identifier** = "SEN.Softgate";

vendor-option-space SEN-SG;

}

subnet 172.15.3.0 netmask 255.255.255.0 {

option broadcast-address 172.15.3.255;

option routers 172.15.3.1;

option time-offset 3600;

range 172.15.3.220 172.15.3.229;

```
}
host pcie3-SG41 {
option subnet-mask 255.255.255.0;
option routers 172.15.3.1;
option SEN-SG.ngs-ip-address 172.15.3.13;
option ntp-server 192.1.1.253
option host-name "pcie3-SG41";
option domain-name-servers 172.28.12.19, 172.28.12.20;
option domain-name "global-intra.net";
hardware ethernet 00:1a:e8:3c:e5:b6;
fixed-address 172.15.3.40;
option time-offset 3600;
}
```

In the DHCP Server configuration, there are different possibilities for the IP address configuration of the NGS server:

1) You can add the option **SEN-SG.ngs-ip-address** to the class section, if you want to use the same IP address for all OpenScape 4000 SoftGates (like a default value).
2) You can add the option **SEN-SG.ngs-ip-address** to the host section. This would be preferable, if you will use different NGS servers.
3) You can mix the two possibilities, if you want to specify a default NGS server and you will have OpenScape 4000 SoftGates with a different NGS server.

Sample configuration of a Cisco DHCP server

```
ip dhcp excluded-address 172.15.3.1 172.15.3.219
ip dhcp excluded-address 172.15.3.230 172.15.3.254
!
ip dhcp pool 172-15-3
network 172.15.3.0 255.255.255.0
option 2 hex 0000.0E10
option 60 ascii "SEN.Softgate"
option 43 hex 0104.ac0f.020d
option 42 ip 192.1.1.253
default-router 172.15.3.1
lease 0 4
!
ip dhcp pool 172-15-3-40
host 172.15.3.40 255.255.255.0
hardware-address 001a.e83c.e03a
client-name pcie3-SG41
```

option 60 ascii "SEN.Softgate"

option 43 hex 0104.ac0f.030d

option 42 ip 192.1.1.253

dns-server 172.28.12.19 172.28.12.20

domain-name global-intra.net

lease 0 4

Sample configuration of a Windows DHCP server

The configuration of a Windows DHCP server differs from one Windows version to another.

You will find information on the DHCP server configuration in the Microsoft server documentation.

Example of communication between a DHCP server and OpenScape 4000 SoftGate

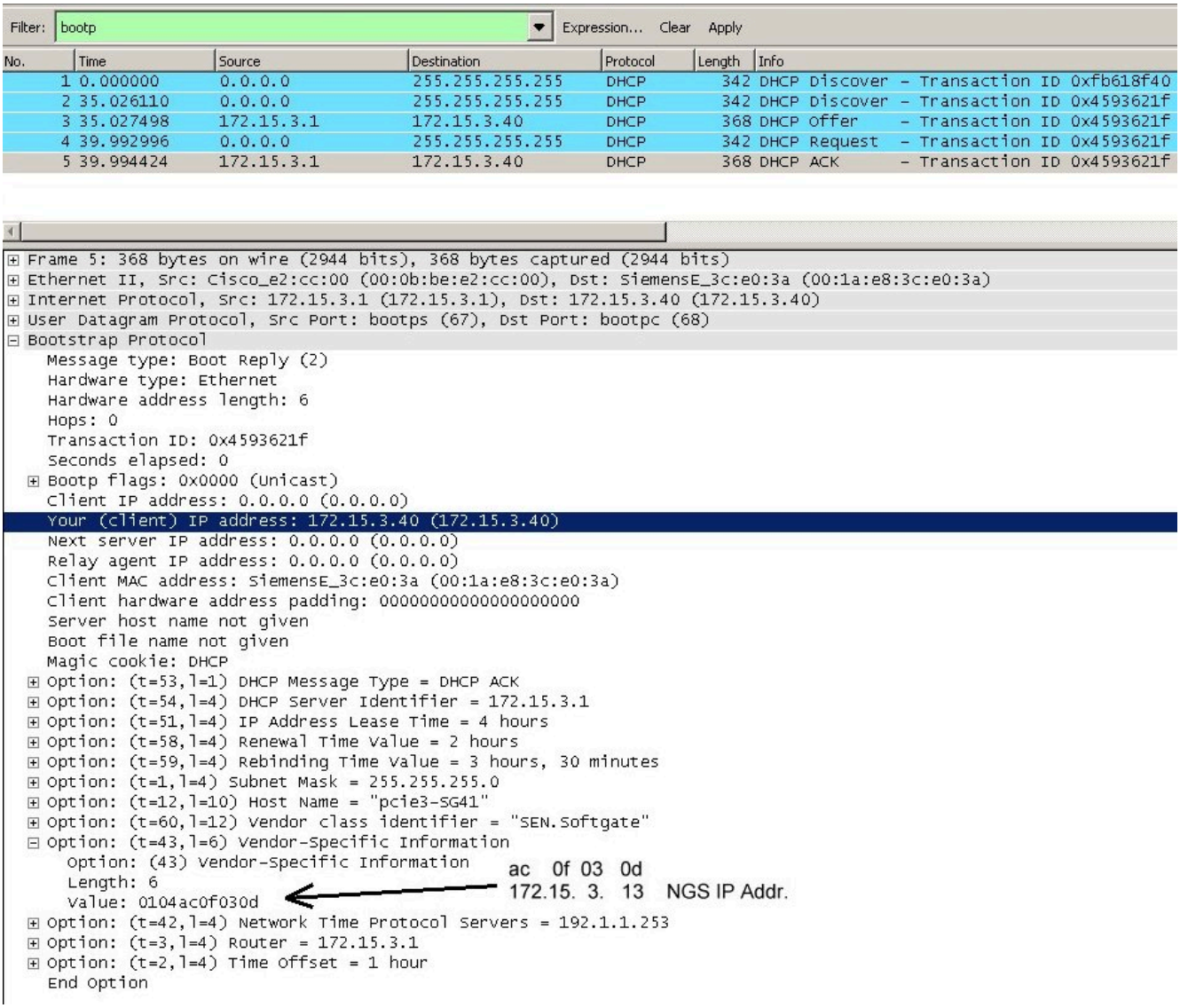


Figure 33: Communication between DHCP server and OpenScape 4000 SoftGate

Table 33: IP addresses

IP address of DHCP server	172.15.3.1
Setup IP address for OpenScape 4000 SoftGate (eth0)	172.15.3.40 (this was assigned by DHCP to the OpenScape 4000 SoftGate)
IP address of NGS server	The IP address of the NGS server can be found in the Section **Vendor-specific Information**. This address is always represented in hexadecimal notation.

2.4.3.2 Zero Local Configuration in case of separate Customer and IPDA LAN

The LAN interface eth0 is assigned to the customer LAN. The LAN interface eth1 is assigned to the IPDA LAN.

A DHCP server is required in the customer LAN, which assigns the IP address for the OpenScape 4000 Platform Administration (Portal) to the OpenScape 4000 SoftGate. The OpenScape 4000 SoftGate can then be accessed remotely in the network using this address. An SSH connection to this IP address can now be established using the PuTTy program.

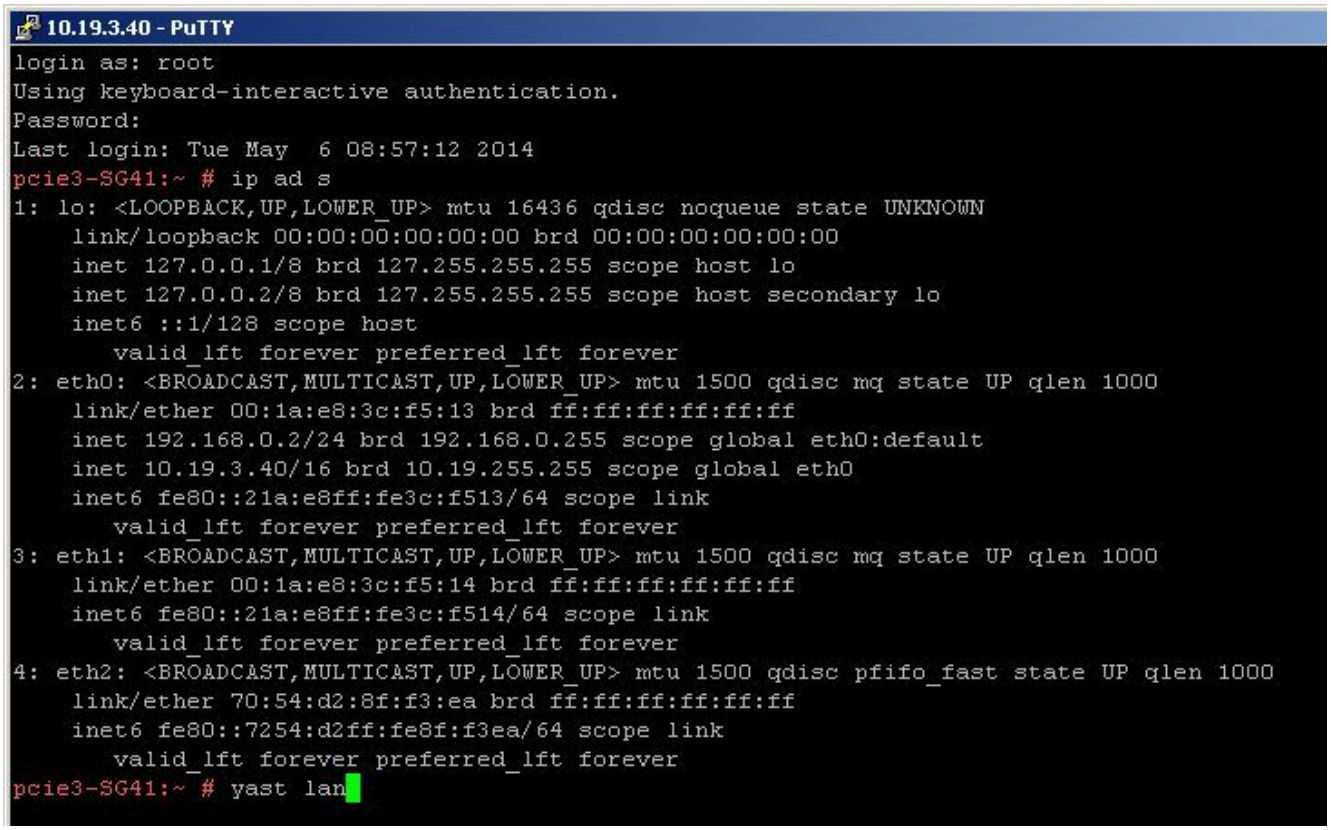


Figure 34: SSH connection to OpenScape 4000 SoftGate

The setting for the LAN interface eth1 then has to be changed to DHCP using Yast.

Network Devices > Network Settings > eth1 > Edit

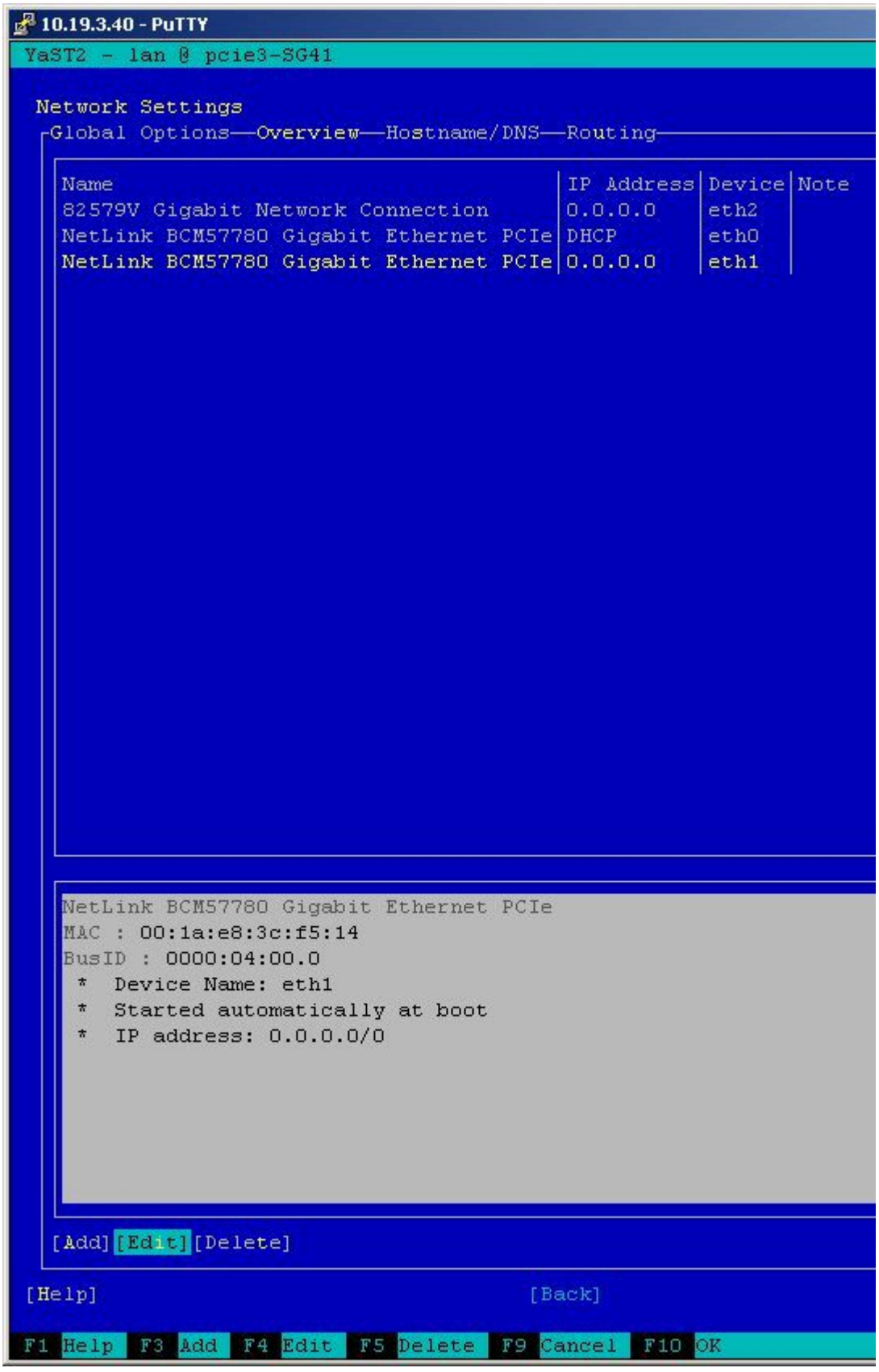


Figure 35: Change eth1 on DHCP

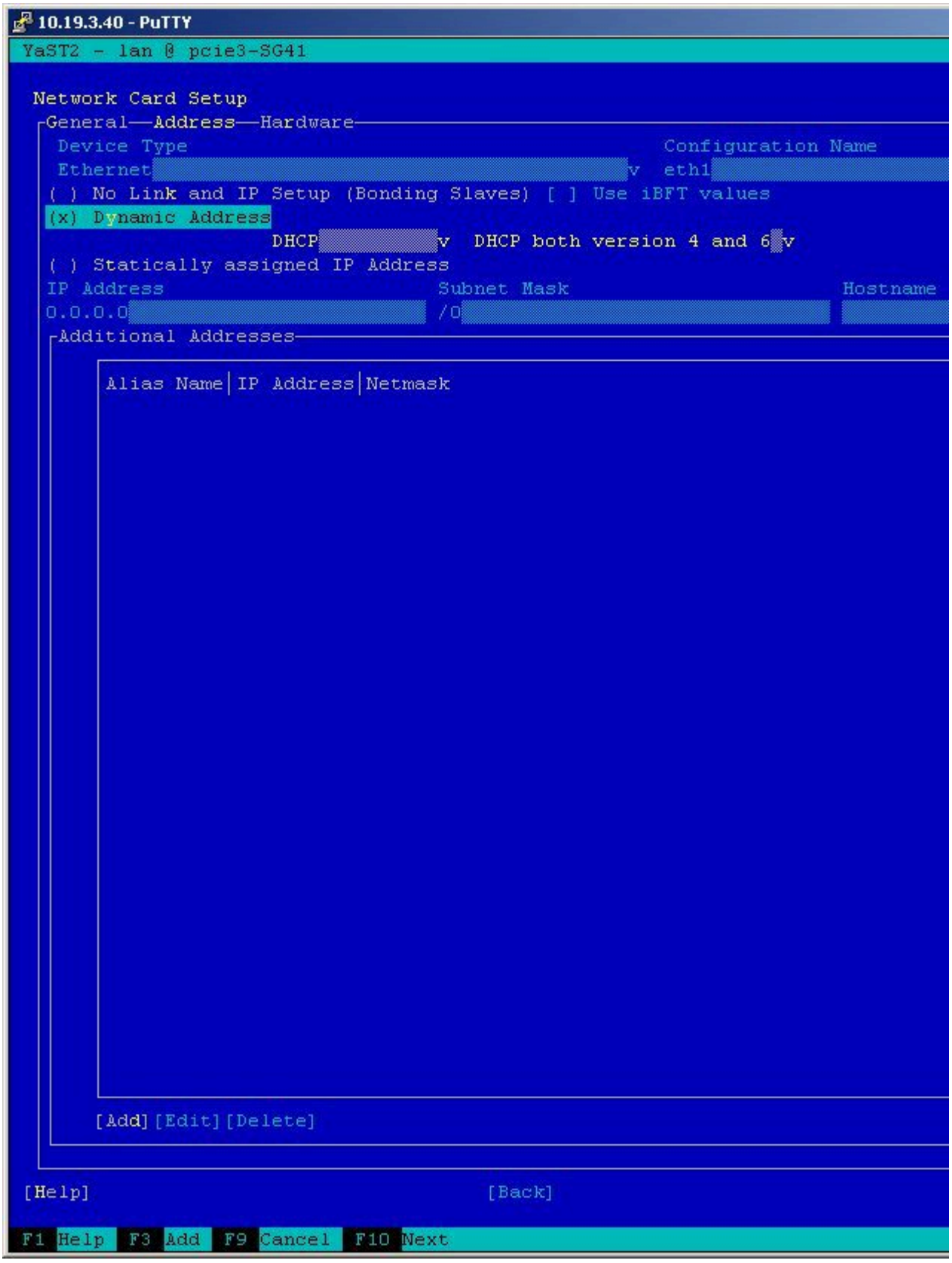


Figure 36: Change eth1 on DHCP

If configuration of the DHCP server in the IPDA LAN and configuration of the OpenScape 4000 SoftGate have now been carried out in accordance with the requirements for this feature, the OpenScape 4000 SoftGate gets its first installation data from the NGS server and starts automatically.

2.4.3.3 Time synchronization of the Linux system time

NOTICE: The OpenScape 4000 SoftGate gets its time settings via AMO SIPCO. Only the Linux time is configured below.

All countries that use daylight saving time have to configure the timezone in YaST following installation since the DHCP client does not permit regional settings.

System > Date and Time

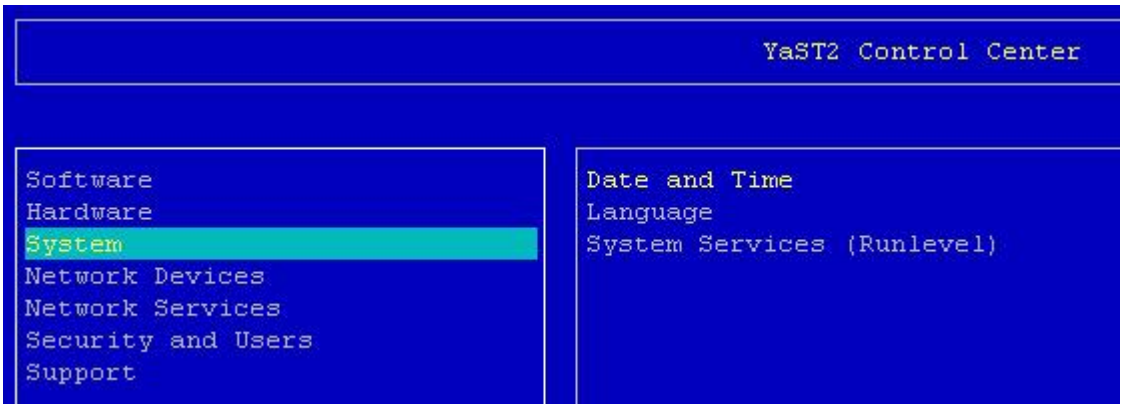


Figure 37: Timezone configuration with YaST

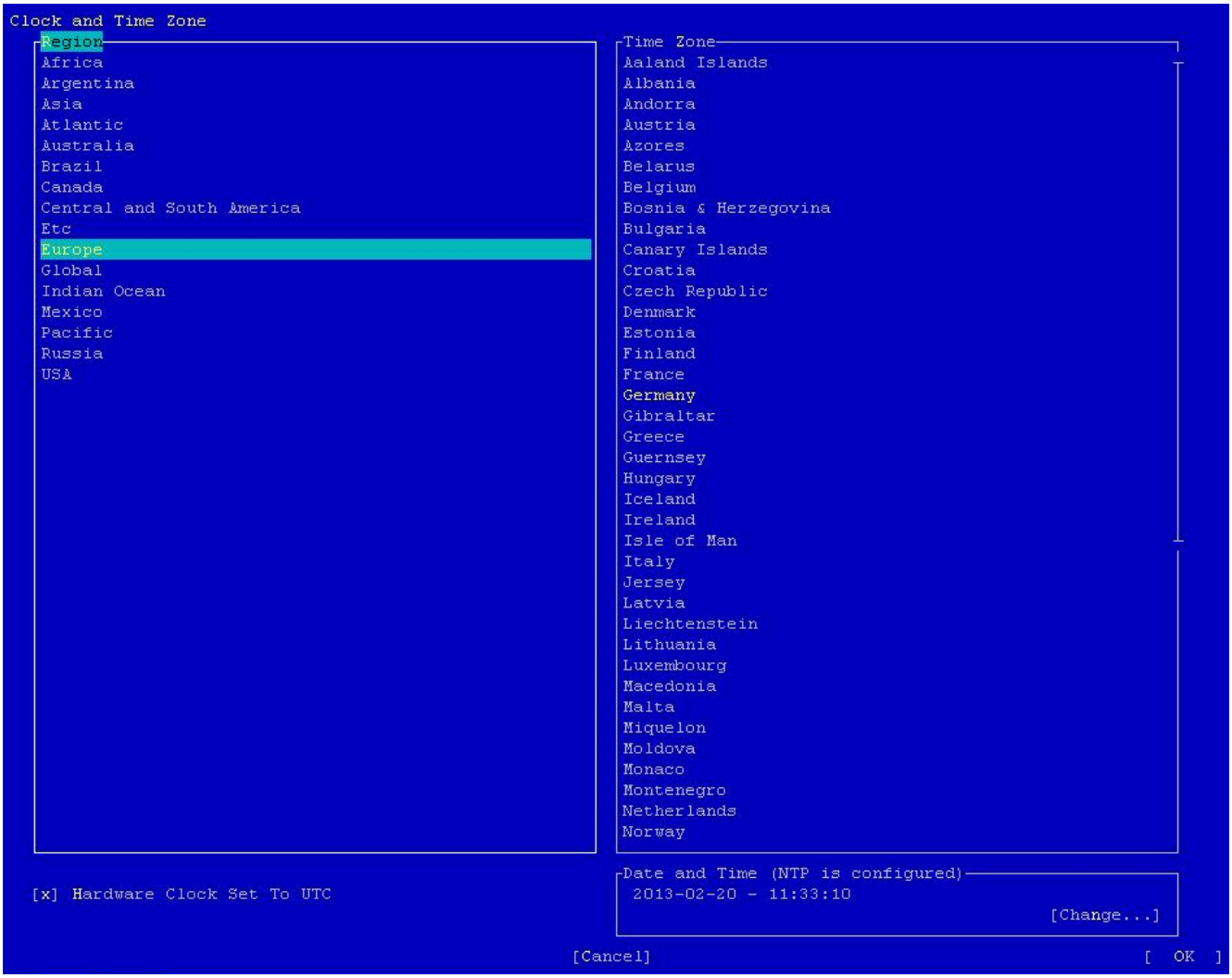


Figure 38: Timezone configuration with YaST

IMPORTANT: The DHCP **time-offset** option can be used for configuring the local timezone in all countries that do not use daylight saving time. The time offset is entered as usual (west of Greenwich with a negative algebraic sign and east of Greenwich with a positive algebraic sign).

If the DHCP **time-offset** option is used to configure the local timezone, it must be ensured that the time offset in the target system is displayed in accordance with POSIX (Portable Operating System Interface). Unlike the usual notation, POSIX uses a positive algebraic sign for west of Greenwich and a negative algebraic sign for east of Greenwich.

Explanation

A system configured with the DHCP time-offset option "-14400", i.e. a timezone 4 hours west of Greenwich, is set up in POSIX format with the timezone "UTC +4". This is visible, for example, when outputting the Linux "date" command.

Example

An OpenScape 4000 SoftGate in Moscow would be configured with the DHCP time-offset option "144002", i.e. 4 hours east of Greenwich ("UTC+4"). The timezone "UTC-4" (POSIX) would then be set up on the OpenScape 4000 SoftGate.

2.4.3.4 Configuring the NGS IP Address

OpenScape 4000 Platform Administration (Portal) > LAN Wizard > IPDA LAN

Configure the IP address of the NGS server (**NGS IP address**).

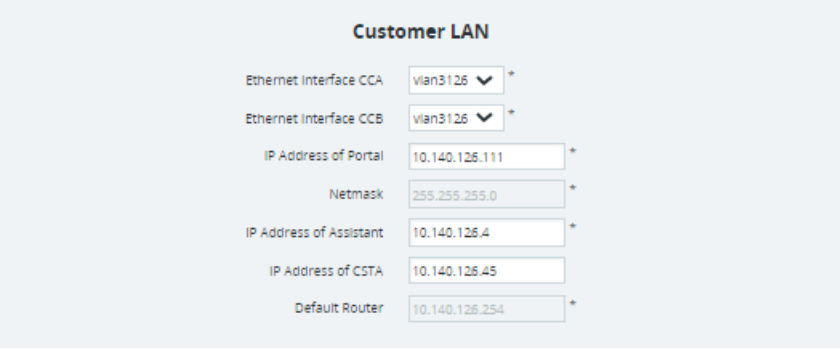


Figure 39: NGS IP address - Customer LAN

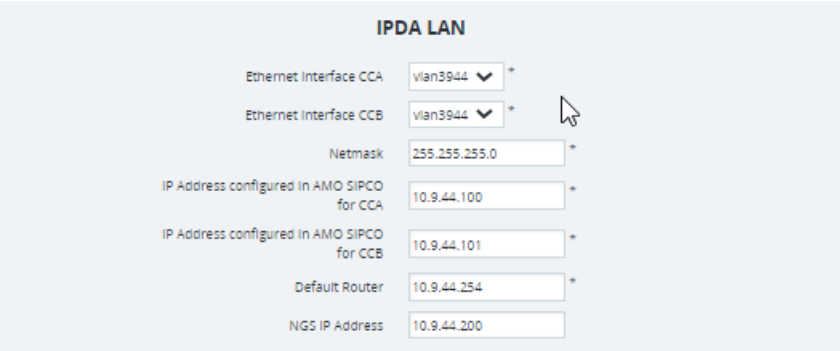


Figure 40: NGS IP address - IPDA LAN

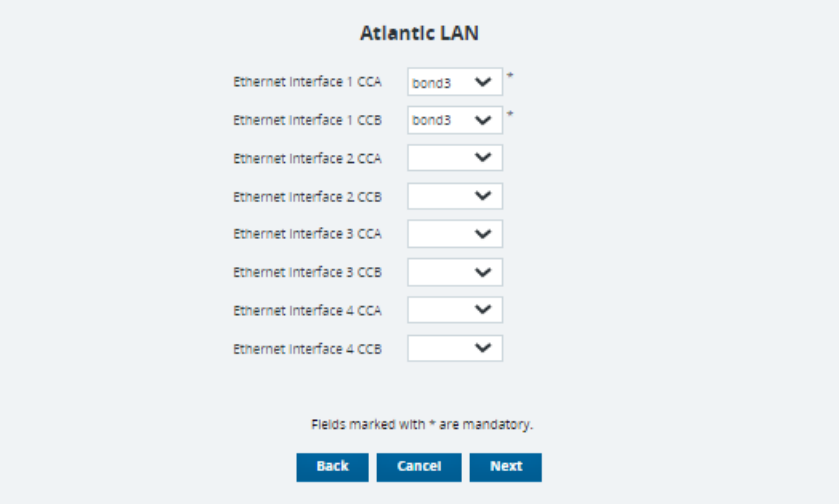


Figure 41: NGS IP address - Atlantic LAN

2.4.3.5 Configuring the NGS

IPDA Wizard > SoftGate Initial Configuration

Enter the IP address of the OpenScape 4000 SoftGate (eth0) assigned by the DHCP server in the **Setup IP Address** field and enable the checkbox **Send to NGS Server**.

IMPORTANT: The Setup IP Address is only stored in the NGS data base. If the first configuration data of the OpenScape 4000 SoftGate will be changed before startup (e.g. in case of a faulty configuration), the setup IP address must be entered again, because it is not stored in the IPDA Wizard.

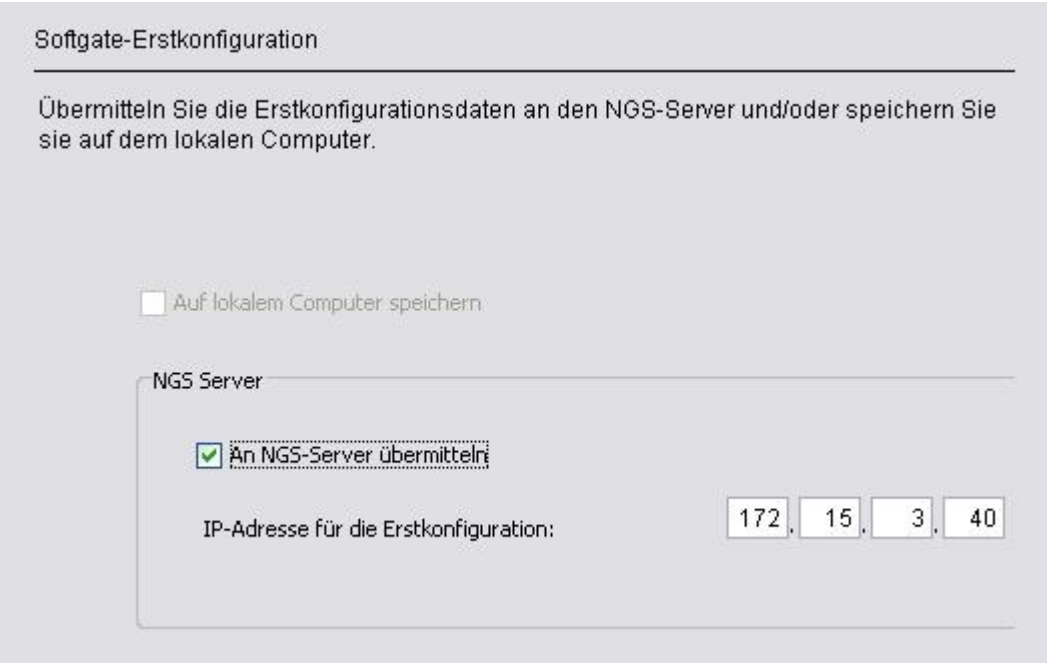


Figure 42: Zero Local Configuration for OpenScape 4000 SoftGate

The OpenScape 4000 SoftGates are registered in the NGS server database. All of these OpenScape 4000 SoftGates are displayed in the OpenScape 4000 Platform Administration (Portal) in the **System > SoftGates** menu.

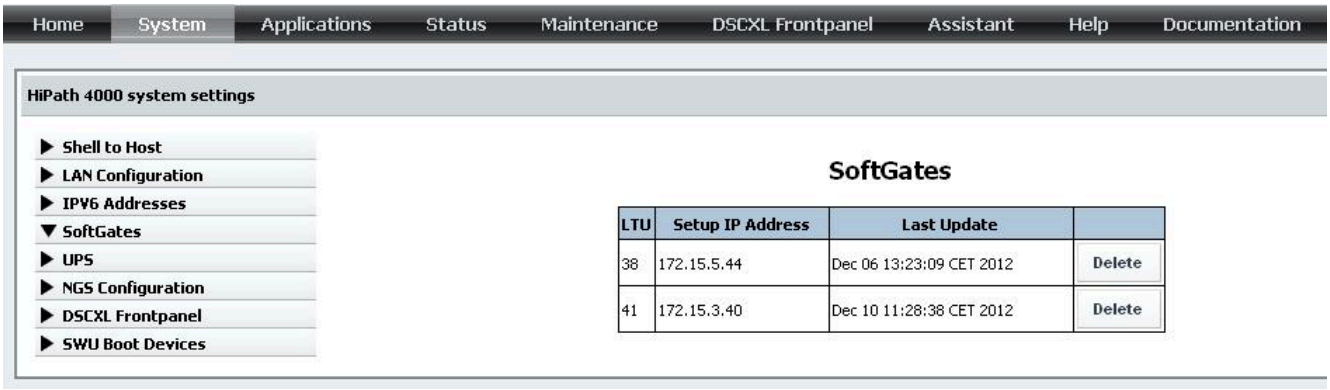


Figure 43: OpenScape 4000 SoftGates registered in the NGS database

2.5 Zero Local Configuration for Survivable OpenScape 4000 SoftGate

The Zero Local Configuration feature also allows installation of a Survivable OpenScape 4000 SoftGate.

The first installation of a stand-alone OpenScape 4000 SoftGate must be performed initially for this purpose (see Section 2.4, "Zero Local Configuration for Stand-Alone OpenScape 4000 SoftGate").

The OpenScape 4000 Platform Administration (Portal) can then be opened with the setup IP address assigned by the DHCP server.

IMPORTANT: If the OpenScape 4000 SoftGate has been configured with a separate customer LAN and IPDA LAN, then the OpenScape 4000 Platform Administration (Portal) can be accessed via the IP address of the customer LAN, which was assigned by a DHCP server in the customer LAN.

In the **OpenScape 4000 Platform Administration (Portal) > LAN Configuration > LAN Assistant** menu, the deployment can now be changed from **Standalone SoftGate to Survivable OpenScape 4000 SoftGate with local survivability unit SW(AP-E)**.

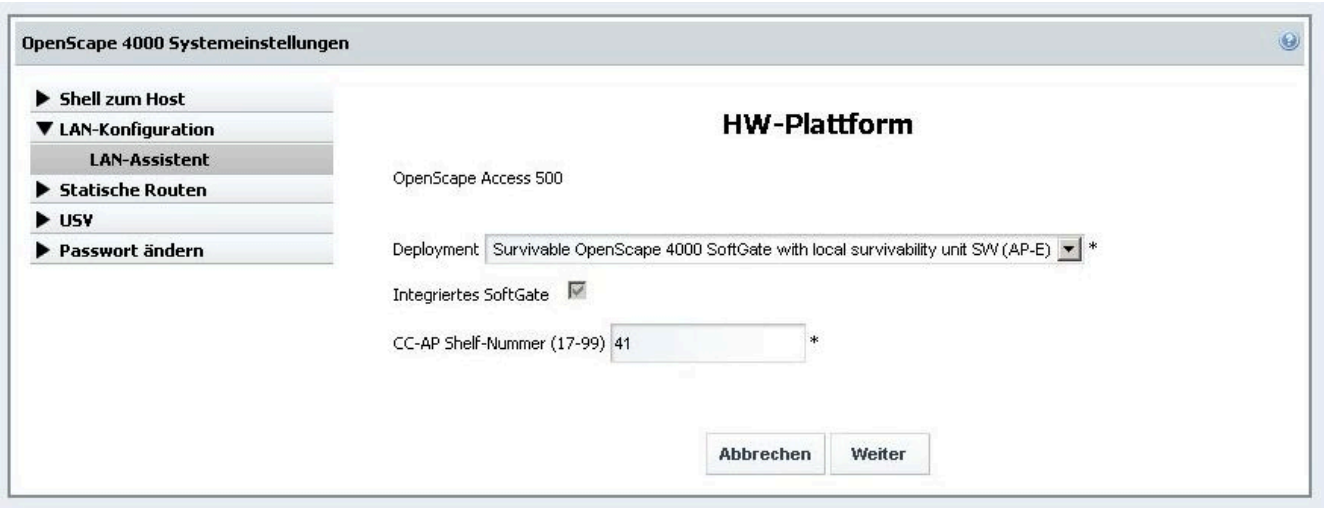
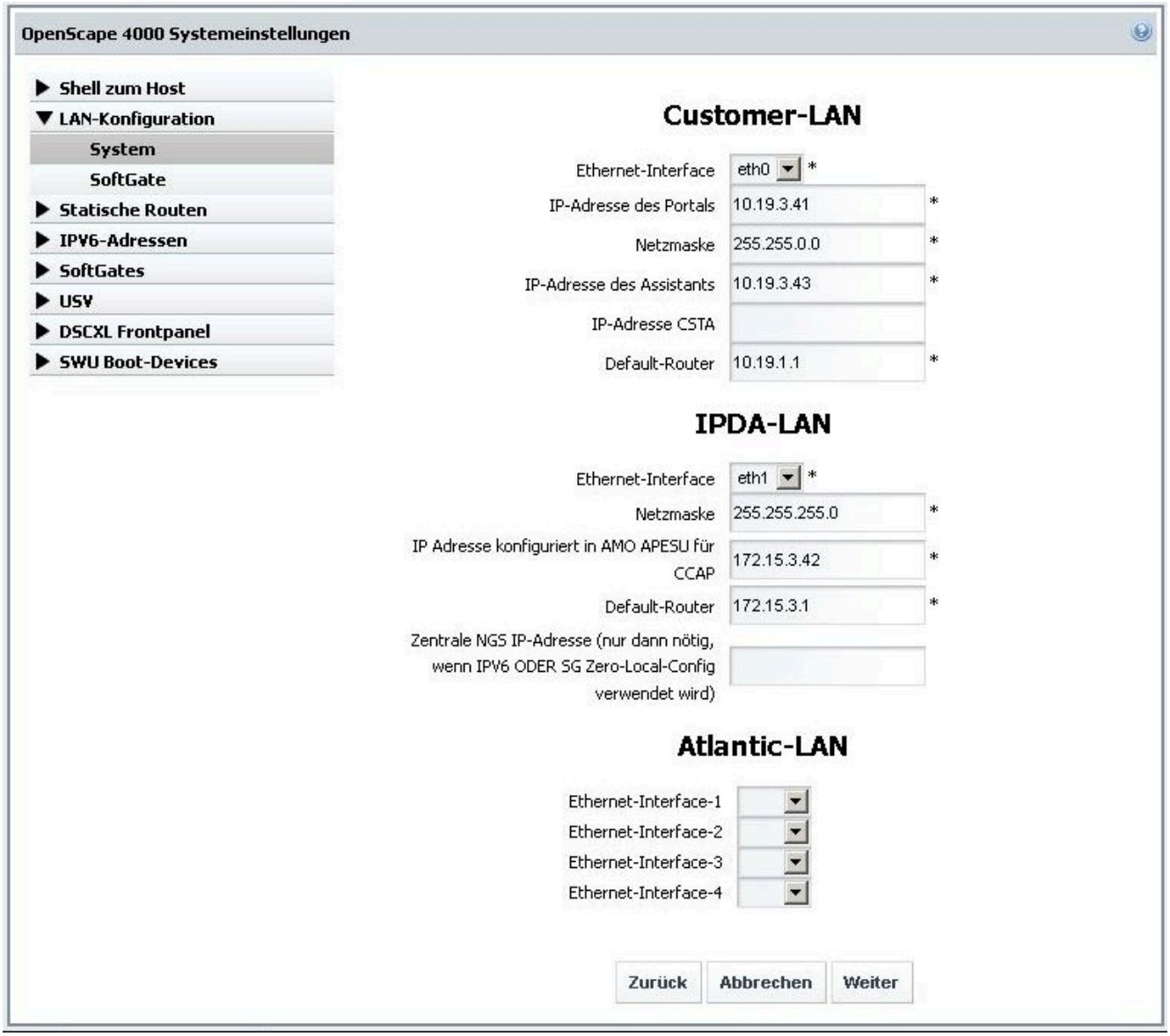
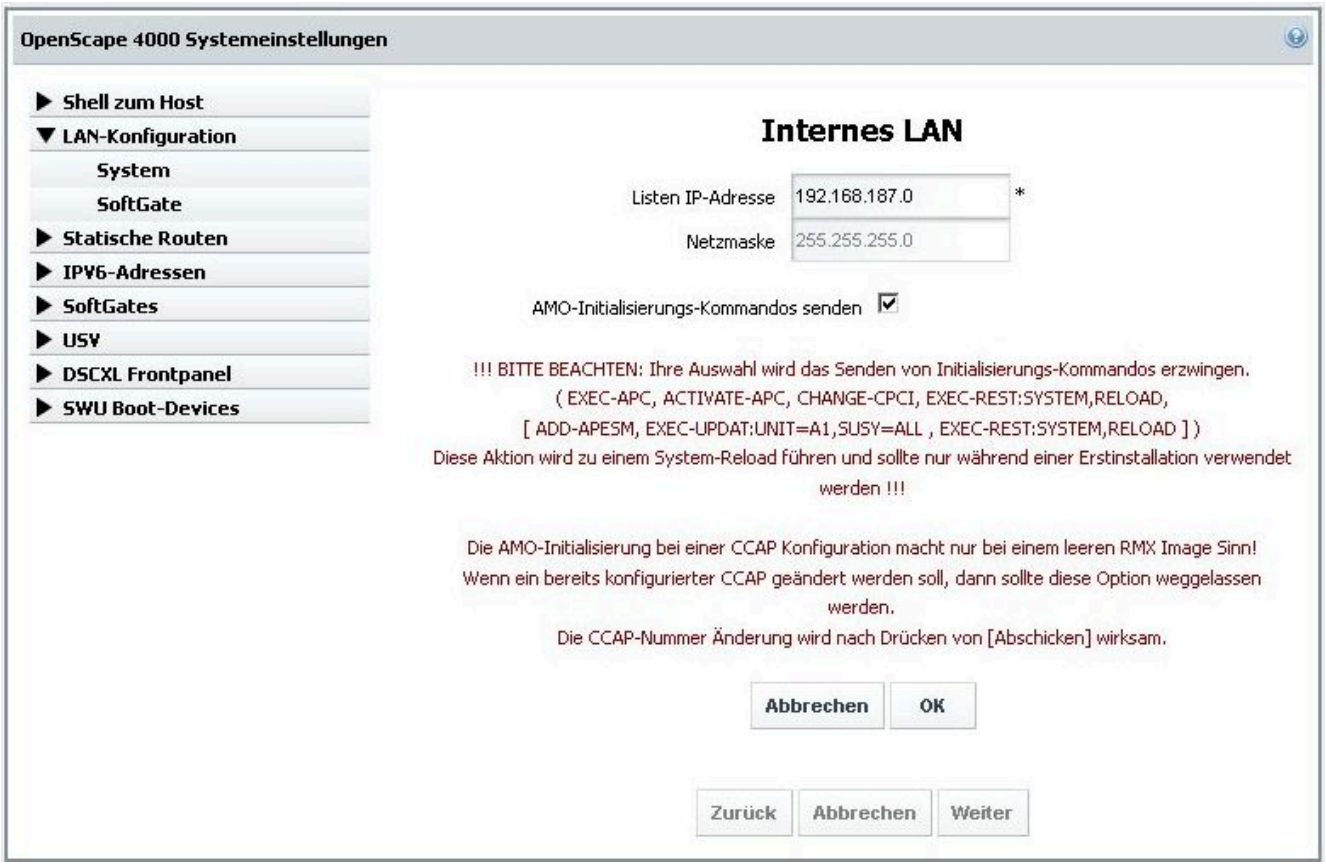


Figure 44: Zero Local Configuration - Change deployment

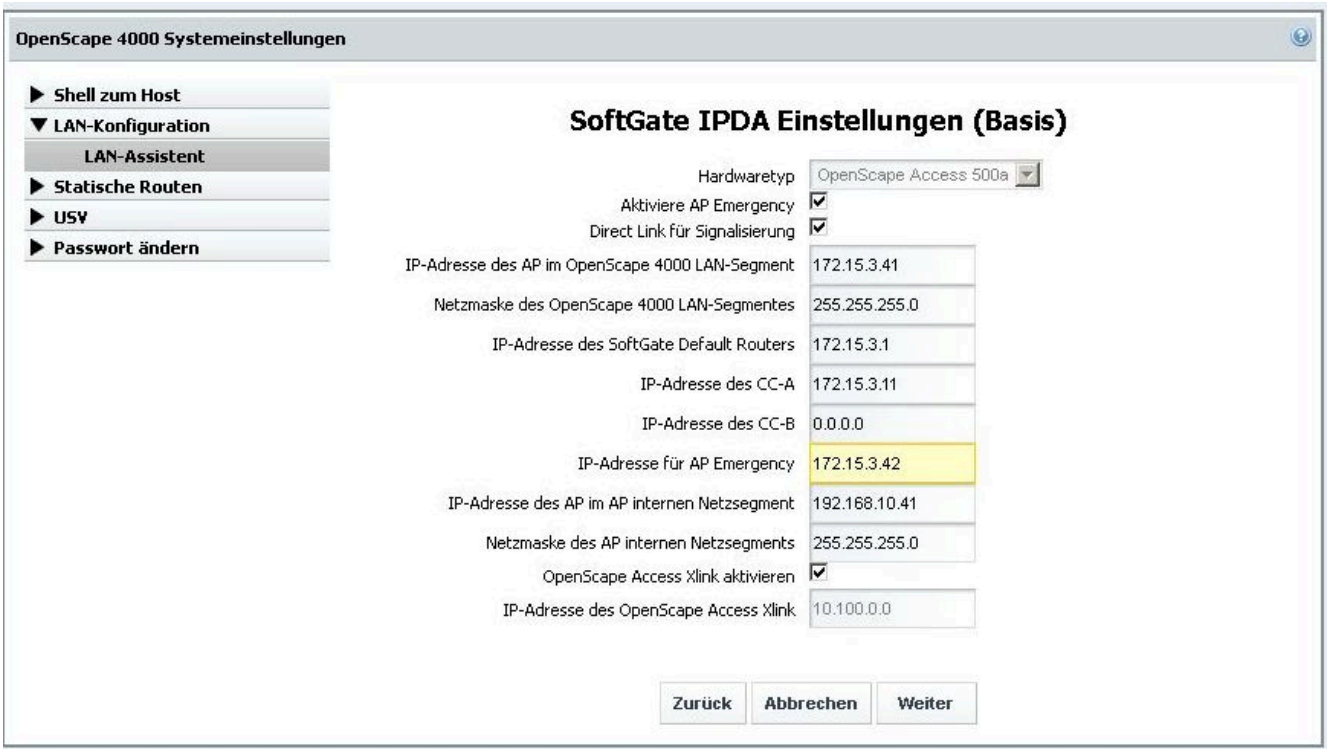
All of the settings required for AP-E operation are prompted in the next screens.


OpenScape 4000 Systemeinstellungen
Shell zum Host
LAN-Konfiguration
System
SoftGate
Statische Routen
IPV6-Adressen
SoftGates
USV
DSCXL Frontpanel
SWU Boot-Devices
Customer-LAN
Ethernet-Interface
eth0
IP-Adresse des Portals
10.19.3.41
Netzmaske
255.255.0.0
IP-Adresse des Assistants
10.19.3.43
IP-Adresse CSTA
Default-Router
10.19.1.1
IPDA-LAN
Ethernet-Interface
eth1
Netzmaske
255.255.255.0
IP Adresse konfiguriert in AMO APESU für CCAP
172.15.3.42
Default-Router
172.15.3.1
Zentrale NGS IP-Adresse (nur dann nötig, wenn IPV6 ODER SG Zero-Local-Config verwendet wird)
Atlantic-LAN
Ethernet-Interface-1
Ethernet-Interface-2
Ethernet-Interface-3
Ethernet-Interface-4
Zurück
Abbrechen
Weiter


OpenScape 4000 Systemeinstellungen
Shell zum Host
LAN-Konfiguration
LAN-Assistent
Statische Routen
USV
Passwort ändern
Internes LAN
Listen IP-Adresse
192.168.187.0
Netzmaske
255.255.255.0
AMO-Initialisierungs-Kommandos senden
Zurück
Abbrechen
Weiter



The screens with the OpenScape 4000 SoftGate settings then follow. These are already filled out fully with the exception of the IP address for AP Emergency.



2.6 Log Files

The installation log files can be found in the directory **_install_logs** of the USB flash image (unless from a DVD where no write access can be made) and in the system under

- /var/log/install-image.<timestamp>.log
- /var/log/kernel-messages.<timestamp>.log
- /var/log/first-ha-config.<timestamp>.log

3 OpenScape 4000 installation on VMware ESXi

Installation as a virtual machine is possible for the following deployments:

- Simplex with and without integrated SoftGate
- Standalone SoftGate
- Separated Duplex with and without integrated SoftGate
- Survivable with and without SoftGate

Corresponding OVF templates are available on the installation media, under **VMware_ovf** > **Templates**.

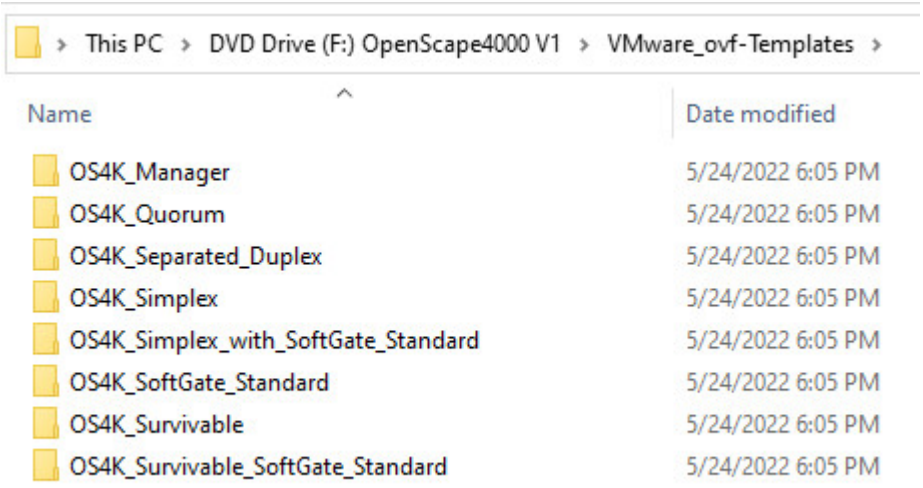


Figure 45: OVF templates

3.1 Important Notes

General Information

1) The VMware tools are installed as part of the Appliance Software. Updates of the tools are not permitted, for example via the vSphere administration interface.

   It may happen under certain circumstances that the graphical Sphere Administration interface issues a message stating that the tools are obsolescent. This is simply a display message in VMware and can be ignored.
2) Additional tools are required for the VMware installation as of OpenScape 4000 V10 or higher.

   These tools are located in the `\DriversAndTools \VMWare_Installation_Resources` directory and have to be copied to your local Windows PC.
3) Further general information and tips (e.g. details regarding dimensioning, general product information, VMware feature compatibility) can be found in **OpenScape Solution Set, OpenScape Virtual Machine Resourcing and Configuration Guide > 5 Virtualization Dimensioning Details > 5.4 OpenScape 4000**.
4) High swap-in latency: Swapping in pages is expensive for a VM. If the hypervisor swaps out a guest page and the guest subsequently accesses

that page, the VM will become blocked until the page is swapped in from disk. High swap-in latency, which can be tens of milliseconds, can severely degrade guest performance.

To prevent any RAM swapping effects of the hypervisor, please refer to the VMware memory management documentation.

5) Ensure **Forged Transmits** is also enabled - without the setting the Standby processor of RMX will not load.

NOTICE: Standard ESXi vSwitches use the default of **Accepted**, whilst ESXi distributed switches (VDS) use default of **Disabled**.

OpenScape 4000 System Installation

1) A valid and accessible DNS server must be configured in the `/etc/resolv.conf` file on all nodes on the Linux SOCO2 platform. The data for the DNS server is entered in the first installation XML file (see Section 3.11.2, "DNS Server").
2) If a connection is set up directly via the Atlantic LAN port, then **Promiscuous Mode** must only be configured under ESXi for the Atlantic LAN. This setting is also mandatory for Separated Duplex deployments (see Section 3.6.1, "Preparations on the ESXi Host").

NOTICE: The setting is not required if access is performed via OpenScape 4000 Expert Access (Comwin) using the OpenScape 4000 Assistant.

IMPORTANT: **Promiscuous Mode** must not be activated for other interfaces. This would increase the I/O unnecessarily for these virtual machines.

NOTICE: It is optional to remove the USB controller included in the OVF templates after the installation, by editing the Virtual Machine settings.

3.2 Required Software and Hardware

- ESXi environment Version V5.1 or higher

  NOTICE:

  ESXi environment Version V5.1 or higher is required for V10R0.

  ESXi environment Version V6.5 or higher is required for V10R1.

  IMPORTANT: vMotion is not supported with ESXi versions lower than V5.1U3. If you want to use vMotion, you must use ESXi V5.5 or higher.

- The CPU hardware must support Intel VT-x/EPT or AMD-V/RVI technology
- Service PC with Windows
- ISO file from SWS (ZIP file extracted to ISO)

For more information about the software and hardware requirements, please refer to the OpenScape Solution Set V10, OpenScape Virtual Machine Resourcing and Configuration Guide, Service Documentation, chapter 5.4 OpenScape 4000.

3.3 Information Required from the Customer

- Network identification names

  e.g.: Management, Voice, Atlantic
- First installation file `firstinst-netw-XXXXX.xml` (including the configuration data for OpenScape 4000 Softgate, if this is available)
- REGEN file for the RMX configuration
- Free IP address from the customer address range for the Service PC (for Service PC tasks, refer to Section 3.5, "Service PC")
- MAC address

3.4 Service PC

The Service PC is used for the following tasks:

- Accessing the OpenScape 4000 Assistant following the first installation
- Accessing the OpenScape 4000 with the assistance of OpenScape 4000 Expert Access (=Comwin) following the first installation
- Using the VMware environment
- Generating and adapting the configuration files
- Creating the installation floppy (see Section 3.12, "Generating a Floppy Image with the Content of firstinst-netw-*.xml")
- Creating the hotfix ISO file (see Section 3.13, "Preparing the Hotfix Installation")

3.5 Preparing the VMware Environment

3.5.1 Preparations on the ESXi Host

- Configure the port groups in accordance with the customer specifications in the virtual switches for the eth interfaces for Customer LAN, IPDA LAN, Atlantic LAN as well as Corosync LAN (only for Separated Duplex deployment).

  IMPORTANT: There are numerous possibilities for configuring the virtual switches. This depends on the customer's specifications. In our example, we have selected a separate virtual switch with its own physical network interface for every port group.

  IMPORTANT: This configuration should suffice in the virtual switch (**Standard Switch**) in the Staging Center. The configuration is often required however in the physical switch (**Distributed Switch**) in the customer environment.

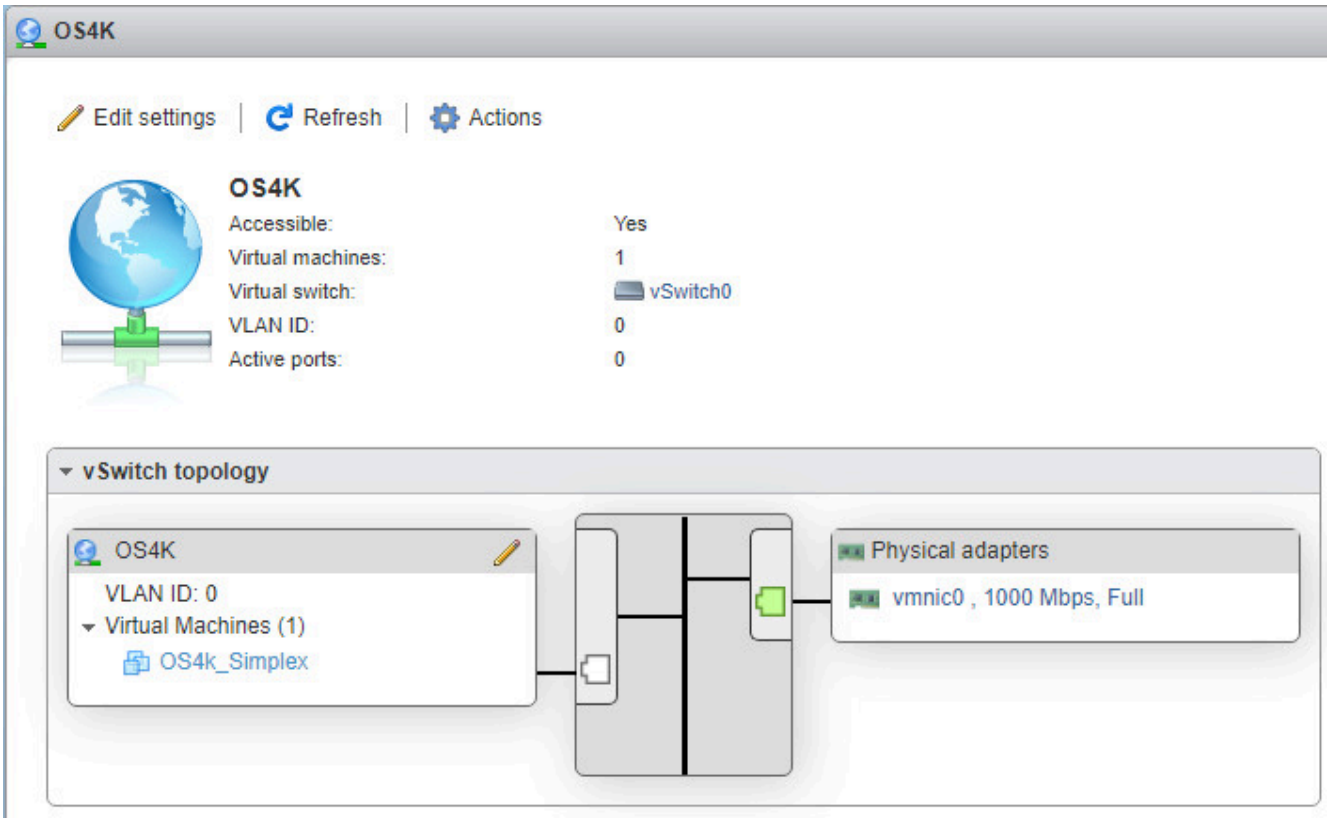


Figure 46: Default configuration of virtual switch following ESXi host installation

In order to add a virtual switch, click **Add standard virtual switch**.

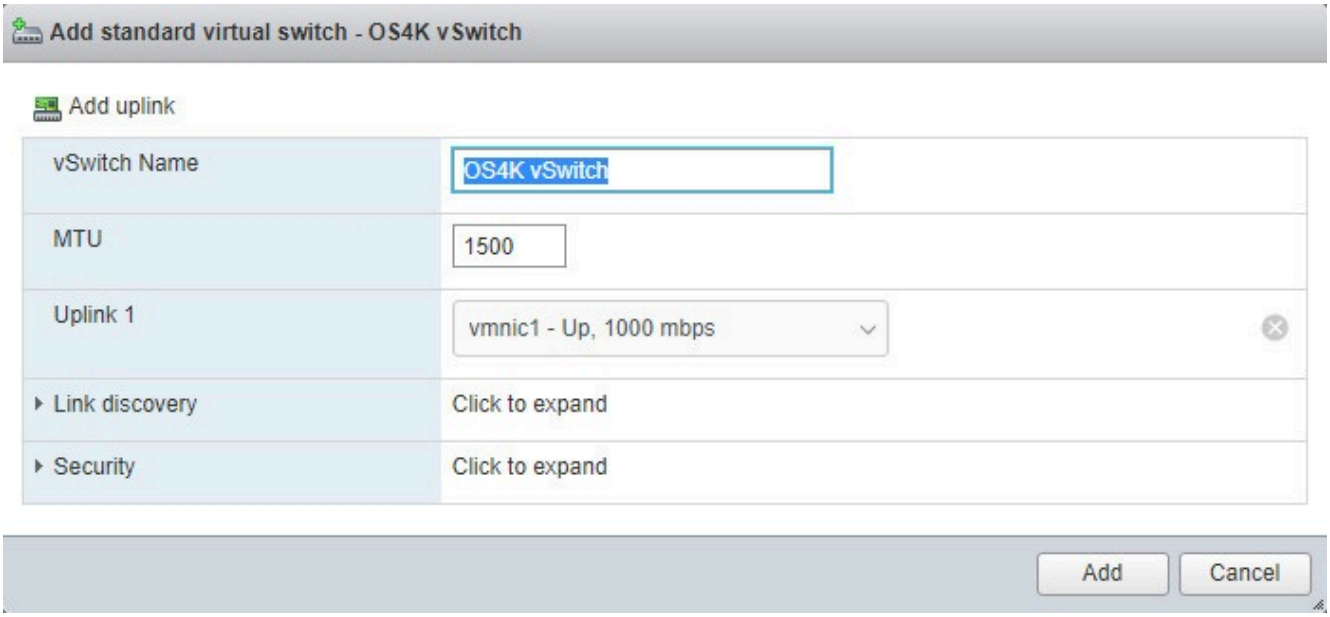


Figure 47: Adding a virtual switch

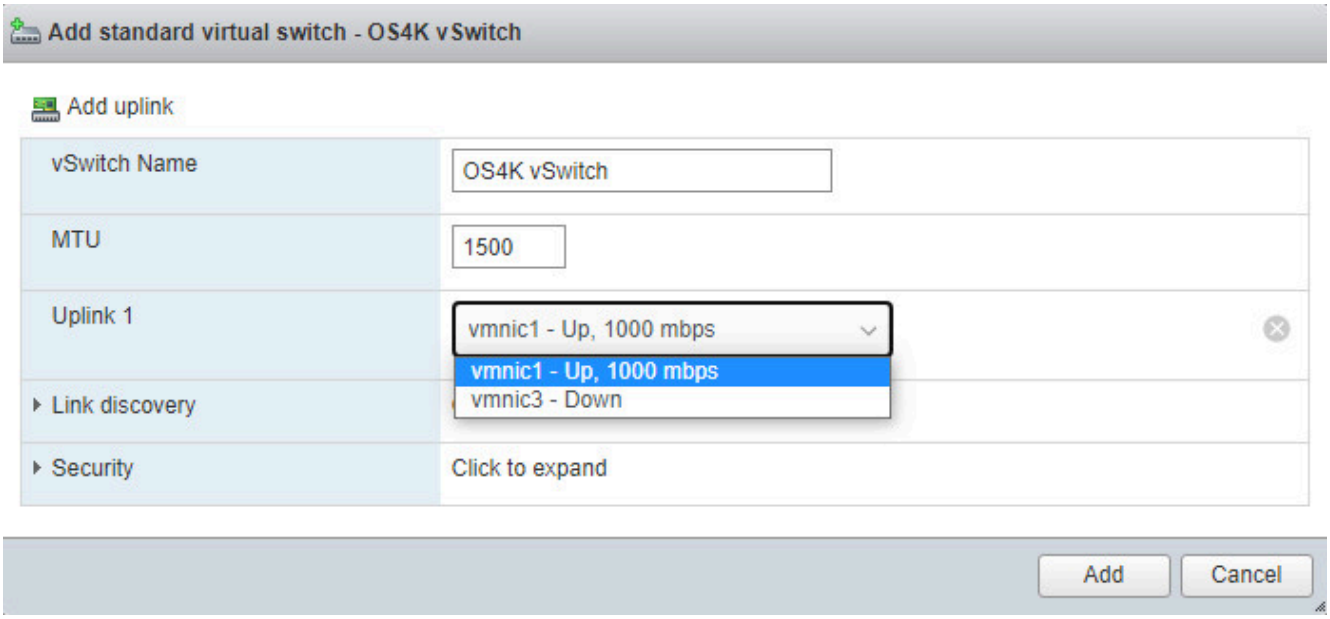


Figure 48: Physical network interface for virtual switch

Select the physical network interface that is to be added to the virtual switch. Click **Add** to continue.

In order to add a port group, click **Add port group**.

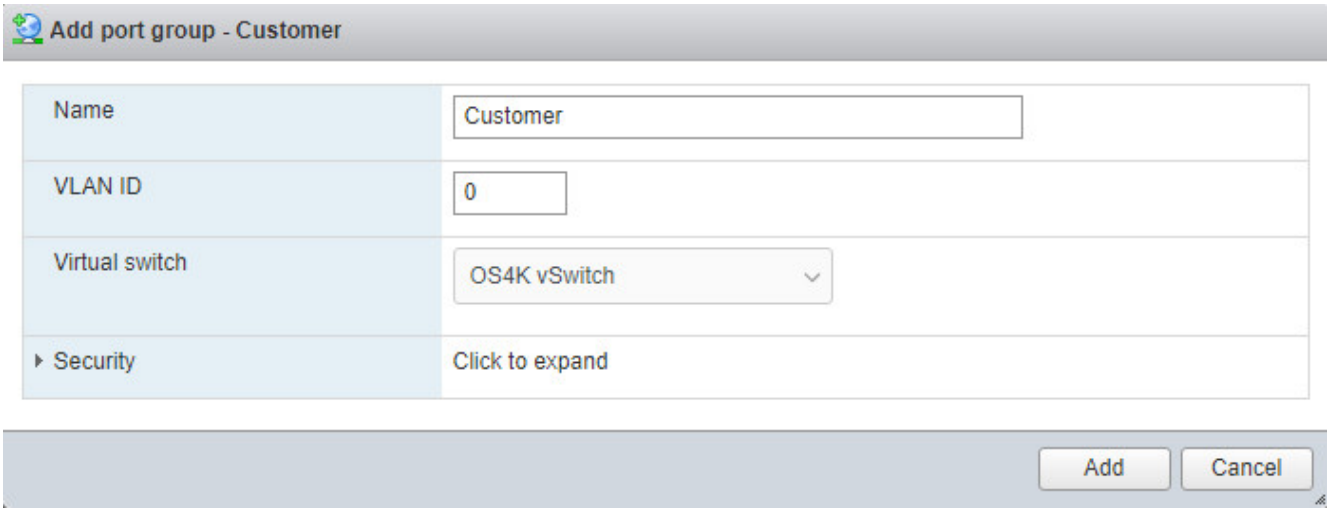


Figure 49: Name of port group

Specify the name of the port group (e.g. Customer). Click **Add** to continue.

The new virtual switch with the associated port group "OS4K Customer" and the physical network interface "vmnic1" is added to the network.

Also configure IPDA LAN and Atlantic LAN. In our example, each of these has its own port group, its own vSwitch, and its own physical network interface. The network overview then looks as follows:

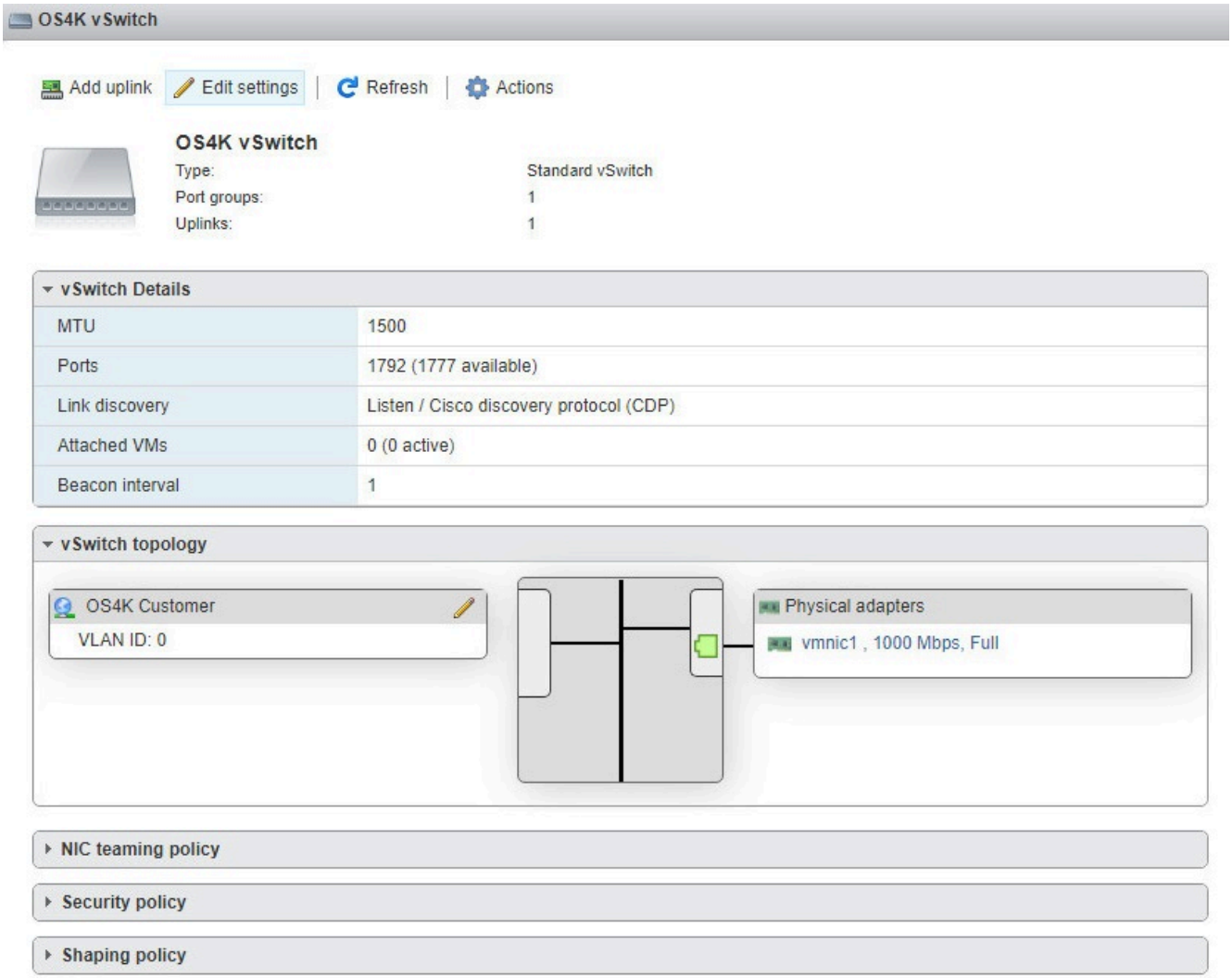


Figure 50: Network overview with three virtual switches (vSwitch 1)

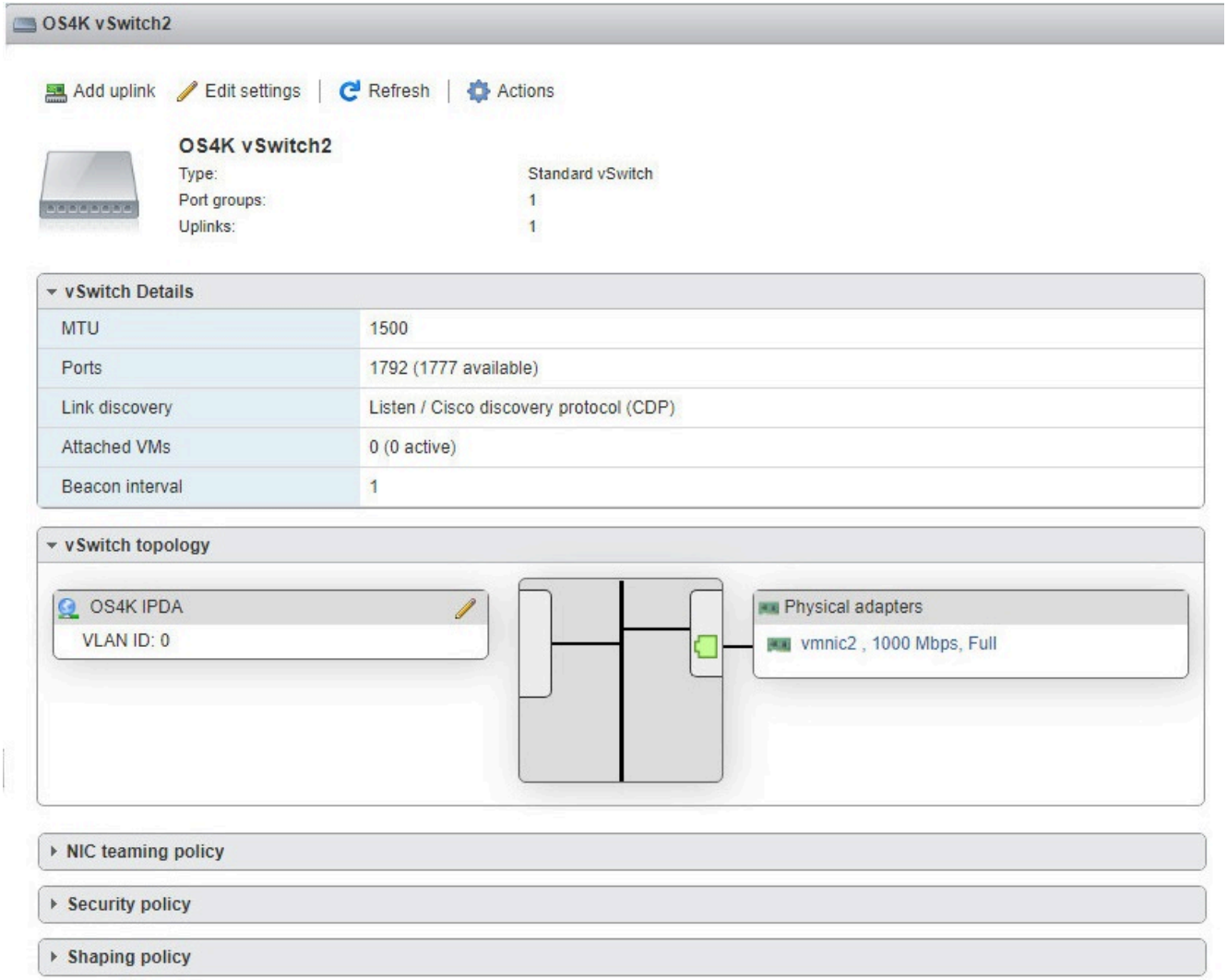


Figure 51: Network overview with three virtual switches (vSwitch 2)

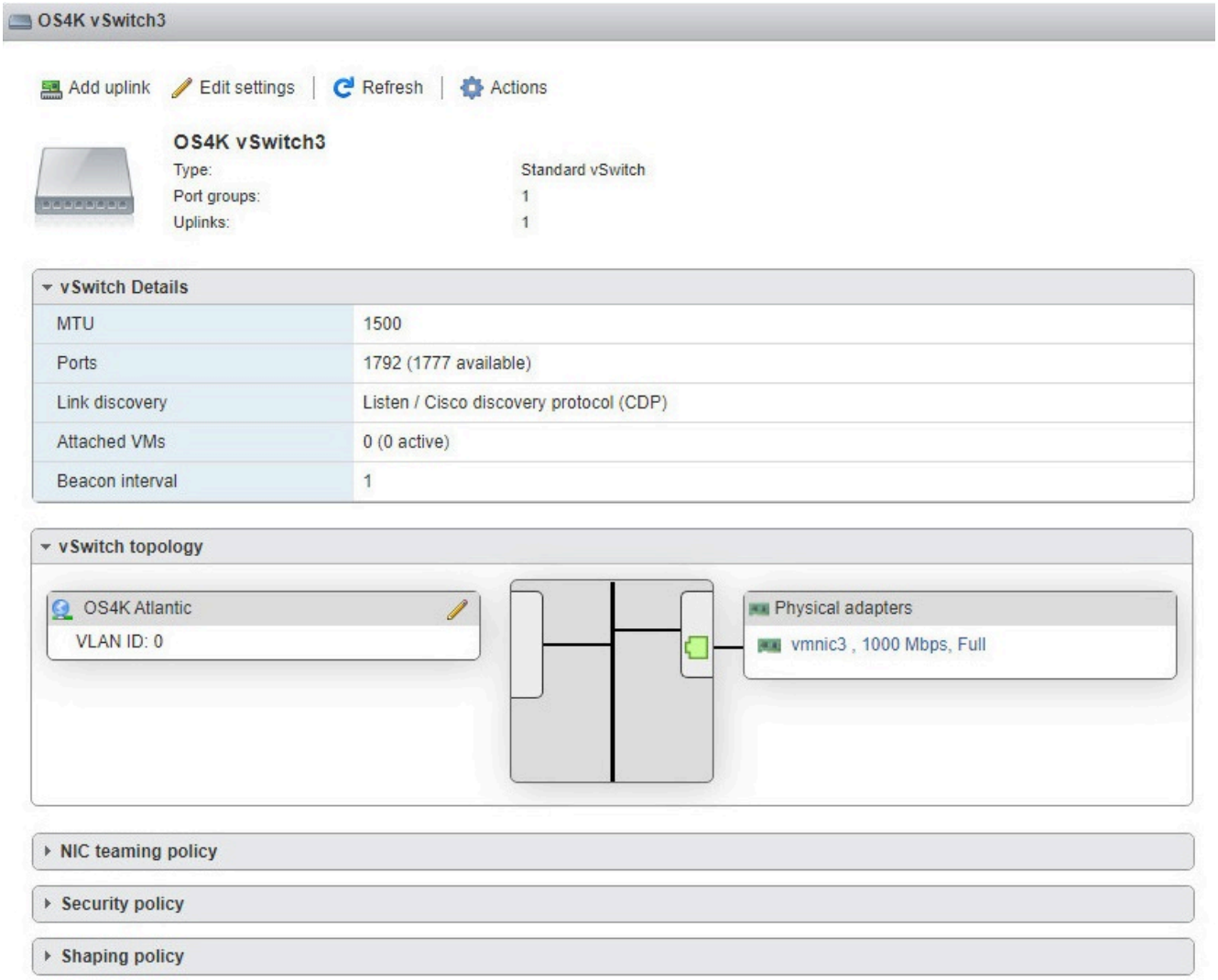


Figure 52: Network overview with three virtual switches (vSwitch 3)

- If the Atlantic LAN is to be accessed via OpenScape 4000 Expert Access then Atlantic LAN must now be set to **Promiscuous Mode**. This setting is also mandatory for Separated Duplex deployments.

  IMPORTANT: If this setting is not performed, the Atlantic LAN will not be accessible.

  NOTICE: Activating Promiscuous Mode on the virtual switch means that all incoming IP packets will be mirrored across all port groups and physical network interfaces as in a network hub. A separate virtual switch should therefore be configured if possible for the Atlantic LAN.

On the relevant host from the list of hosts, navigate to **Networking**.

In the **Virtual switches** tab, edit the settings of vSwitch3 (as displayed in our example), on which the port group "Atlantic" is configured. The Properties page for the virtual switch opens.

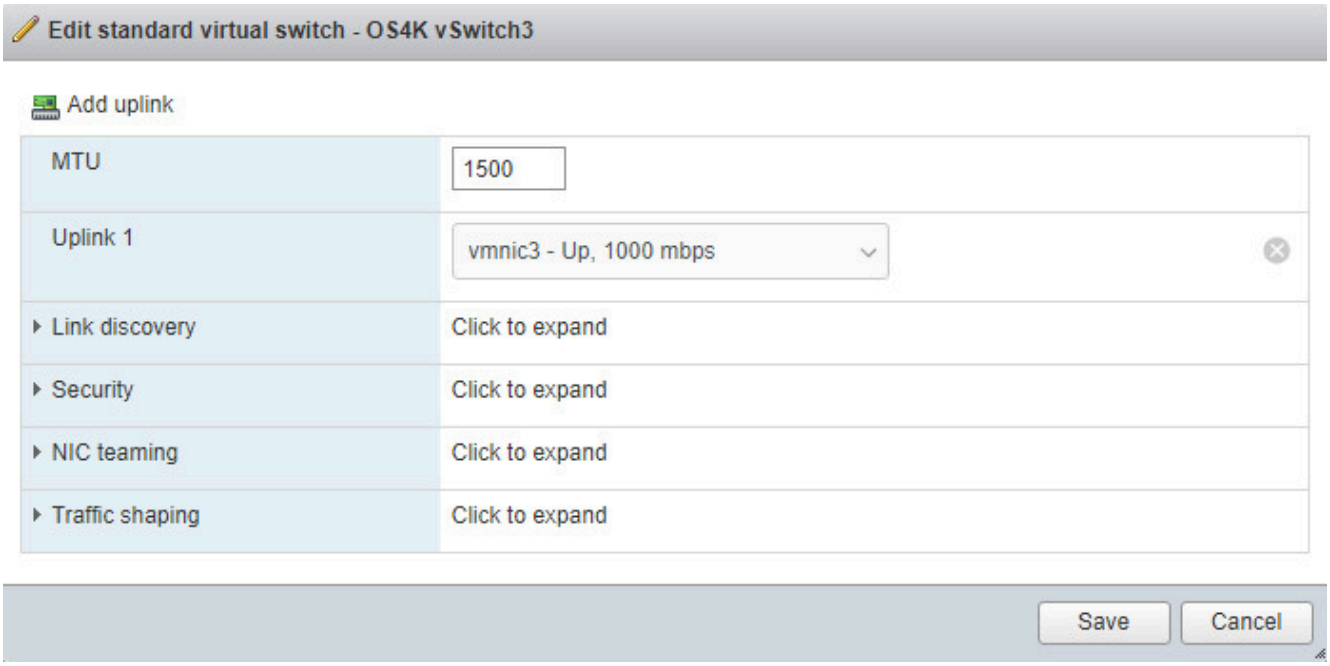


Figure 53: Properties of the virtual switch

Expand the **Security** tab.

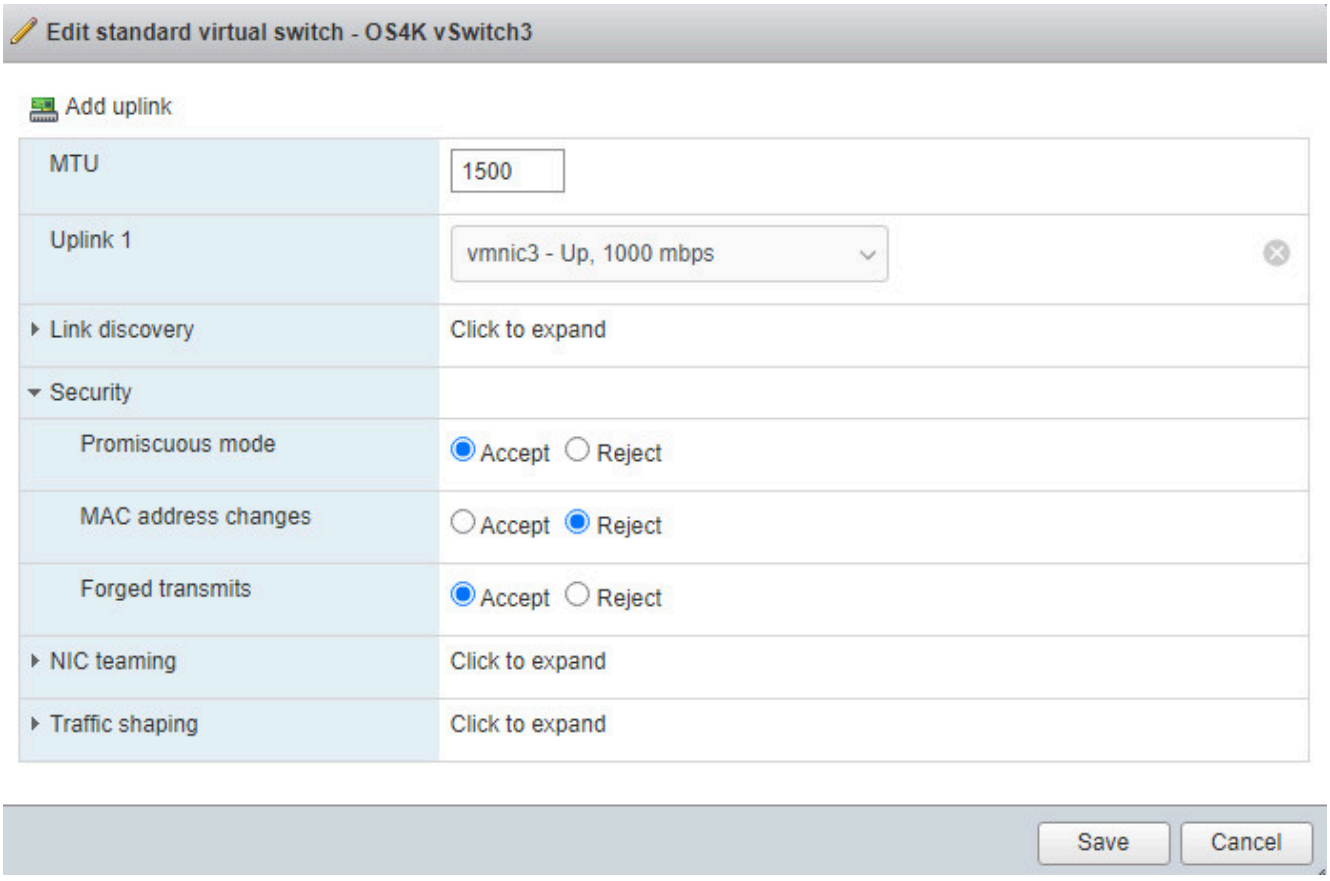


Figure 54: Promiscuous Mode for Atlantic LAN

Now set **Promiscuous Mode** to **Accept** on the **Security** tab.

Ensure **Forged Transmits** is also enabled - without this setting the Standby processor of RMX will not load.

Click **Save** to confirm the changes.

NOTICE: Standard ESXi vSwitches use the default of **Accepted**, whilst ESXi distributed switches (VDS) use default of **Disabled**.

3.5.2 Preparations on the Service PC

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

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

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

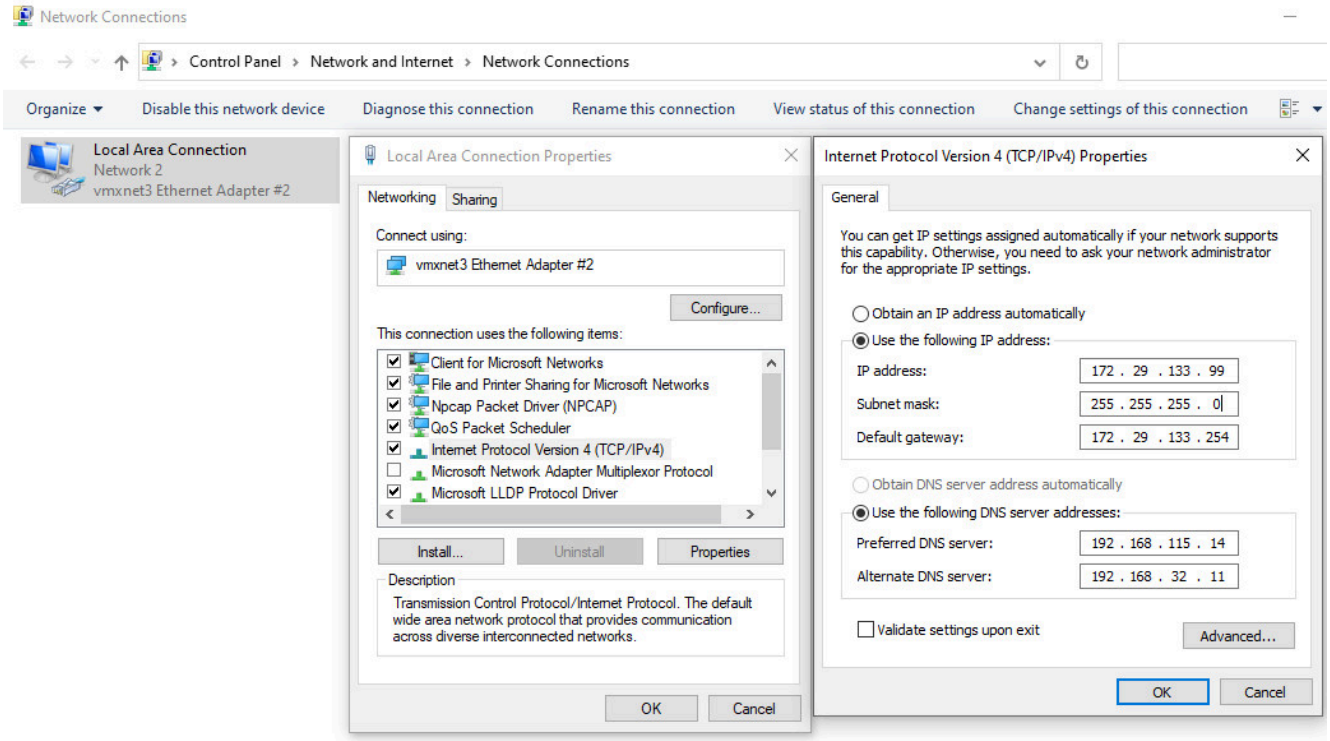


Figure 55: IP address and netmask example for the Service PC

- Create a working path on the PC for:
  - XML file
  - REGEN file
  - Floppy and image tools
  - Floppy image file
  - Log files
  - Hotfixes

- Copy the installation ISO file to a location that can be accessed by the vSphere Client (e.g. datastore).
- Extract the `VMware_ovf-Templates` directory from the `...InstallImage.iso` file.

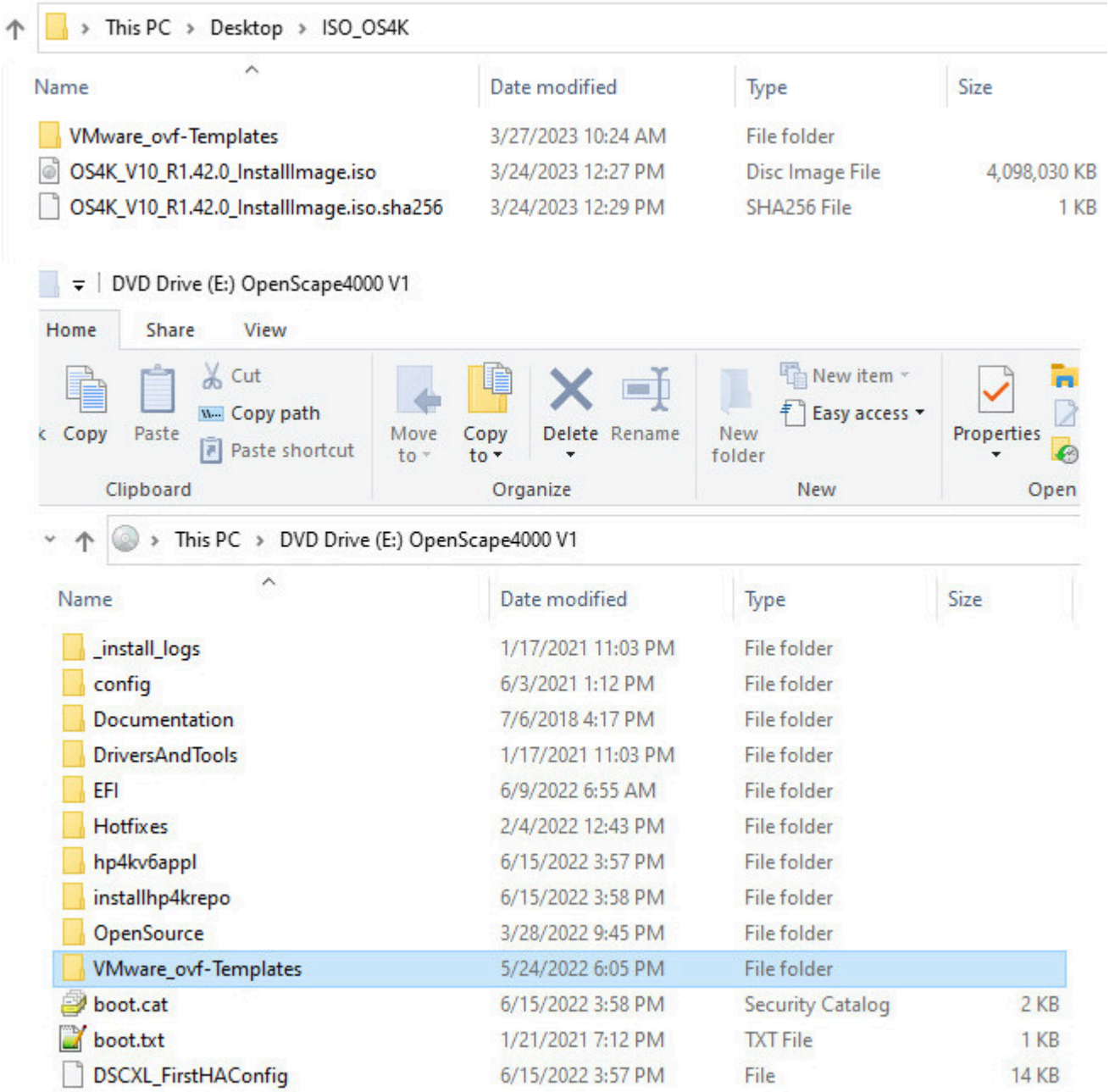


Figure 56: Extracting the "VMware_ovf-Templates" directory

These OVF templates have to be stored together with the ISO file on a datastore.

NOTICE: The content of these files is not changed and can be defined as read-only.

- Extract the `DriversandTools\VMware_Installation_Resources` folder into the previously created working path on the Service PC. This folder contains the floppy and image tools as well as a blank floppy image file.

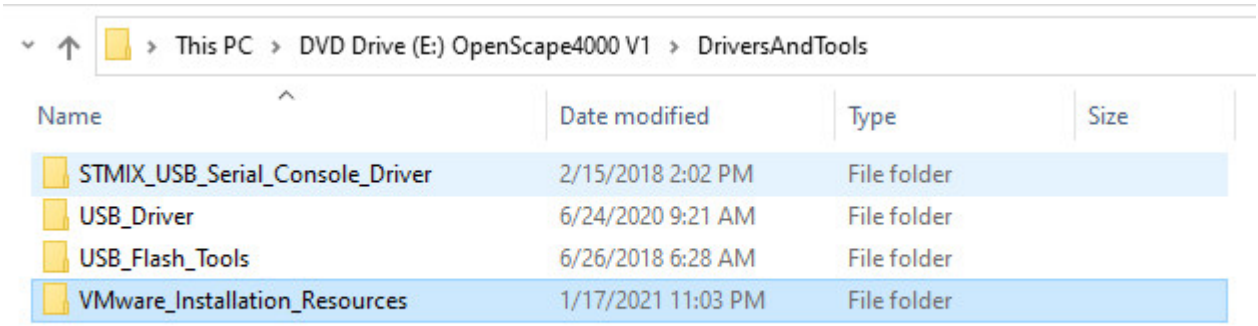


Figure 57: Extracting the "VMware_Installation_Resources" directory

- Copy the XML file to the working path.

  The content of the working path should now have the following content:
- Directories: mkisofs and mtools
- Files: empty.flp, getdir.bat, getlogs.bat, mk-iso.bat and prepare.bat and firstinst-netw-*.xml

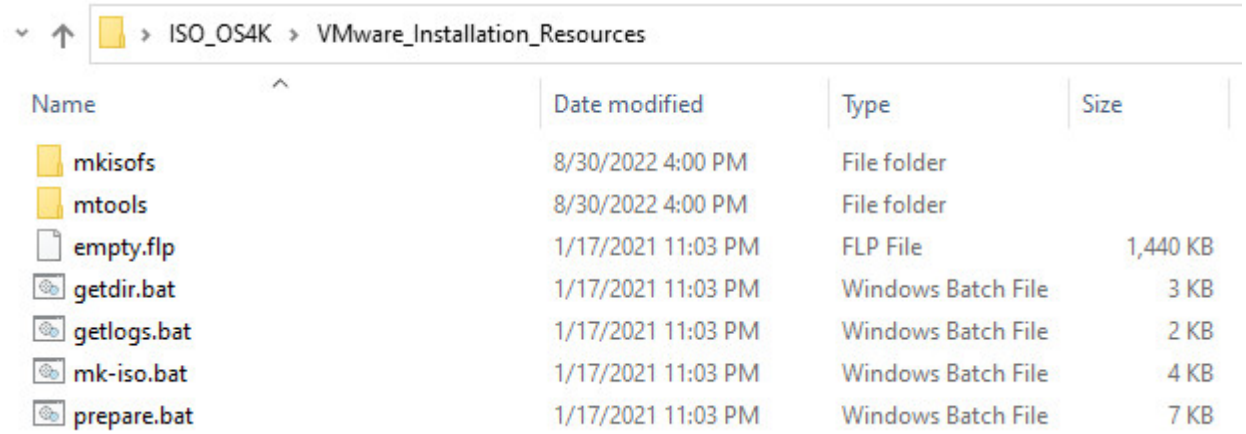


Figure 58: Content of working path on the Service PC

3.6 Dimensioning/Requirements of the Virtual Machine

The usage of the OS4k OVF templates is mandatory.

3.6.1 Dimensioning

The OpenScape 4000 requires certain resources that are defined when the virtual machine is created (importing of OVF template). These are:

- Number of CPUs
- Hard disk space required
- Size of RAM working memory

- Reservations for working cycle

The requirements for these resources vary depending on the OpenScape 4000 deployment to be installed. The precise dimensioning details can be found in the following documentation:

OpenScape Solution Set, OpenScape Virtual Machine Resourcing and Configuration Guide > 5 Virtualization Dimensioning Details > 5.4 OpenScape 4000

Number and type of LAN cards, DVD drives and floppy drives can be configured in accordance with customer requirements.

3.6.2 Hardware Virtualization

Hardware virtualization must be possible on the ESXi host in order to perform an OpenScape 4000 host installation. This is activated automatically when the OVF template is imported.

3.7 Importing an OVF Template (Example: Simplex)

IMPORTANT: The OVF import has to be performed for every node, in other words in the case of a separated duplex system, this OVF import and the subsequent installation have to be performed three times (Node 1, Node 2 and Quorum). The installation has to be performed three times because these are three separate virtual machines. The same applies for every OpenScape Softgate that is to be installed.

In VMware ESXi:

1) Right-click on **Virtual Machines** and select **Create/Register VM**

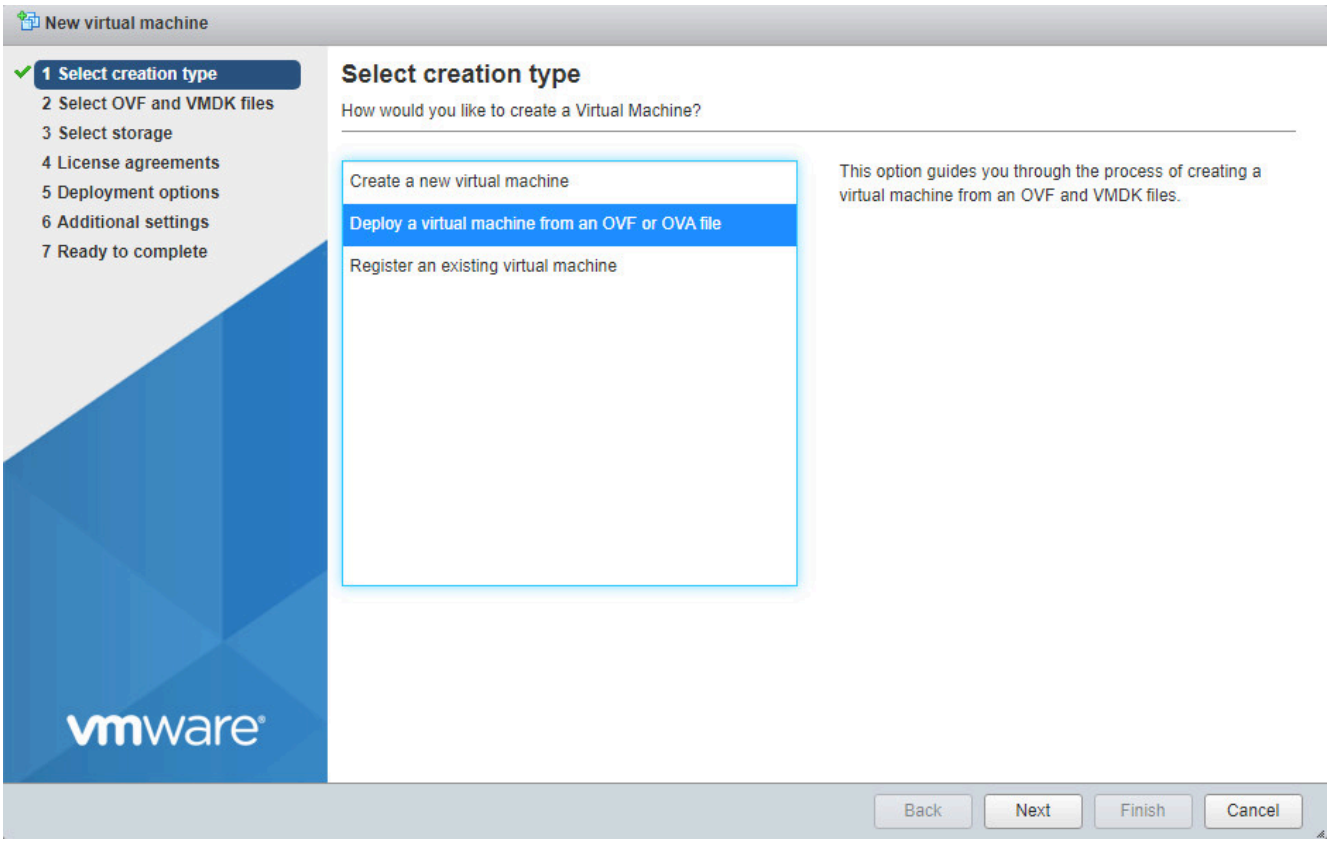


Figure 59: Importing OVF

2) Select the correct deployment (in this case: `OS4K_Simplex.mf`, `OS4K_Simplex.ovf`, `OS4K_Simplex-disk1.vmdk`).

NOTICE: The file names of the OVF templates are derived from the deployment being installed.

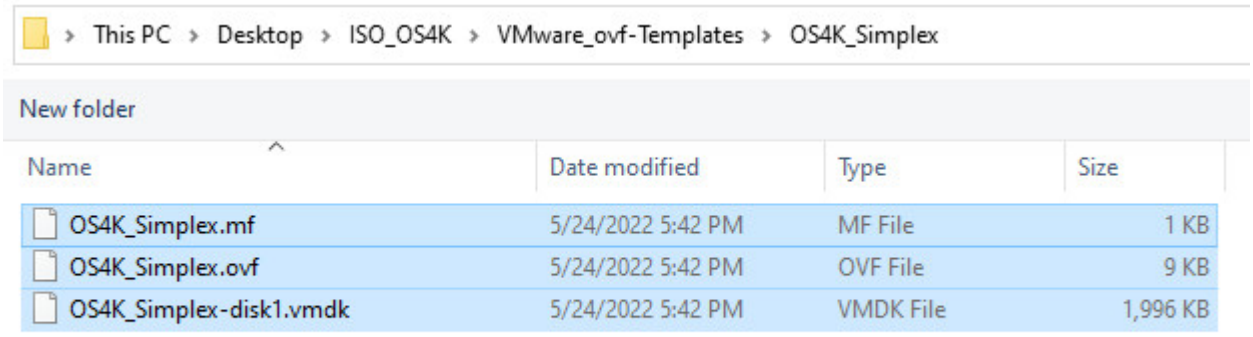


Figure 60: Selecting the deployment

Click **Open**.

3) Enter a name for the virtual machine.

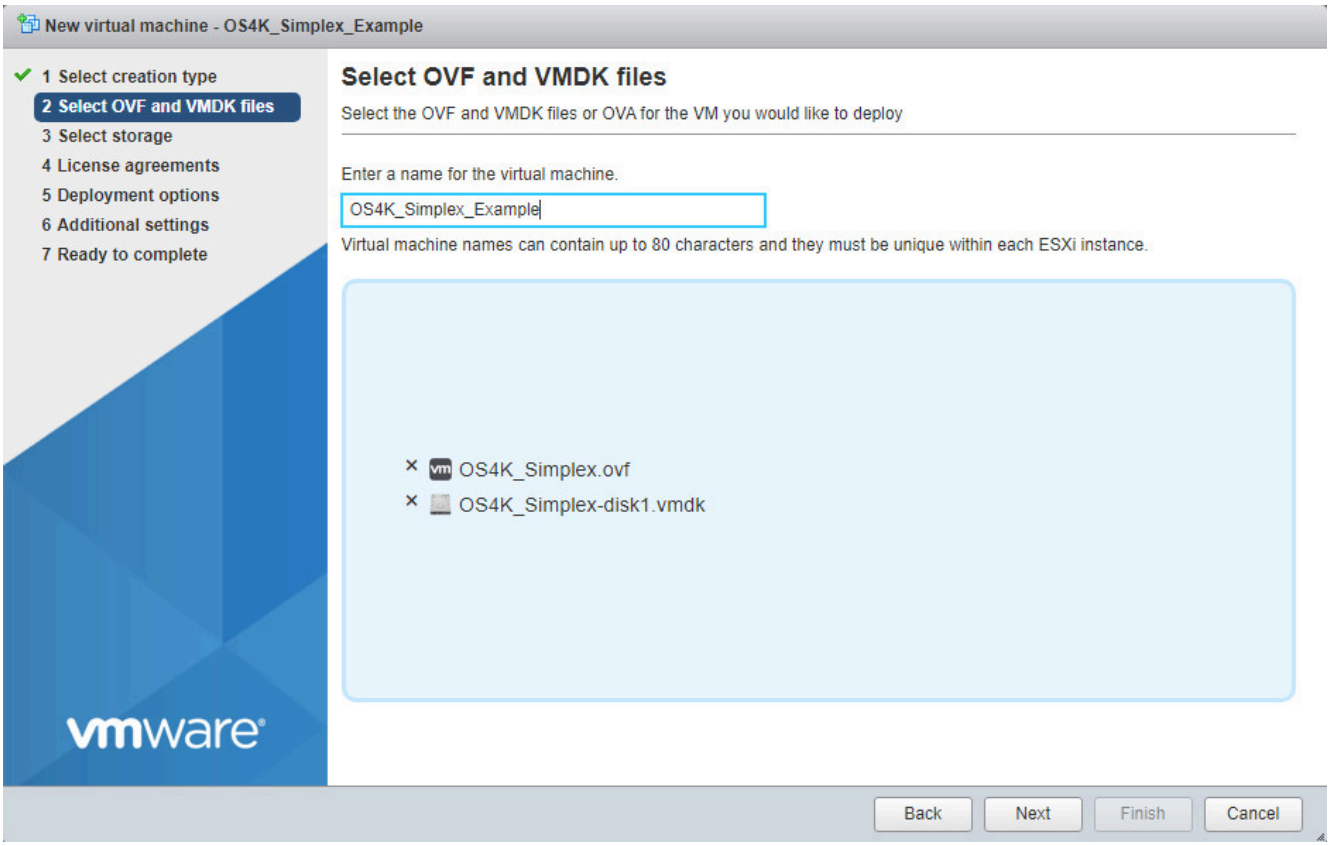


Figure 61: Naming the Virtual Machine

Click **Next**.

4) Specify the designated datastore.

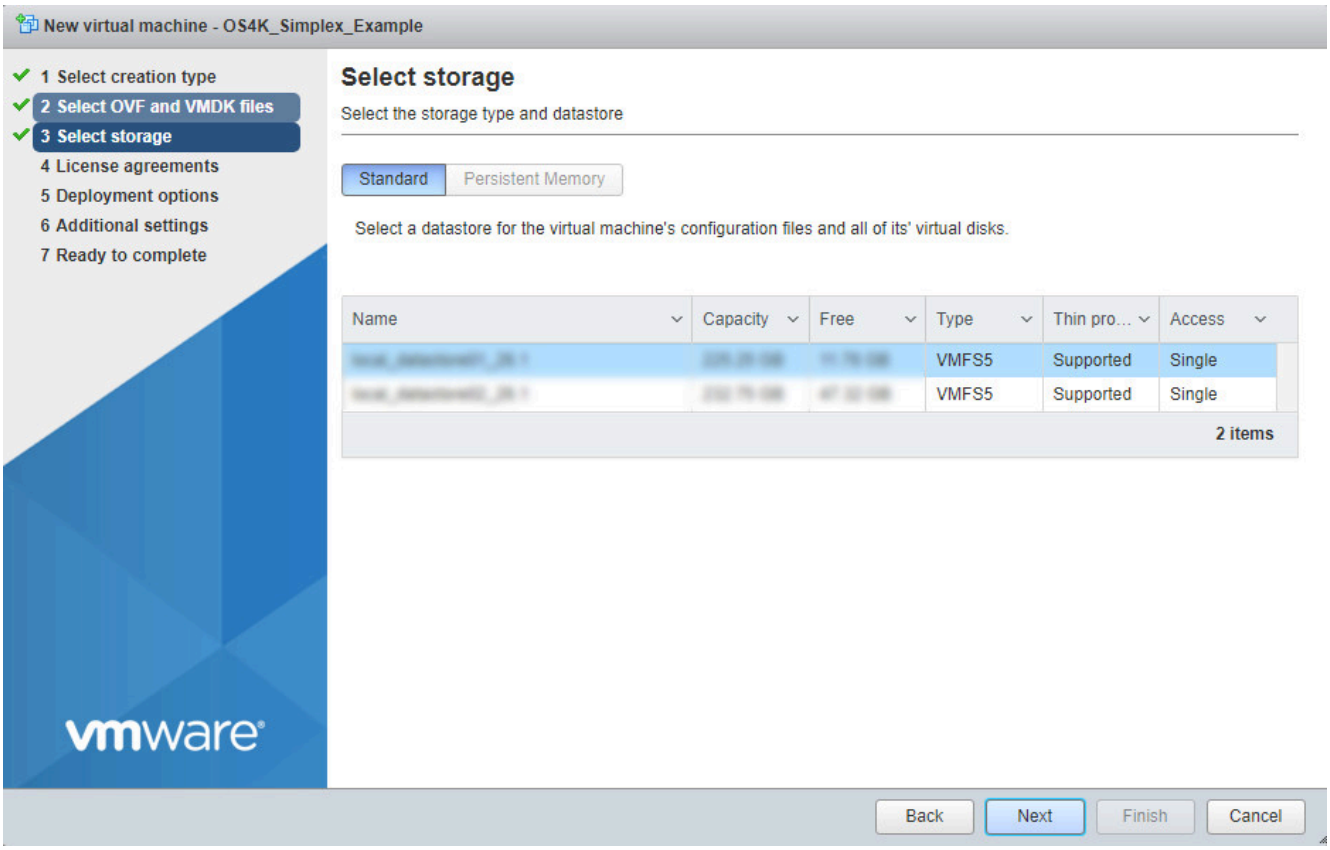


Figure 62: Select the storage for the Virtual Machine

Click **Next**.

5) Choose the specific network mappings.

NOTICE:

Check **Thick** for **Disk provisioning**.

Disable the **Power on automatically** option.

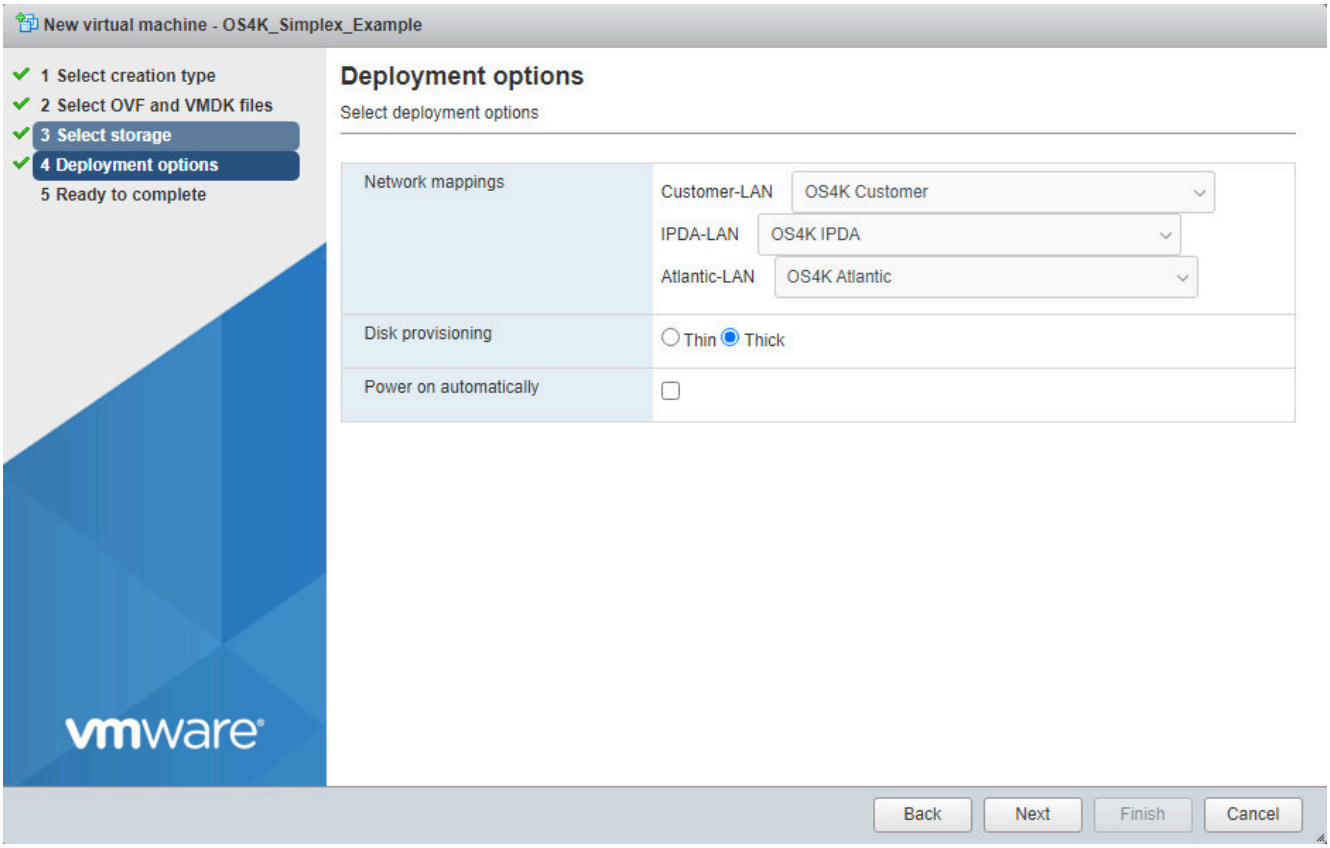


Figure 63: Deployment options

Click **Next**.

6) A summary is displayed.

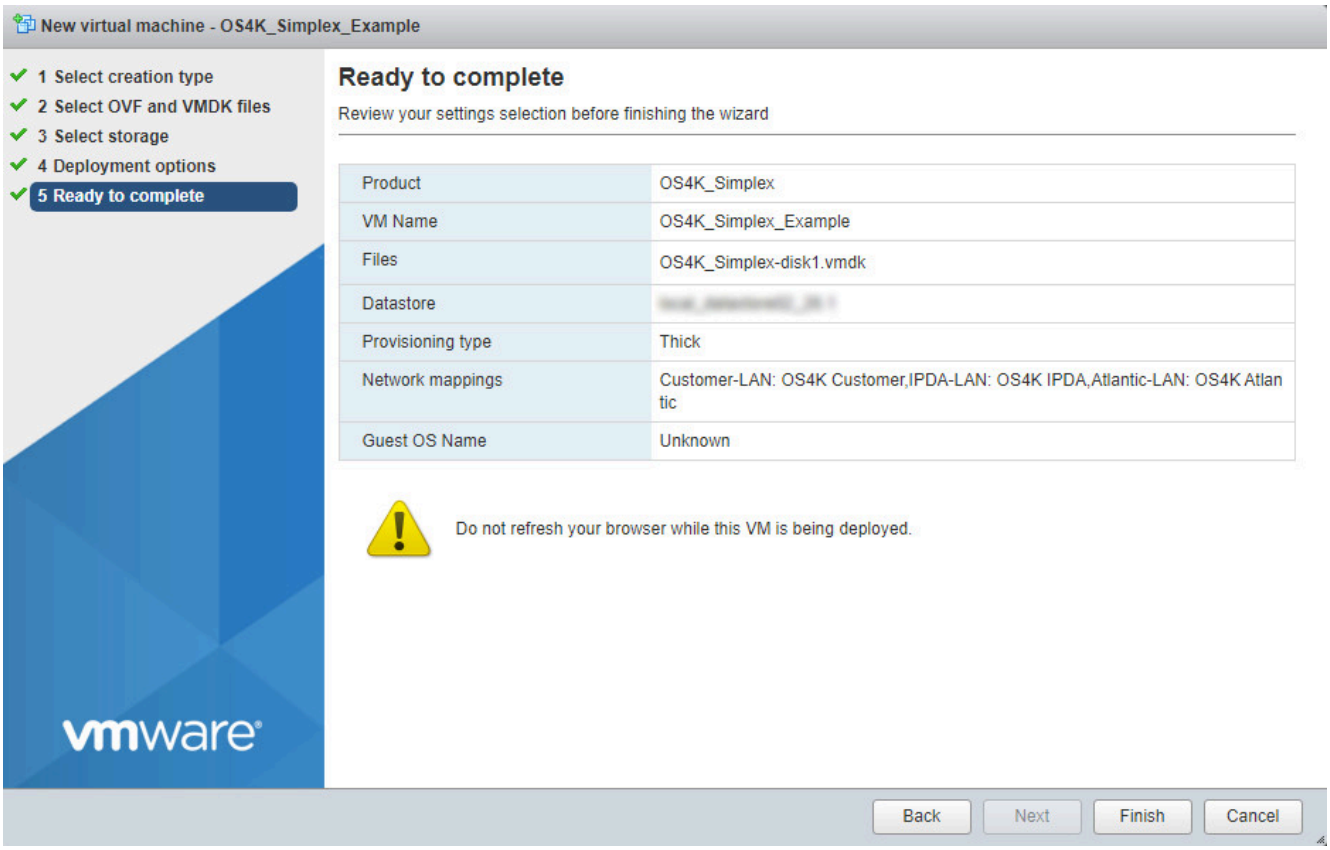


Figure 64: Summary (Ready to Complete)

Click **Finish**.

The virtual machine is now deployed and other settings can be made if needed.

3.8 CPU Settings

NOTICE: Custom may be displayed instead of High when deploying from OVF. Custom or High are both fine and the importance is the value of the reservations (which must meet the requirement listed in the OpenScape Virtual Machine Resourcing and Configuration Guide).

IMPORTANT:

Reservation must not be modified from the default 8000 Mhz.

The core(s) / socket(s) ratio should always be set to **all cores / one socket** (e.g. 4 cores / 1 socket).

VMWare sets by default the Cores per Socket value to 1, which means the CPU will have 1 core/multiple sockets.

It is recommended to change this setting after deploying the OVF. **Edit VM Settings** > **Expand CPU settings** and configure

> **Cores per socket** parameter to be equal with the CPU number resulting in all cores/one socket.

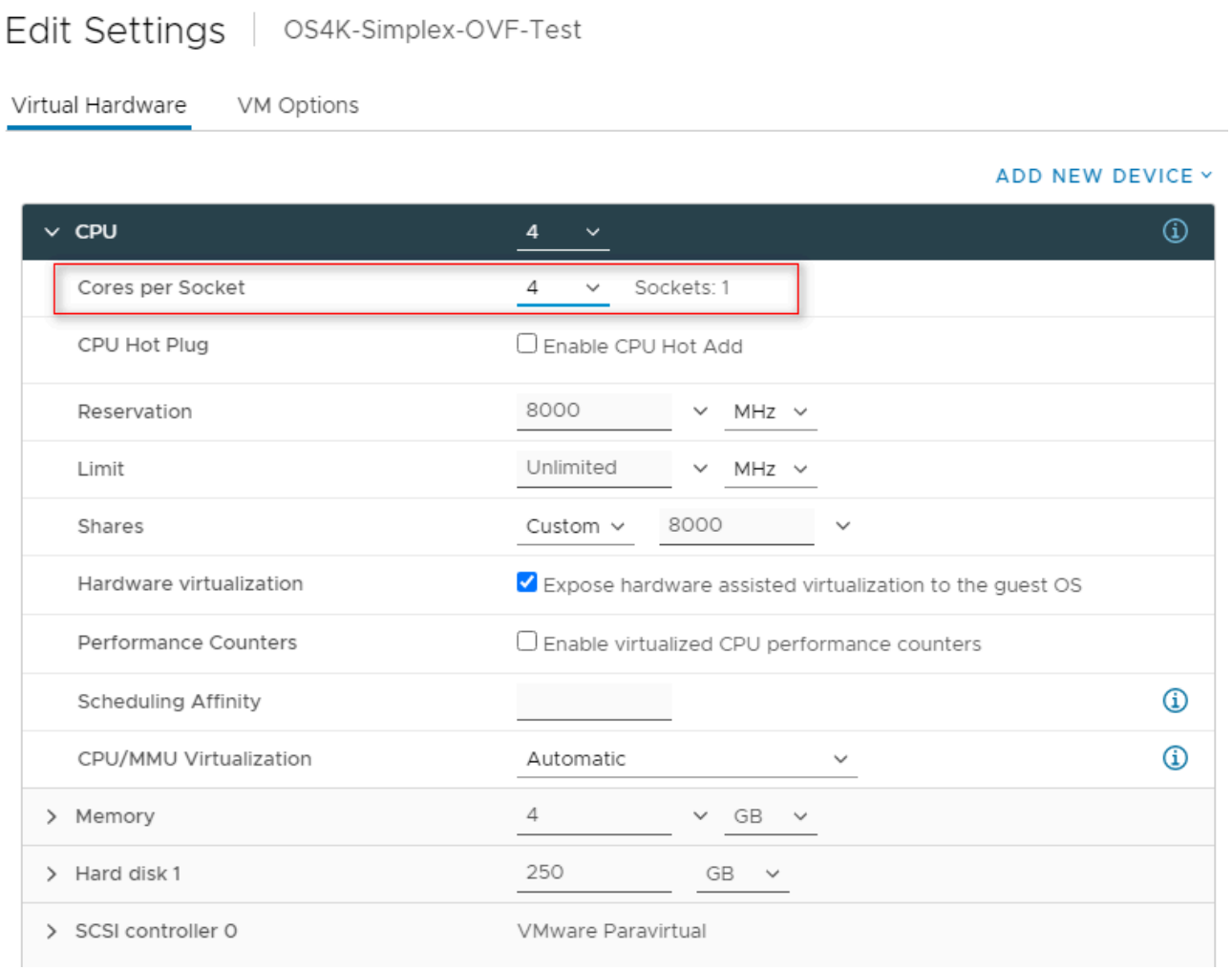


Figure 65: Setting Cores per Socket

3.9 Disconnect unused Network Adapters

IMPORTANT: After OVF deployment it is imperative to disconnect any network adapters not used.

E.g. for a Simplex Deployment where the Administration and IPDA LAN are shared on eth0 and there is no ATLAN connection, then Network Adapters 2 & 3 should have the **Connect...** flag removed.

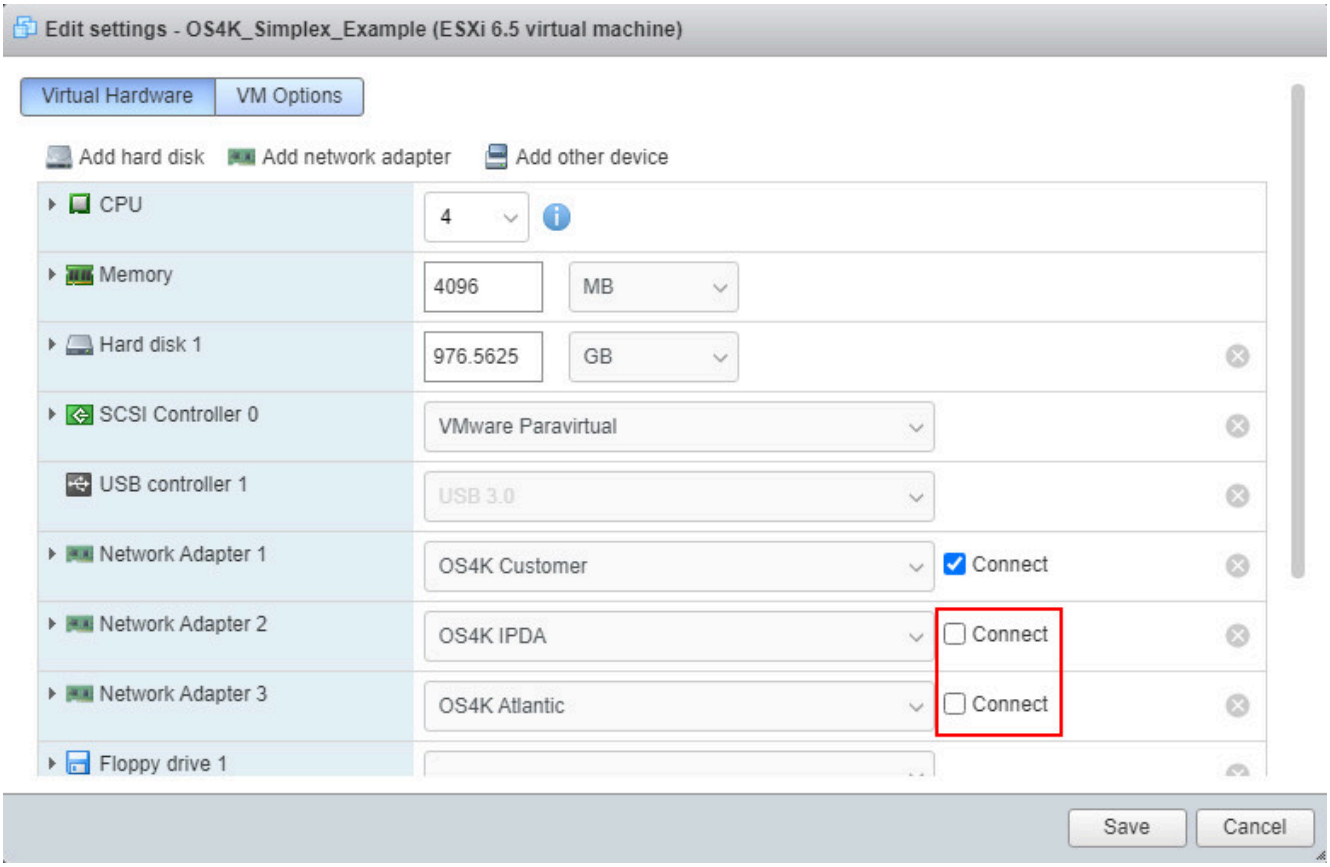


Figure 66: Disconnect network adapters

3.10 Generating a First Installation XML File

The `firstinst-netw*.xml` file is created as usual. The MAC address and the IP address of the DNS server must now be entered, as described in the MAC Address on page 99 and DNS Server on page 102 chapters.

3.10.1 MAC Address

The `firstinst-netw*.xml` file is created as usual and must then be supplied with the MAC address.

Enter the MAC address of the network card of the virtual machine at the relevant position in the `firstins-netw-*.xml` file.

```
<entry key="mac-address">mac-address of network card in
 virtual machine</entry>
```

3.10.1.1 Transferring the Automatically Generated MAC Address (standard case)

The MAC address is generally visible when the OVF template has been imported.

NOTICE: In some environments, the MAC address is only generated when the machine has been started. You then have to start the virtual machine and stop it again immediately in order to get the MAC address.

Search for the automatically generated MAC address and then enter this in the `firstinst-netw-*.xml` file.

Select the virtual machine and right-click on it. Then, select **Edit Settings** and expand the **Network Adapter 1** section. The MAC address is available in the **MAC Address** area.

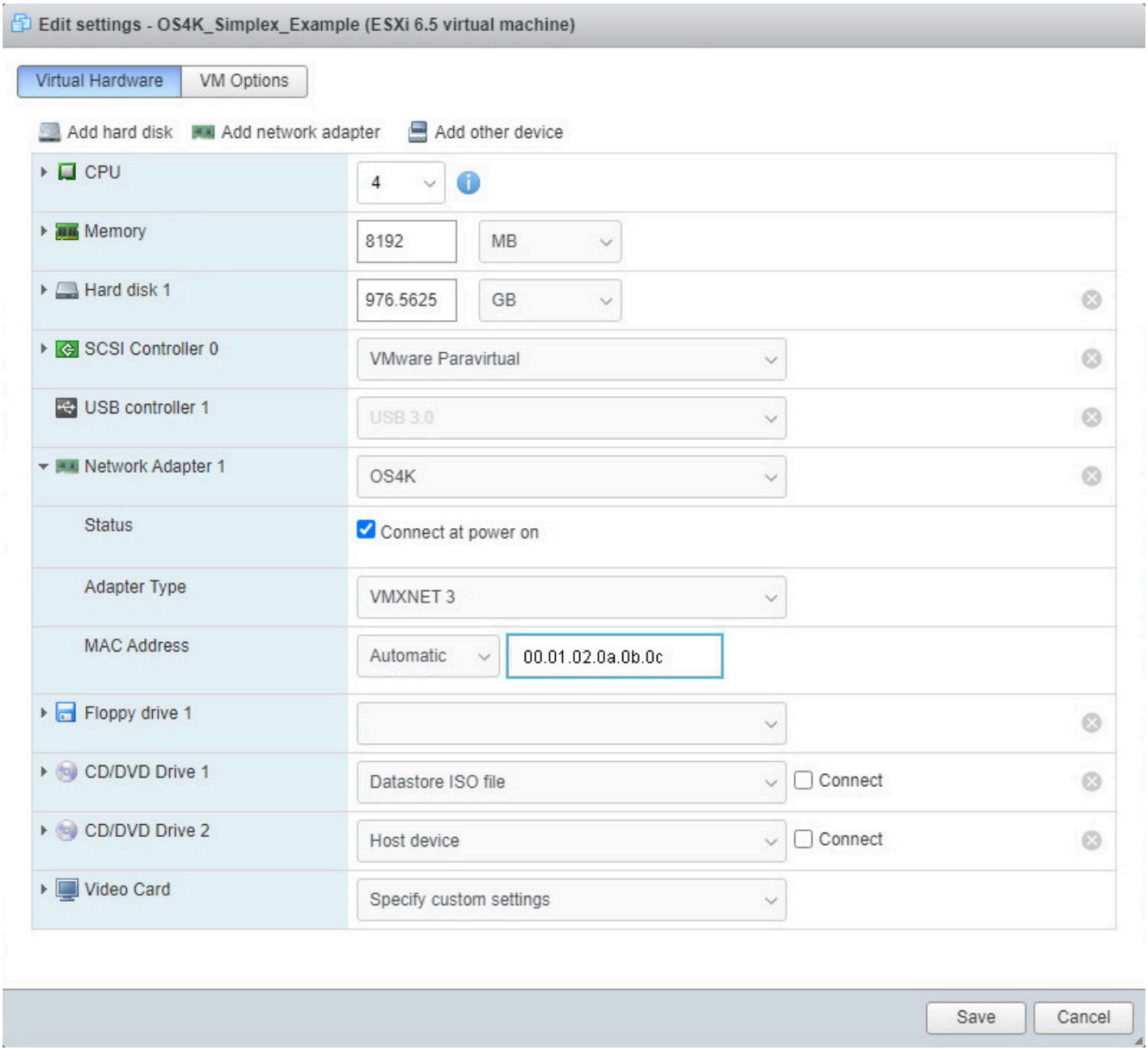


Figure 67: Automatically assigning the MAC address of the virtual machine

3.10.1.2 Transferring the Manually Generated MAC Address (Staging Center)

According to current Service requirements, the customer's valid license is to be used in the Staging Center. The MAC address requested and supplied by the customer has to be entered for this purpose.

IMPORTANT: Only a MAC address that has been created manually by the customer can be entered. An automatically generated MAC address cannot be entered manually.

Select the virtual machine and right-click on it. Then, select **Edit Settings** and expand the **Network Adapter 1** section. The MAC address is available in the **MAC Address** area.

Select **Manual** from the drop-down menu and enter the MAC address.

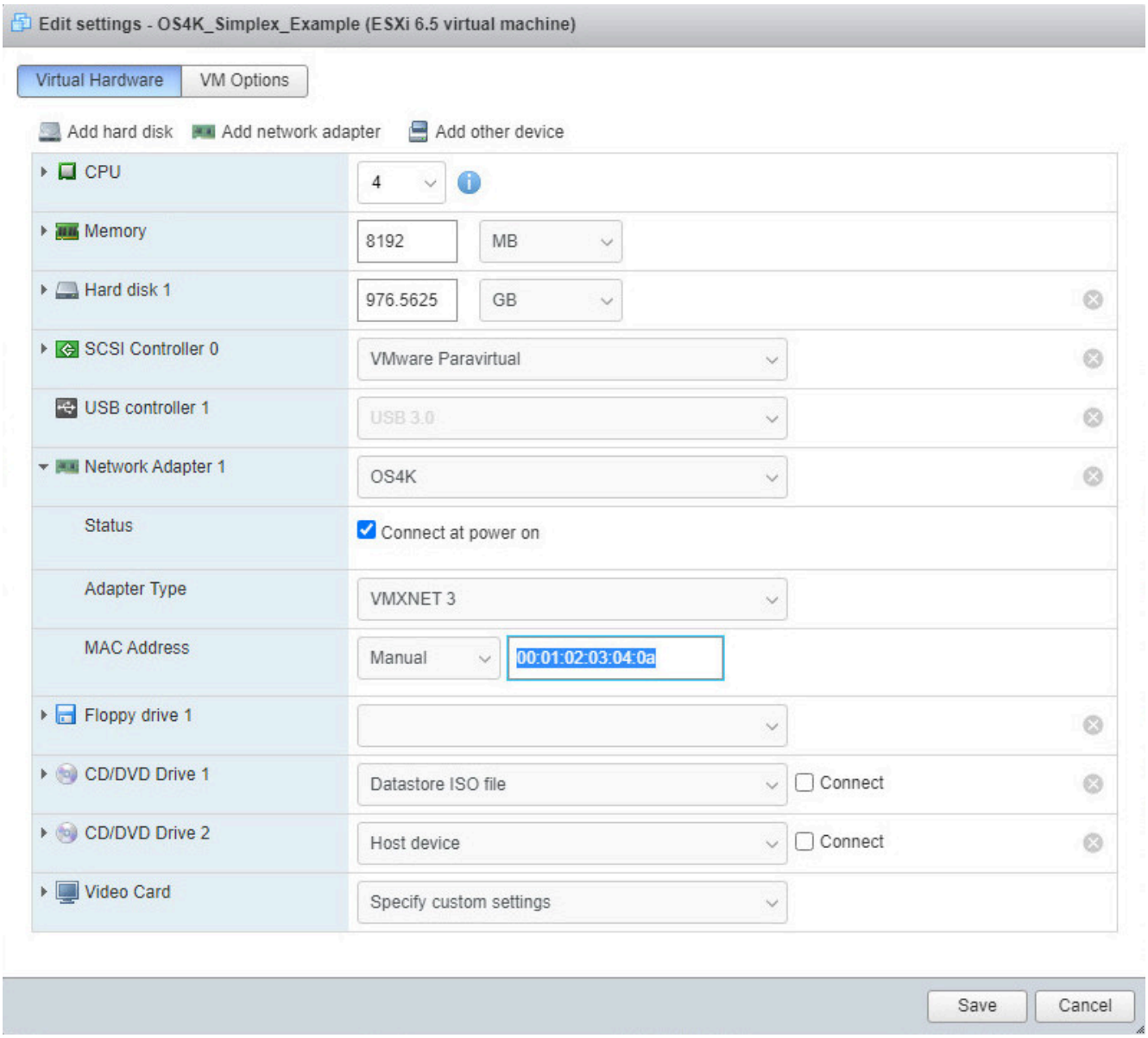


Figure 68: Manually assigning the MAC address of the virtual machine

Now enter the MAC address in the `firstinst-netw-*.xml` file.

3.10.2 DNS Server

A valid and accessible DNS server has to be configured.

The DNS server is required so that the CLA daemon can operate properly. You need the DNS server in order to supply a valid license for the system.

Undesired states would also arise as a result of timeouts from polling an invalid/ inaccessible DNS IP address.

Enter a valid DNS server at the relevant position in the `firstins-netw-*.xml` file.

```
<entry key="customer-dns.server.0">valid DNS IP</entry>
```

3.11 Generating a Floppy Image with the Content of firstinst-netw-*.xml

The OpenScape 4000 should be configured as part of the first installation process even when the installation is performed by means of an ISO file.

The file: `firstinst-netw-*.xml` is used as usual for this purpose.

Because the ISO file (unlike the previously used USB stick) cannot be written, a floppy image file is used as an additional medium.

NOTICE: Alternatively, if ISO editing software is available (e.g. AnyBurn, UltraISO, etc.), all required installation files (XML, Regen, Hotfixes) can be directly added to the ISO before installation. In this case, the custom OS4K ISO can be used as installation media and the steps described in the chapters 3.11 and 3.12 can be skipped. In this case, no installation logs will be available since the ISO is read-only.

A blank floppy image file (`empty.flp`) is included with the delivery.

Tools are required in order to be able to create the `/config` path on this floppy image and to store the `firstinst-netw-*.xml` file below this.

The M-Tools are used in the example below, which are likewise made available with the ISO installation file.

The `prepare.bat` script is used to create the floppy image `install.flp` with the content of `firstinst-netw-*.xml` in the installation directory.

IMPORTANT: The `install.flp` is required for every node in case of a separated duplex installation, in other words three times (for Node 1, Node 2 and the Quorum). You can copy the `install.flp` file for this purpose. The new name should still end in `.flp` and can otherwise be chosen freely (e.g. `bpa.flp`, `bpb.flp`, `q.flp`).

IMPORTANT: If the same floppy image file is being used, not all log files can be recorded because only one installation has write access and can write log files.

3.12 Preparing the Hotfix Installation

Hotfixes can still be activated during the first installation. For this purpose, a separate ISO file containing only the hotfixes must be created.

NOTICE: If a suitable tool is not available, the tool provided with the ISO installation file can be used, as described in this example.

NOTICE: Alternatively, if ISO editing software is available (e.g. AnyBurn, UltraISO, etc.), all required installation files (XML, Regen, Hotfixes) can be directly added to the ISO before installation. In this case, the custom OS4K ISO can be used as installation media and the steps described in the chapters 3.11 and 3.12 can be skipped. In this case, no installation logs will be available since the ISO is read-only.

Copy the required installation files to the working path of the Service PC.

Then run the `mk-iso.bat` script to create the ISO file with the hotfixes: `hotfixes.iso`.

3.13 OpenScape 4000 Installation in the Virtual Machine

3.13.1 Preparations

Connect installimage.iso and floppy image to the ESXi host

1) Start the virtual machine.

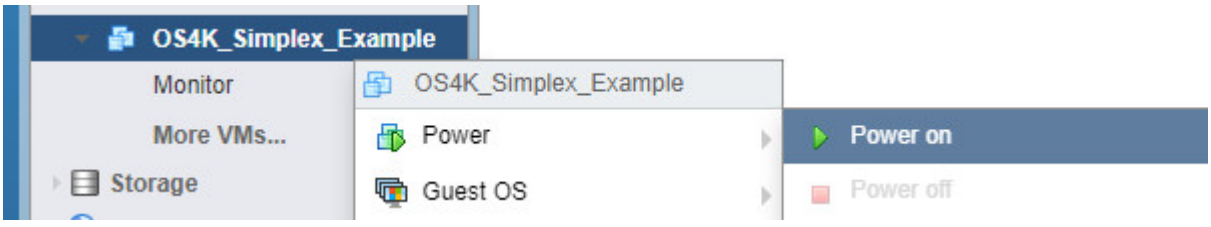


Figure 69: Starting the virtual machine

2) Open the console

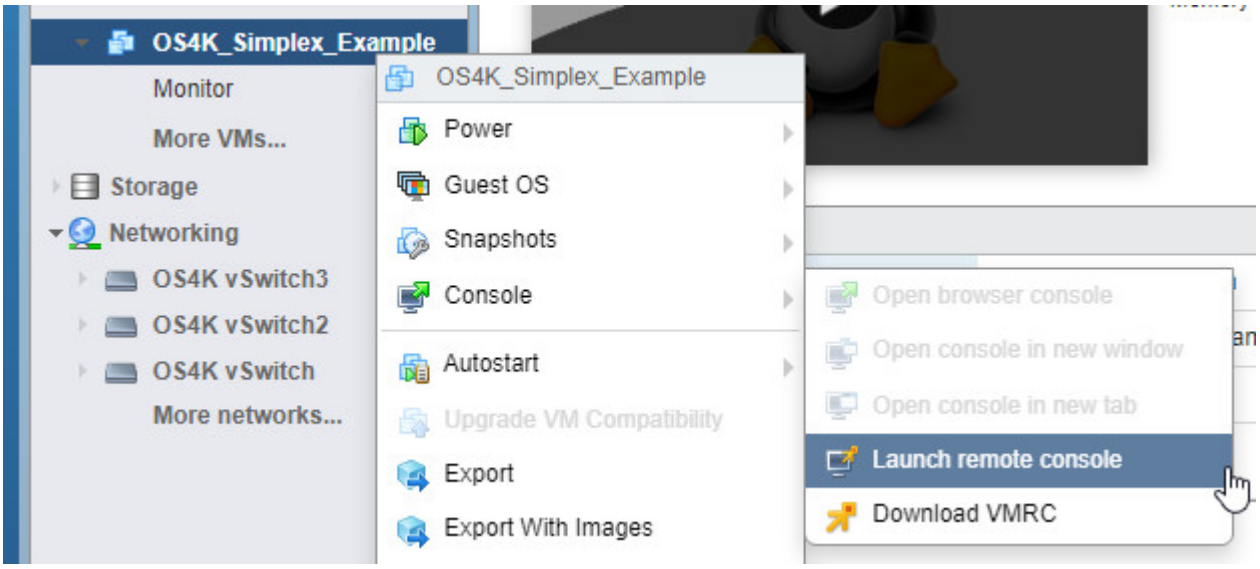


Figure 70: Opening the console

3) Connect `installimage.iso` to the ESXi host.

Select `installimage.iso` in the console via the DVD.

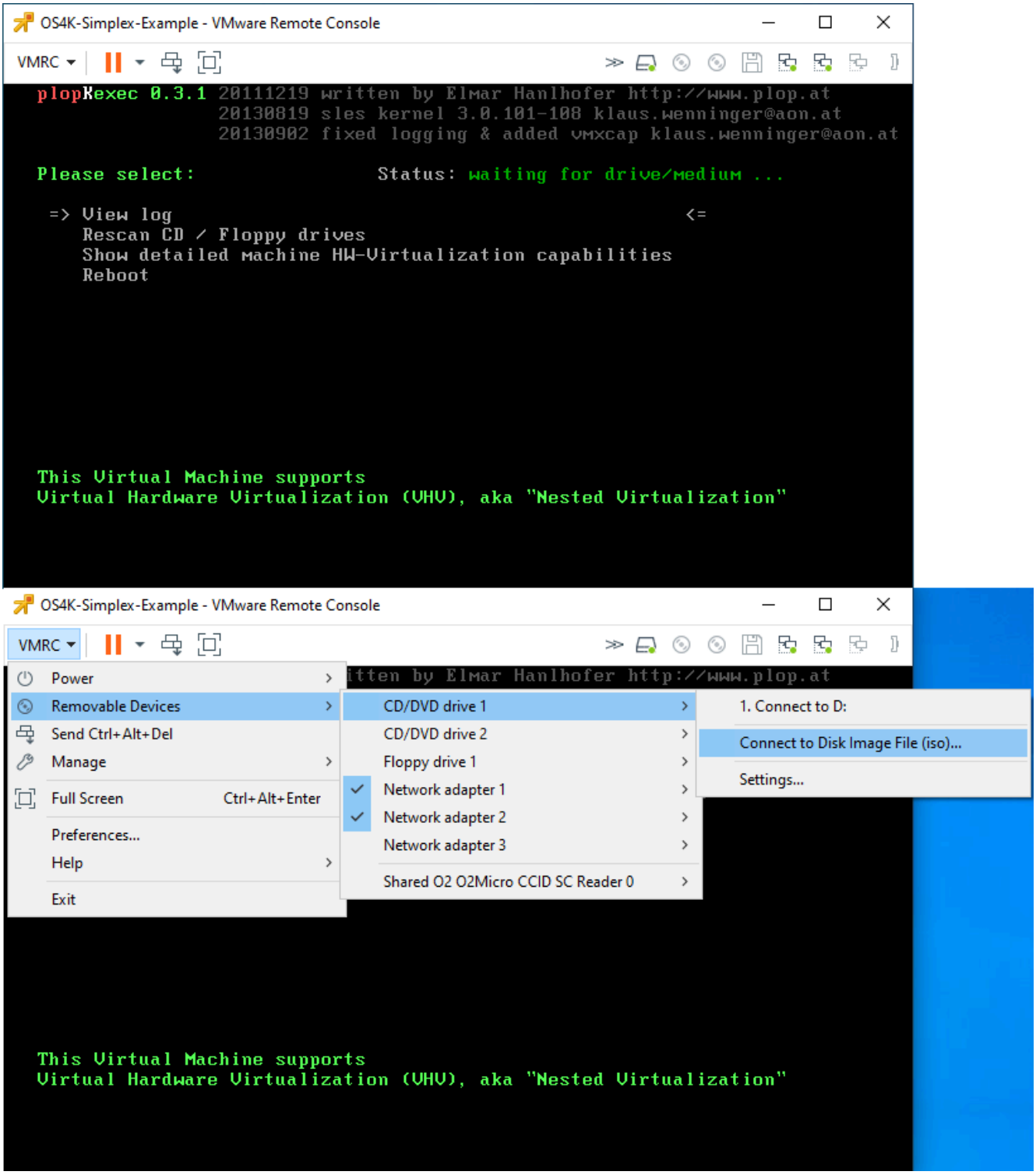


Figure 71: Connecting the ISO image on the datastore to the ESXi host

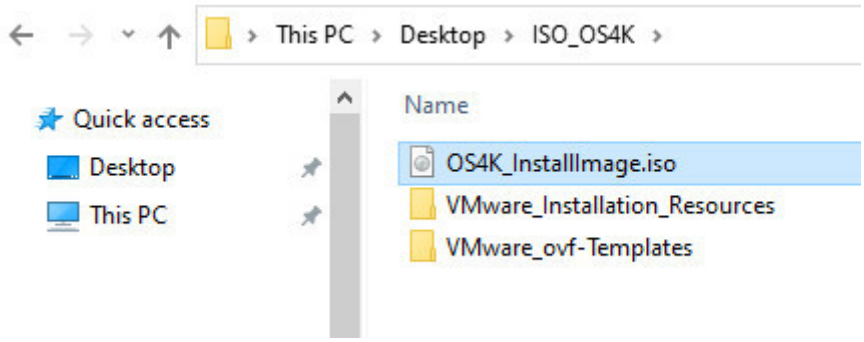


Figure 72: Selecting the ISO image

Wait until the message `=> sr0: OpenScape 4000 <version num>...` is displayed.

Figure 73: ISO image on datastore is connected to ESXi host

4) Connect the floppy image to the ESXi host.

NOTICE: You can skip this step if a custom ISO file is used that already has the needed XML and optional REGEN files.

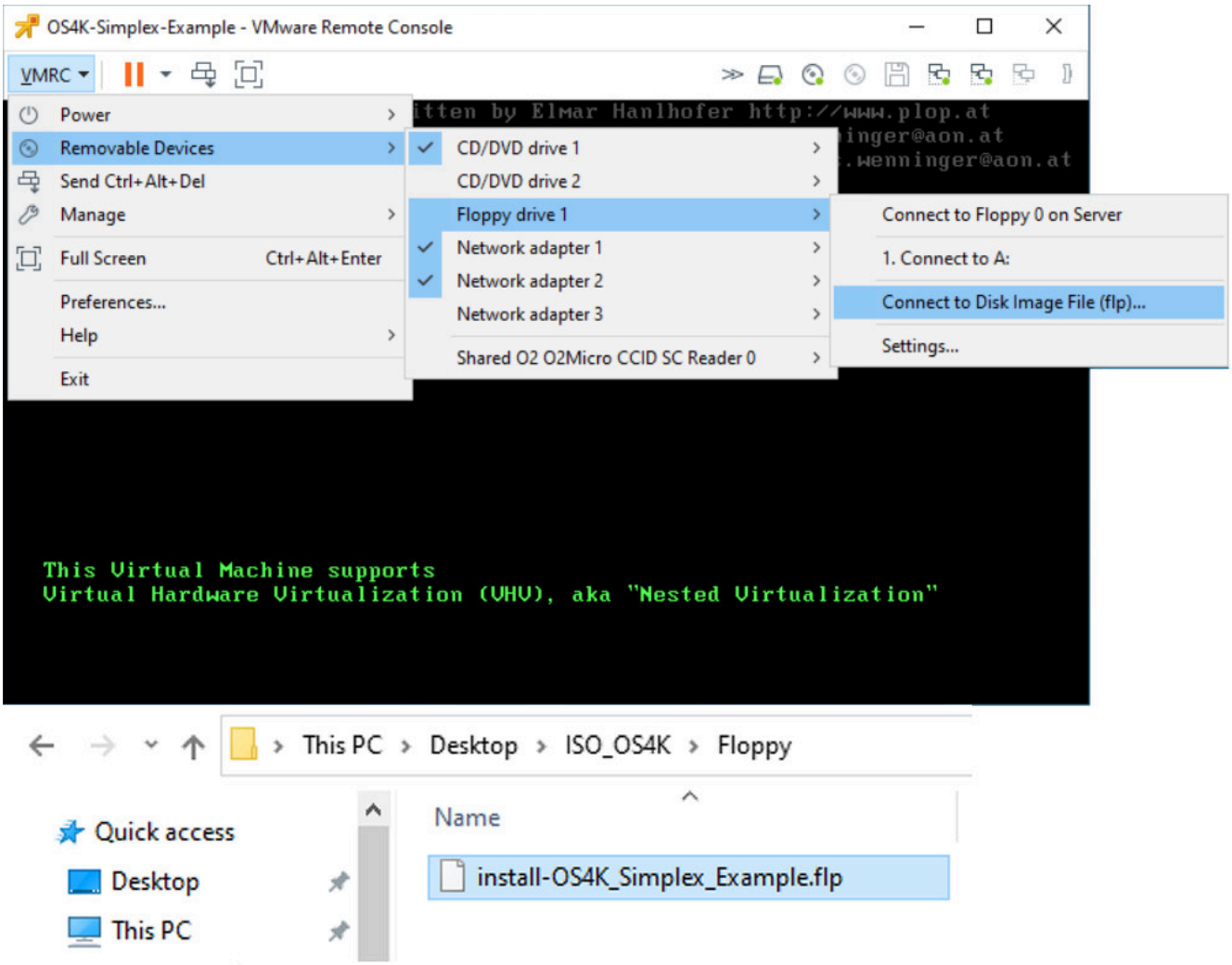


Figure 74: Connecting the floppy image to the ESXi host

Wait until the message `fd0: /config` is displayed.

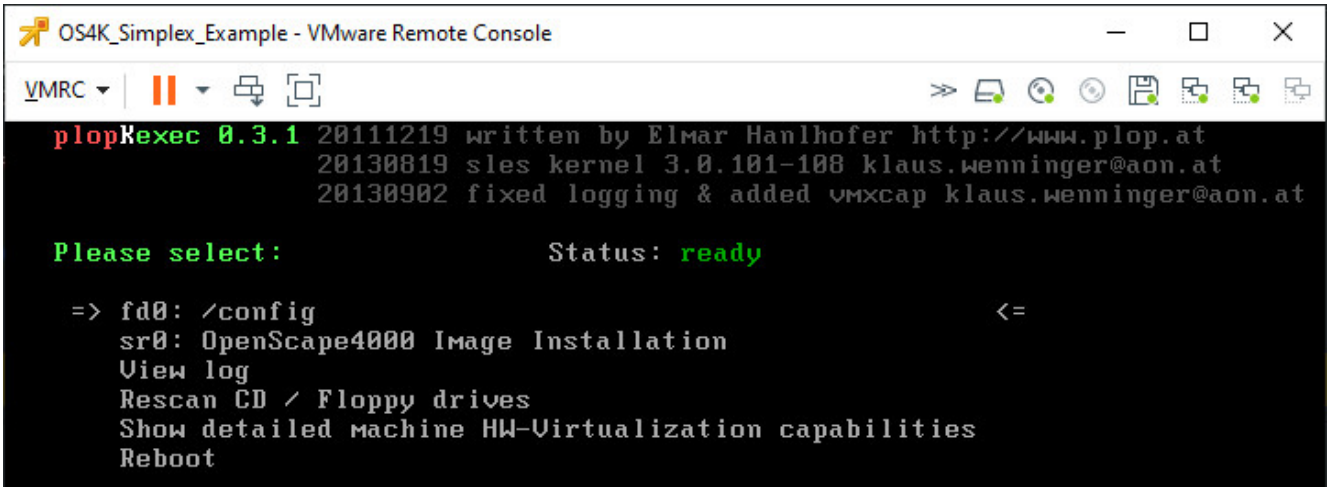


Figure 75: Floppy image is connected to the ESXi host

5) Connect `hotfix.iso` to the ESXi host.

NOTICE: You can skip this step if no hotfix is installed or if a custom ISO file is used that already has the needed hotfixes.

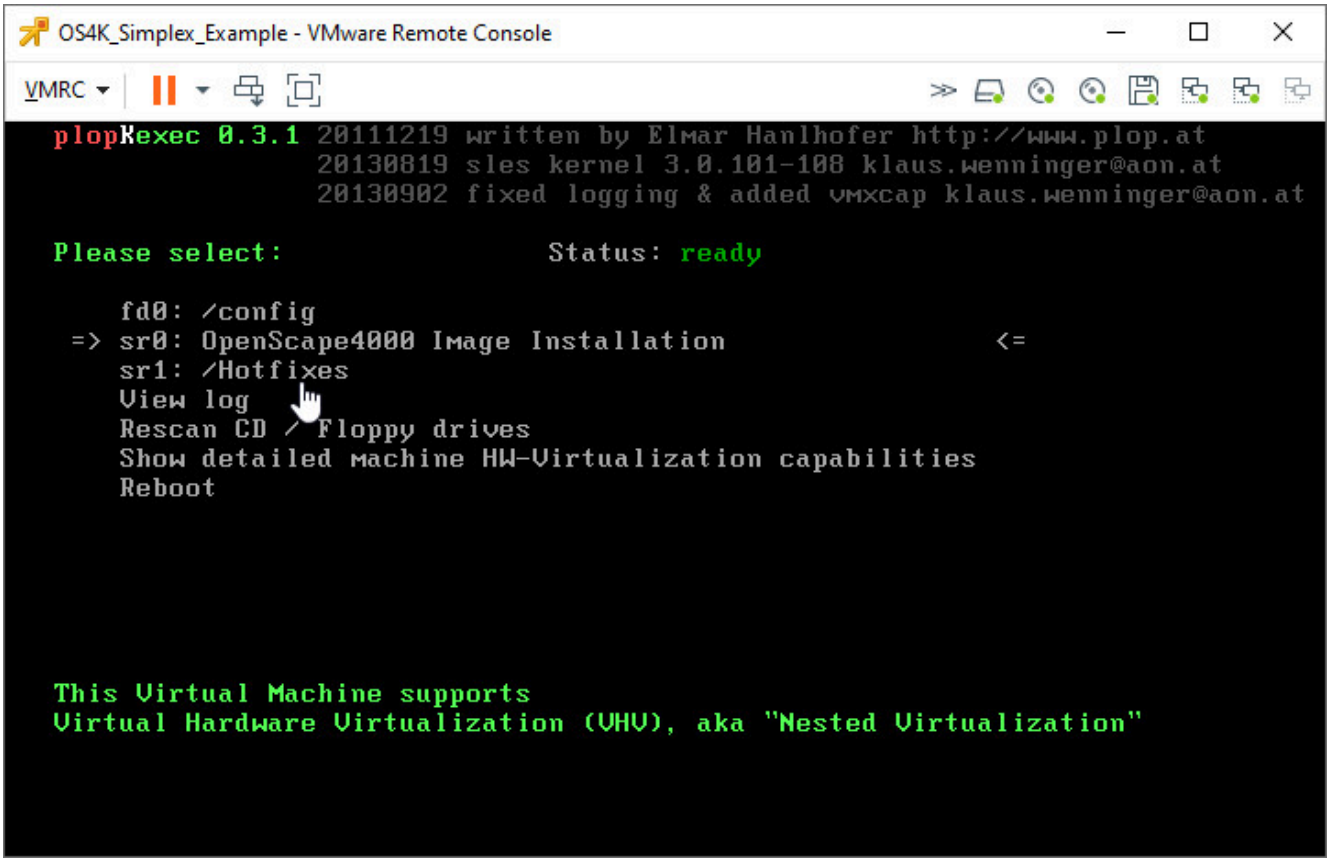


Figure 76: Connecting hotfix.iso to the ESXi host

Use the cursor keys to select **sr0: OpenScape 4000** <software version> **Image Installation** and press the Return key.

3.13.2 Starting the Installation

1) Click in the console window to start the installation and confirm with Return.
2) Accept the EULA with **Accept and install**.

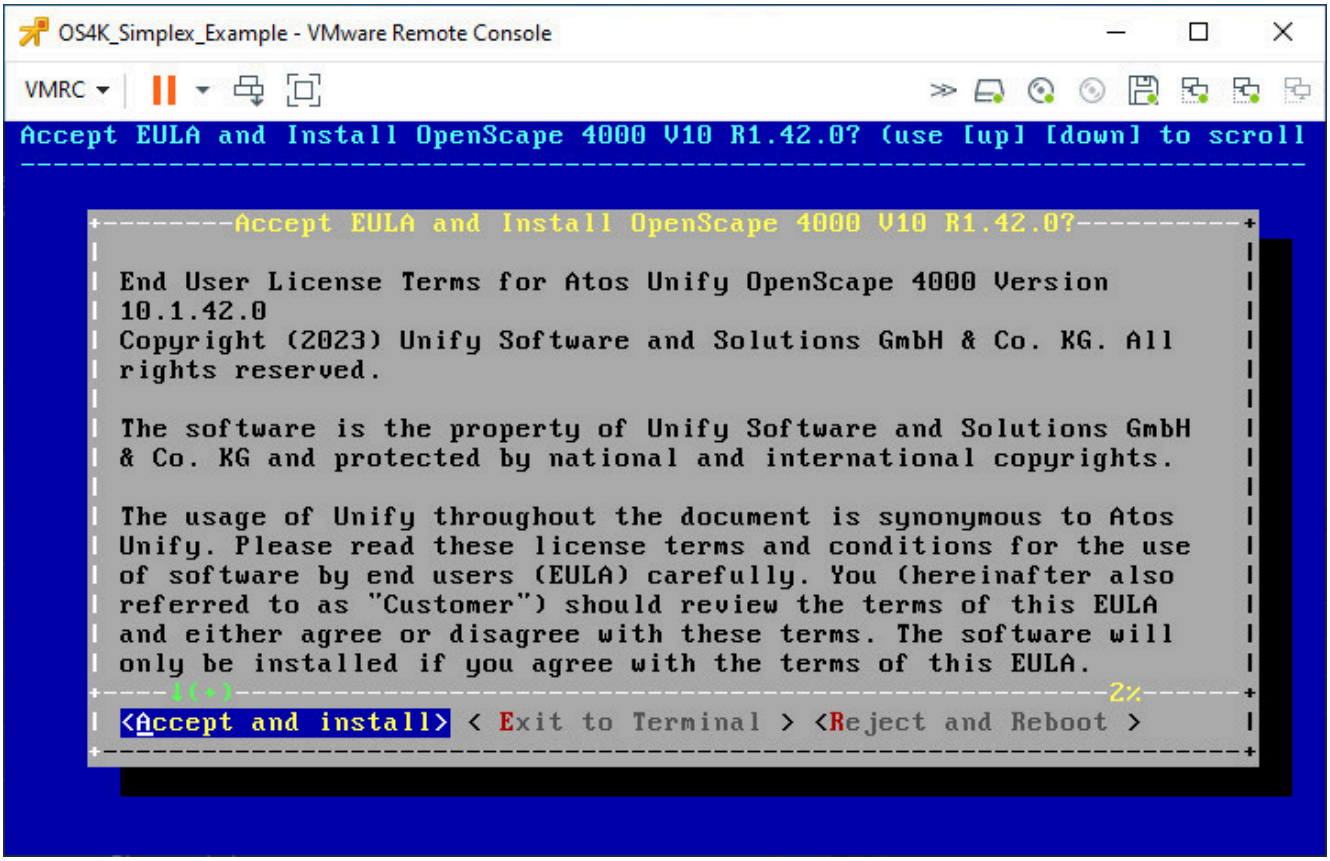


Figure 77: Accepting the EULA

The installation is performed.

3) The installation should have been successfully performed after 25 minutes.
4) Now unmount the ISO and floppy image and confirm with OK. The system is restarted.

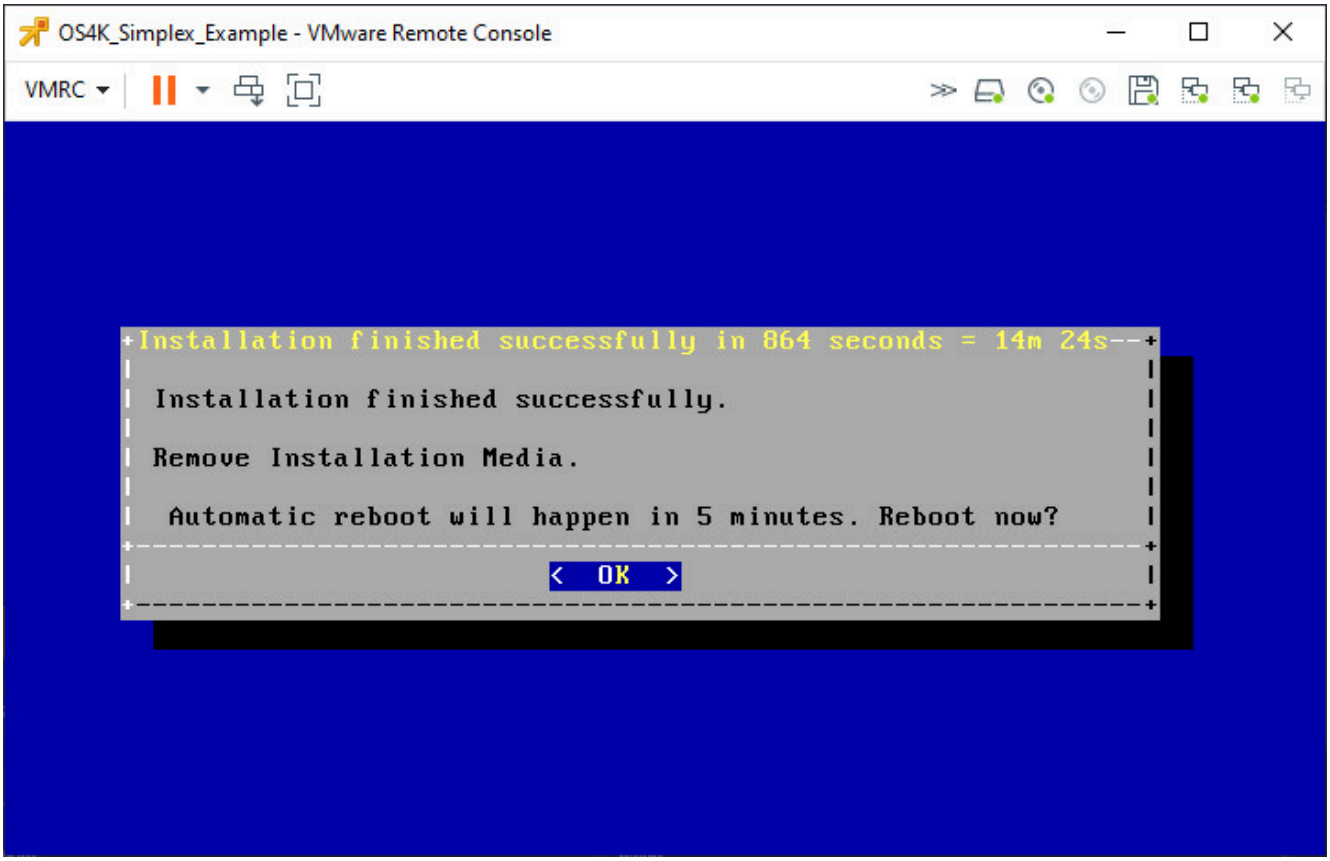


Figure 78: Installation successful

3.14 Changes following Installation

3.14.1 Assigning the LAN Interfaces to the Network Interfaces

1) Query the assignment of the networks to the eth interfaces with the assistance of the XML file.

```
<common>
<entry key="system-deployment">simplex</entry>
<entry key="customer-portal.ip">192.168.220.177/24</entry>
<entry key="customer-lan.assistant-ip-address">192.168.220.175/
<entry key="customer-lan.csta-ip-address">192.168.220.176/24</e
<entry key="atlantic-interface.0">eth1</entry>
<entry key="ipda-interface">eth0</entry>
<entry key="ipda-lan.cca-ip-address">192.168.220.178/24</entry>
<entry key="ipda-lan.default-router-ipda">192.168.220.1</entry>
<entry key="internal-lan.network">192.168.187.0</entry>
<entry key="customer-def.gw">192.168.220.1</entry>
<entry key="integrated-softgate">1</entry>
</common>
<node1>
<entry key="system-root.password">$2y$10$e6tcBA.T4yUJcqP65AqVDe
<entry key="mac-address">00:50:56:98:5b:30</entry>
<entry key="customer-interface">eth0</entry>
<entry key="eth0.ip.0">192.168.220.174/24</entry>
<entry key="eth0.hostname.0">h4k-13</entry>
<entry key="eth0.domainname.0">h4k.sielan.de</entry>
<entry key="eth1.ip.0">0.0.0.0/0</entry>
<entry key="customer-ntp.server.0">192.168.11.33</entry>
<entry key="customer-timezone">Europe/Berlin</entry>
<entry key="customer-keyboard-layout">german</entry>
<entry key="customer-def.gw.dev">eth0</entry>
</node1>
```

Figure 79: Assigning the networks to the eth Interfaces

2) Use the eth interfaces to establish the MAC address of the interface cards with the assistance of the console command `ifconfig | grep eth`.

```
OS4K_Sim:~ # ifconfig | grep eth
  eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:50:56:90:64:76  txqueuelen 1000  (Ethernet)
  eth0:0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:50:56:90:64:76  txqueuelen 1000  (Ethernet)
  eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:50:56:90:94:c0  txqueuelen 1000  (Ethernet)
  eth2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:90:7e:87  txqueuelen 1000  (Ethernet)
  vethdef0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 52:54:00:cc:af:fe  txqueuelen 1000  (Ethernet)
  vethdef1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 52:54:00:dd:af:fe  txqueuelen 1000  (Ethernet)
OS4K_Sim:~ #
```

Figure 80: Querying the MAC addresses of the eth interfaces

3) You can then use these MAC addresses to establish the LAN assignment in the virtual machine.

   Open the **Edit Settings** view, select a specific **Network Adapter** from the list and click the down arrow next to it to expand the section. Choose the network assigned to the MAC address.

   Enable the **Connected** and **Connected at power on** options, by activating the corresponding check boxes in the **Device Status** area.

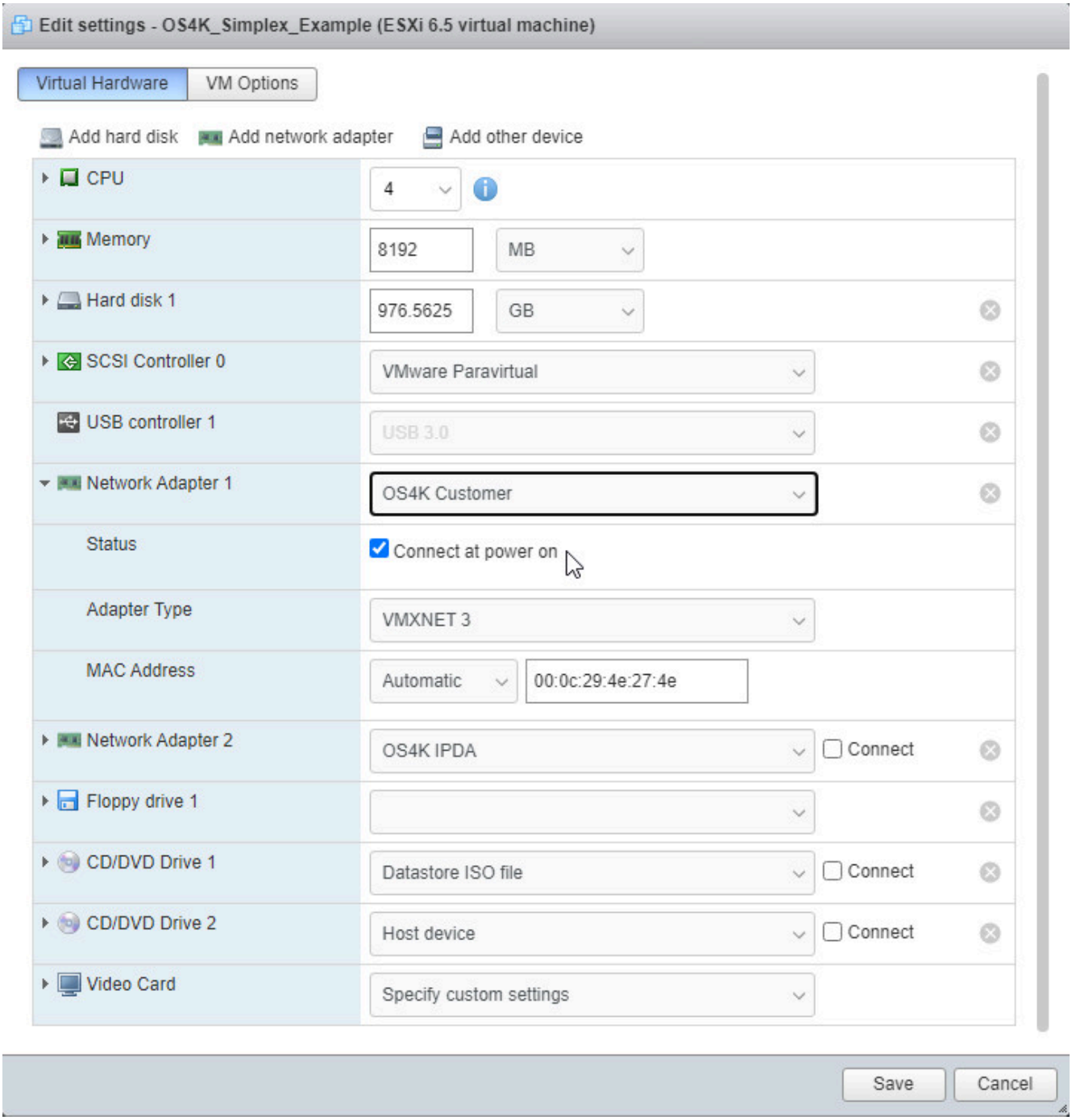


Figure 81: LAN assignment in the virtual machine

IMPORTANT: Delete unused interfaces.

3.14.2 Switching the DVD Drive to "Local Client"

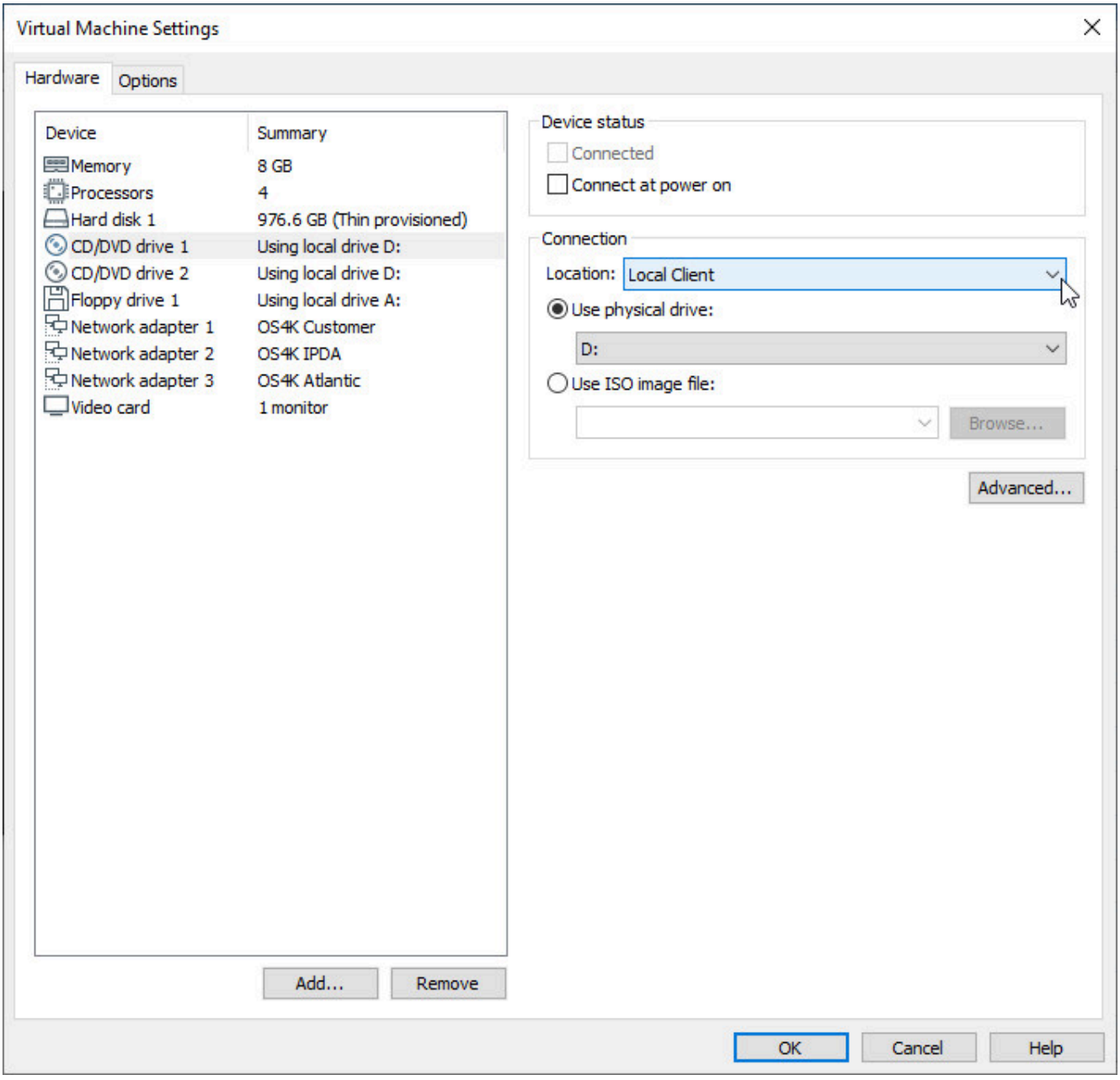


Figure 82: Switching the DVD drive to "Local Client"

Change the device type for the DVD to **Client Device** in the **Device Type** section.

In **Virtual Machine Remote Console**, click the **VMRC** drop-down and select **Manage** > **Virtual Machine Settings...**. Alternatively, you can use the following key combination: `Ctrl+D`.

Next, select a CD/DVD drive from the list, then change the **Location** to **Local Client**. Finally, enable the **Use physical drive** option and click **OK** to apply the settings and exit.

IMPORTANT: This setting is important because the virtual machine should no longer boot from the ISO image following installation.

3.14.3 Checking the installation status of OpenScape 4000

The installation status of OpenScape 4000 can be queried via the **OpenScape 4000 Platform Administration (Portal)**.

There are two options for viewing the installation status:

Status > **Assistant Installation Status**

or

Status > **Installation Status**

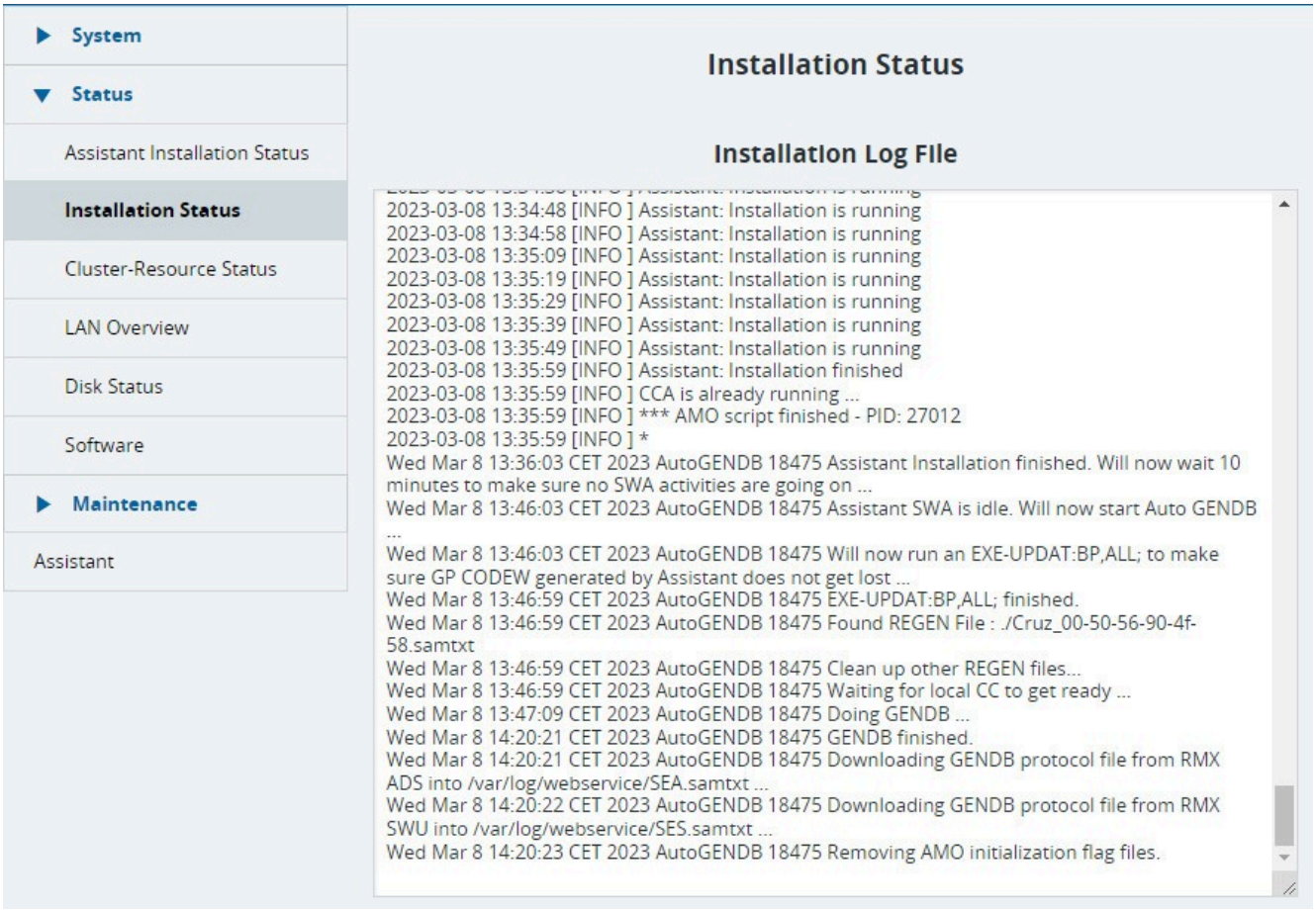


Figure 83: Installation status of OpenScape 4000

3.14.4 Configuring the Customer Data

Execute the RMX and OpenScape 4000 Assistant configuration as before.

NOTICE: If a valid RMX REGEN file is found during the installation, the configuration will be applied automatically.

3.14.5 Checking the System Status

NOTICE: This option is available only on Host deployments.

Open the **OpenScape 4000 Platform Administration (Portal)** and check the 7-segment display to determine whether the status "A" was reached.

System > Frontpanel

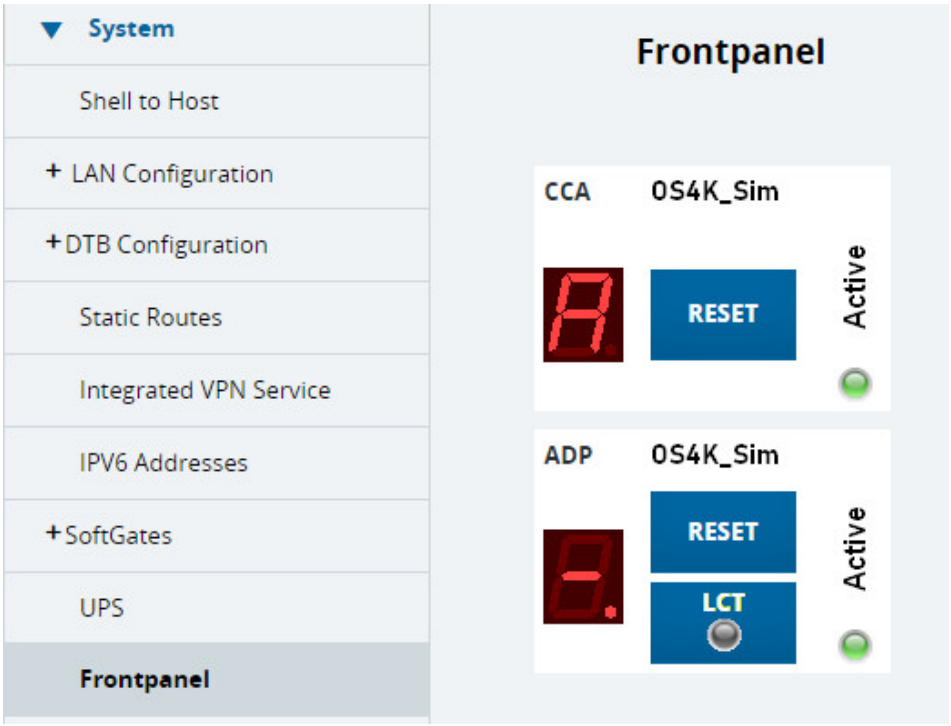


Figure 84: Checking the system status

3.15 Staging Center Availability for End Customers

3.15.1 Exporting the Virtual Machine to an OVF File

1) Shut down the virtual machine.

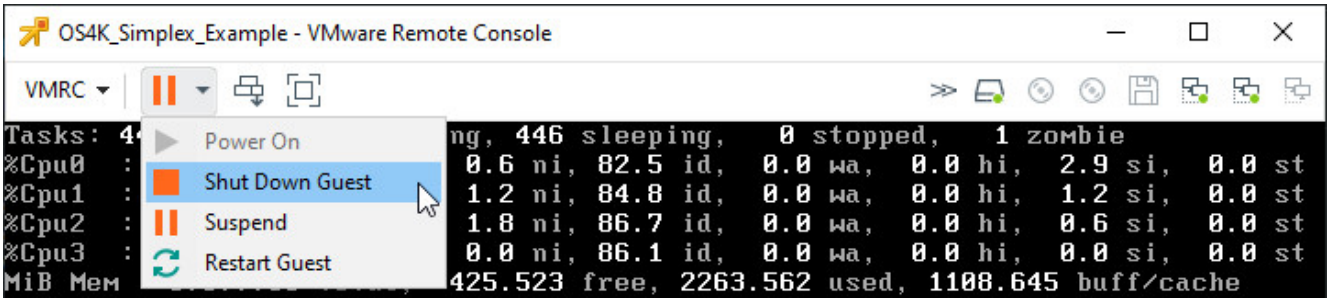


Figure 85: Shutting down the virtual machine

2) Select the virtual machine.
3) Export the OVF template.

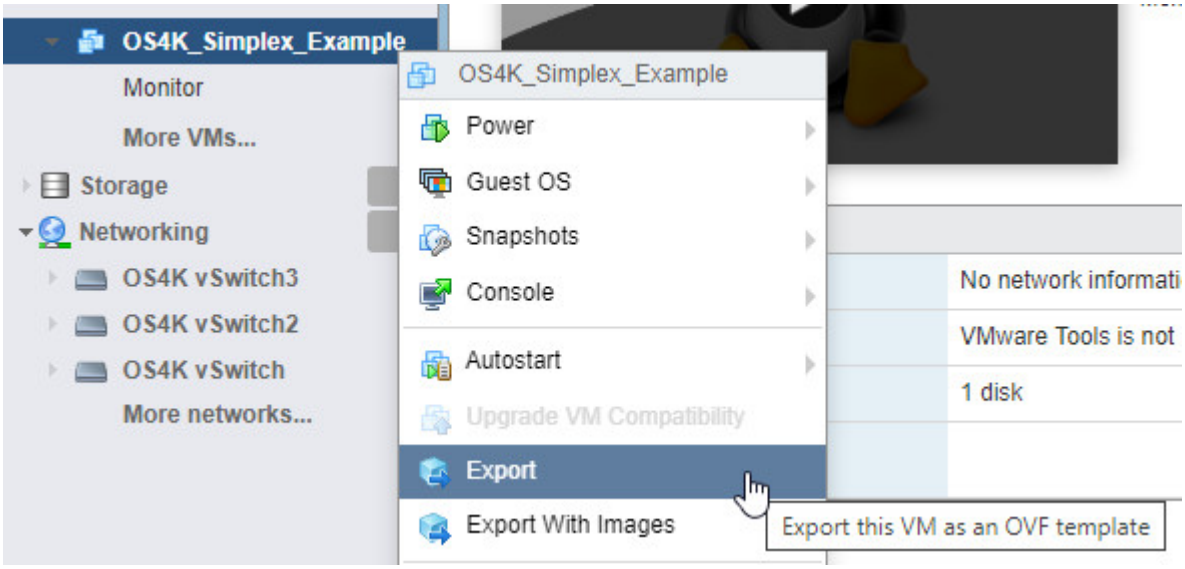


Figure 86: Exporting the OVF template

4) Click **Export** and choose a download location for the selected files.

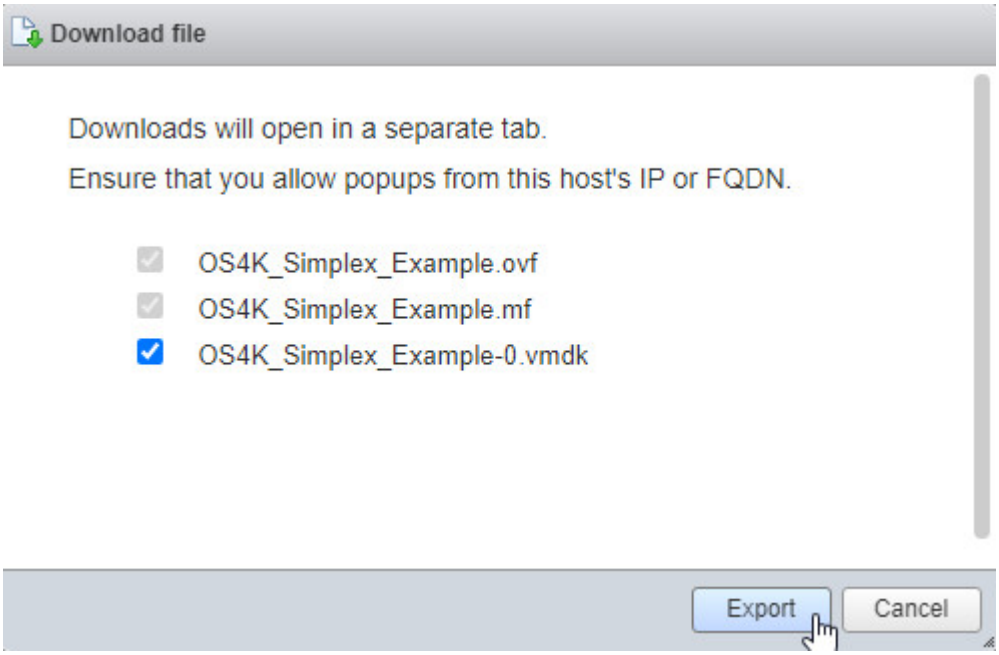


Figure 87: Choosing the storage location for the exported OVF template

3.15.2 End Customer Installation

Installation with vSphere Web Client

Deploy the OVF template from the USB hard disk.

The machine can be started directly following the import (Deploy OVF).

3.16 Notes and Possible Error Sources

3.16.1 Log Files during Installation

Error causes during the installation can often be analyzed using the log file written to the floppy.

The `getlogs.bat` script, which is part of the ISO installation file, is used to copy the log files from the floppy to the PC.

NOTICE: If a custom OS4K ISO was used with required installation files (XML, Regen, Hotfixes), no installation logs will be available since the ISO is read-only.

3.16.2 Installation and Configuration Steps

With Remote Major Update process a central host system running HiPath 4000 V7R2 can be updated to OpenScape 4000 V10 from remote.

This process involves using a second system of the same hardware type as the remote system for preparing and creating a Recovery ISO Image containing the OpenScape 4000 V10 R1 Software plus complete system configuration.

This ISO Image will be then transferred to the remote host system and used for the remote major update process.

NOTICE: Starting with V10R1, Remote Major Update (RMU) is no longer supported.

3.17 Re-Installing the OpenScape 4000 Software

Requirement:

The virtual machine has booted and is running with the old software.

Re-installation steps

1) Open the console

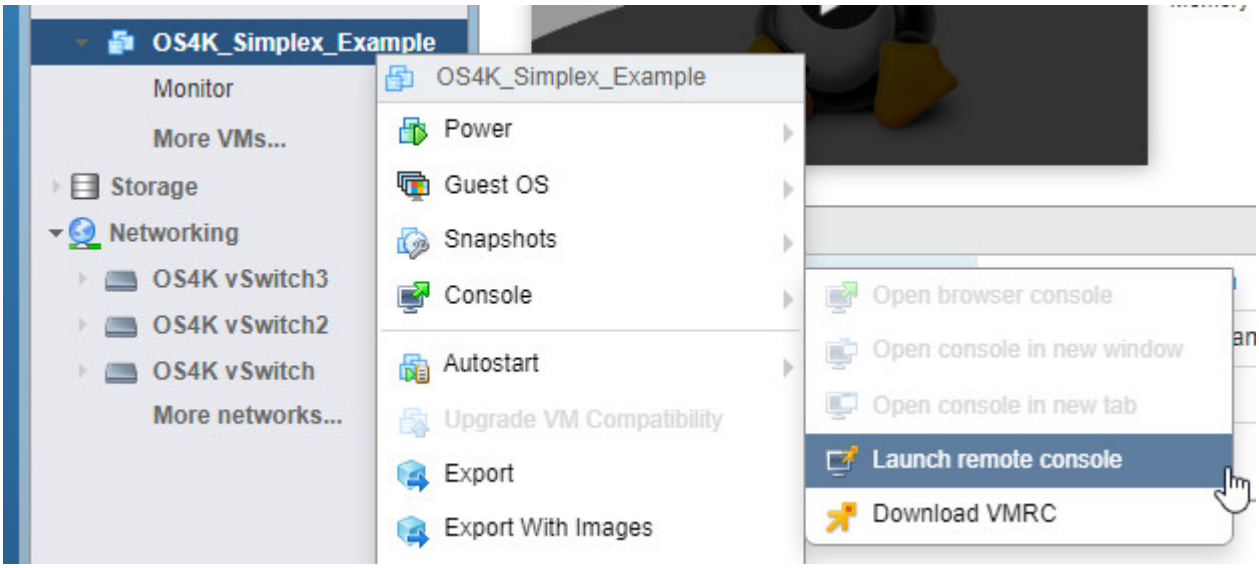


Figure 88: Opening the console

2) Connect `installimage.iso` to the ESXi host.

Select `installimage.iso` in the console via the DVD.

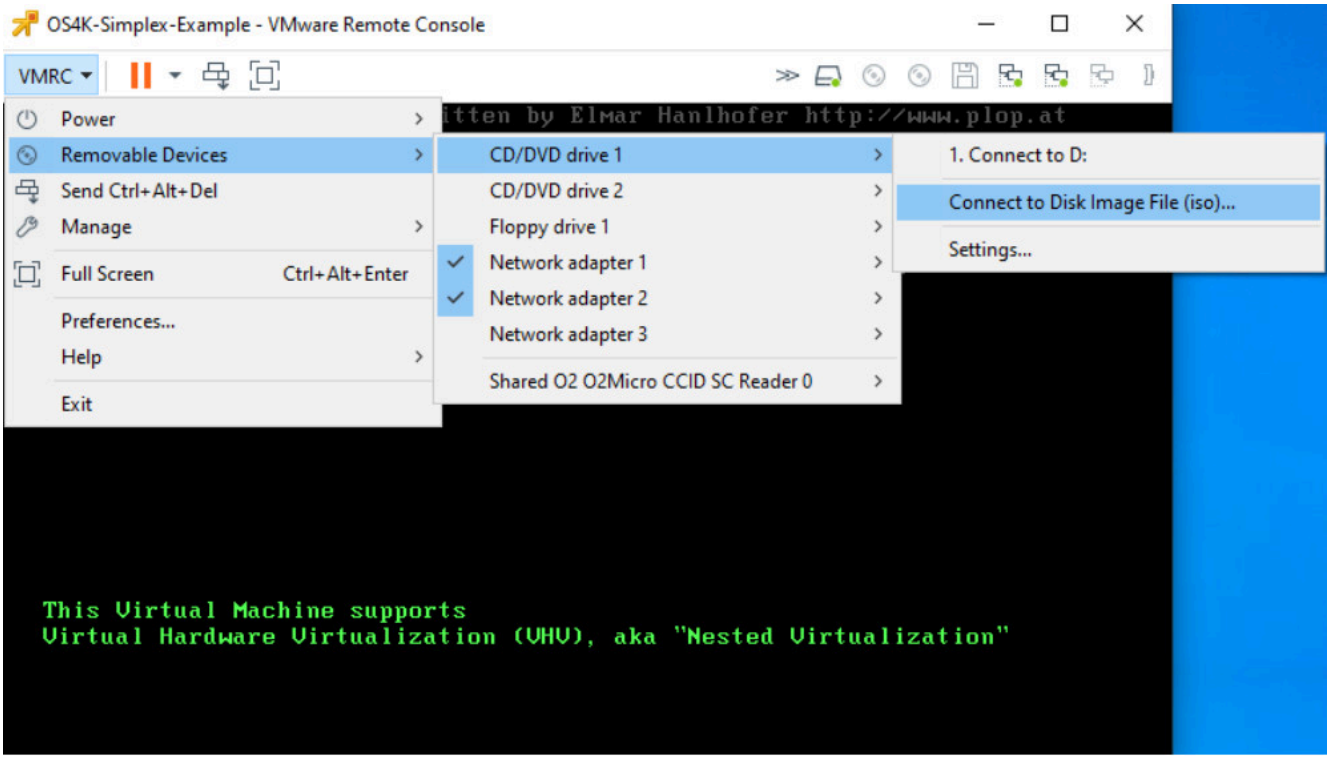


Figure 89: Connecting the ISO image

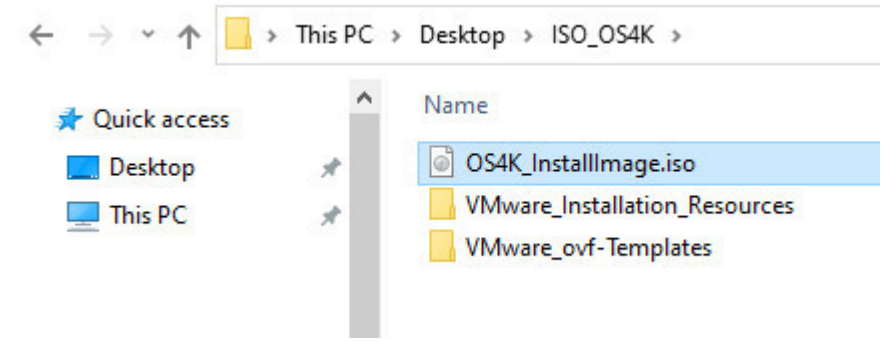


Figure 90: Selecting the ISO image

3) Connect the floppy image to the ESXi host.

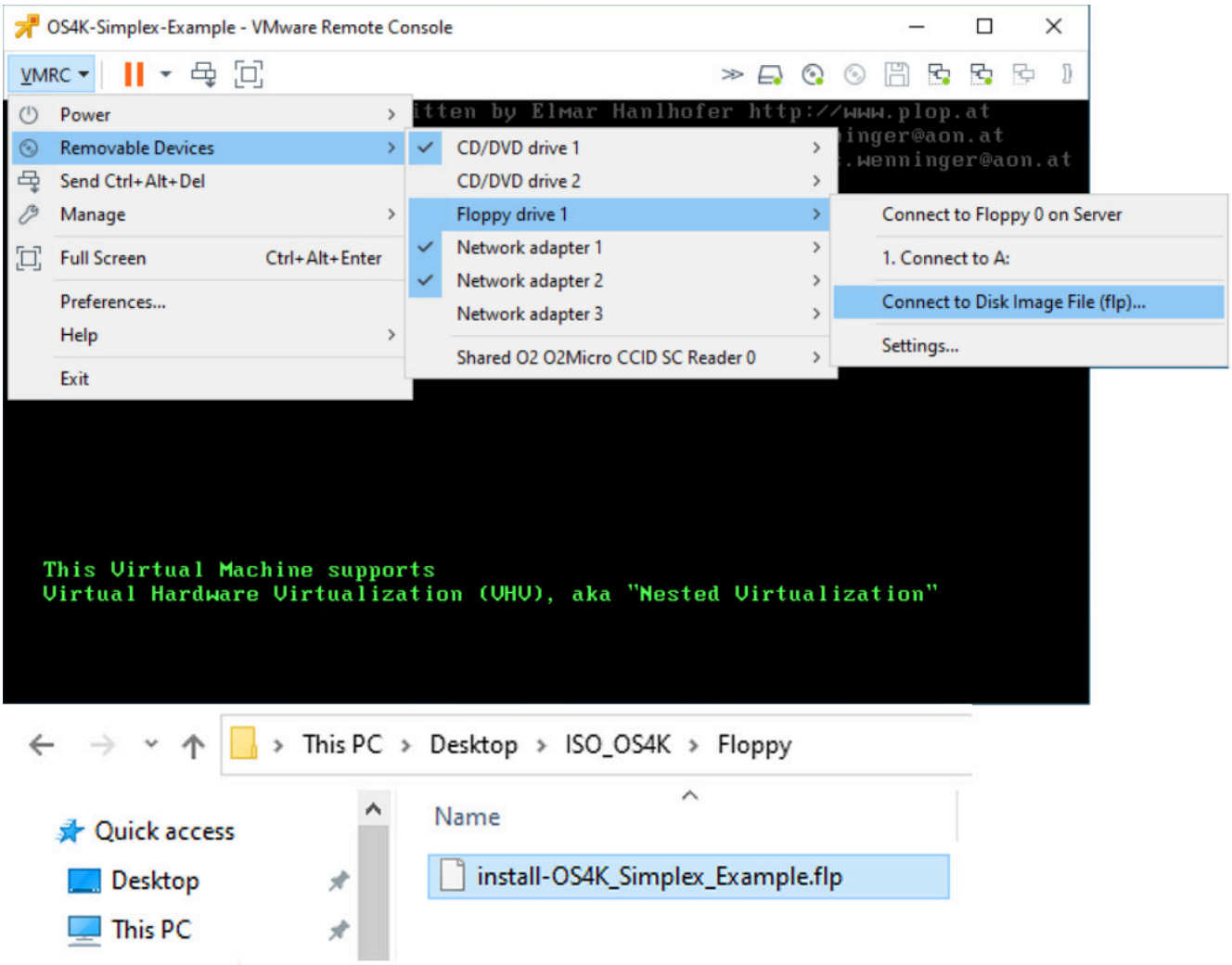


Figure 91: Connecting the floppy

IMPORTANT: You have to mount a new floppy image (install.flp) for the re-installation, which has not already been used for a previous installation.

4) Log in to the active virtual machine and enter the command `#reboot`.

NOTICE: Starting with V10 R1, the **reboot** command has been replaced with **os4k-reboot**.

5) Reboot the active virtual machine and boot from the mounted ISO.

4 Migration and Reinstallation of legacy systems

4.1 Preparation

Migration is intended to help the user to update from HiPath 4000 V6 and V7 to OpenScape 4000 V10 easily and to reduce the effort of building a system from scratch in just a few easy steps and in the quickest time possible.

Before starting the migration process there are a few tools that you need:

- USB Stick
- Putty or any other SSH client
- ComWin

Optional items are:

- WinSCP can be used to transfer the files between your local computer and the system.
- Hard disk for Recovery

NOTICE: It is recommended to make a recovery hard disk of the HiPath 4000 V6 system for fallback before you start the migration.

NOTICE: After an upgrade to the latest software version, the OpenScape 4000 Assistant browser client preparation has to be carried out a new on all client PCs. Starting with V10R1, Client Preparation requires openwebstart. For more details, see the Assistant Public Page -> Client Preparation.

Version/HW	HiPath4000 >= V6 R2.x	OS4000 >= V7 R2.x	OS4000 >= V8 R2.22	OS4000 V10 R0	OS4000 V10 R1
VMware	✓ [1]	✓	✓	✓	✓
EcoServer	x	✓	✓	✓	✓
Branch	x	x	✓	✓	✓
OS EcoServer	x	x	✓ [2]	✓	✓
OS EcoBranch	x	x	✓ [2]	✓	✓
DSCXL2	✓	✓	✓	✓ [3]	x
DSCXL2+	✓	✓	✓	✓ [3]	x
OSA500	✓	✓	✓	✓	✓ [4]

Figure 92: Migration to OpenScape 4000 V10 R1 - HW information

= possible

x = not possible

NOTICE:

1) Only Standalone SoftGate deployment is allowed.
2) Support from PLT HF V8R2.22.6.
3) Only APE deployment is allowed.
4) Only OSA500 with 8GB RAM is compatible.

4.2 Before Migration of the HiPath 4000 V6 Host System

RMX Regen and a logical backup of the OpenScape 4000 Assistant must be taken and saved offline somewhere.

4.2.1 Backup RMX Database

Execute a REGEN to save the RMX database of the system you want to migrate. Convert the RMX Regen with PC DACON to the desired version (e.g. OpenScape 4000 V10 R1). Save the new RMX database offline.

4.2.2 Make the Logical Backup

Step 1: The logical backup of the OpenScape 4000 Assistant is the one that is best suited for the migration and will ensure a full functionality after the restore is done in this situation.

NOTICE: During the backup of HG3550M (CGW/NCUI Configuration Backup) the gateways must be still connected to the old system.

Prerequisites:

1) In order to backup correctly the HG3550M the gateways must not be switched into the SECURITY mode. You can achieve this either by switching them all to MAINTAIN mode in Gateway dashboard or globally by disabling the feature **Enable Gateway Secure Mode** in Security Mode configuration.
2) All the gateways' loadware must be upgraded to the new version before backup.
3) Please make sure all checkboxes are enabled in Configuration of HG3550M.

Backup & Restore > Administration > Configuration

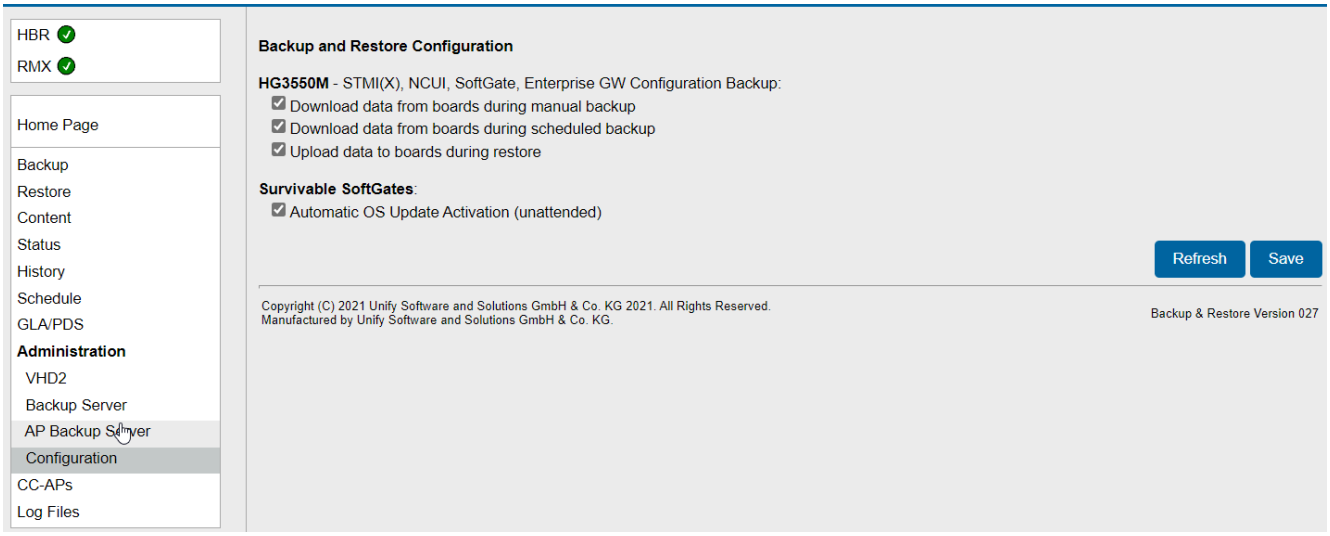


Figure 93: Configuration of HG 3550M

Perform the following steps for the logical backup:

1) Access the OpenScape 4000 Assistant web interface.
2) Navigate to **Software Management > Backup & Restore > Backup**.
3) Select **Buffer** as **Archive** medium. If you have a server or you think it's better in your case to use a hard disk you can use those options, but it is recommended to use the **Buffer** as backup medium.
4) Select **Logical (export)** as backup **Type**.
5) Check all the boxes under **Unix Configuration Data** except **RMX ((RMX Regenerate database)** and **BEER Platform Configuration data)**.
6) After selecting the above options press **Start Backup**.

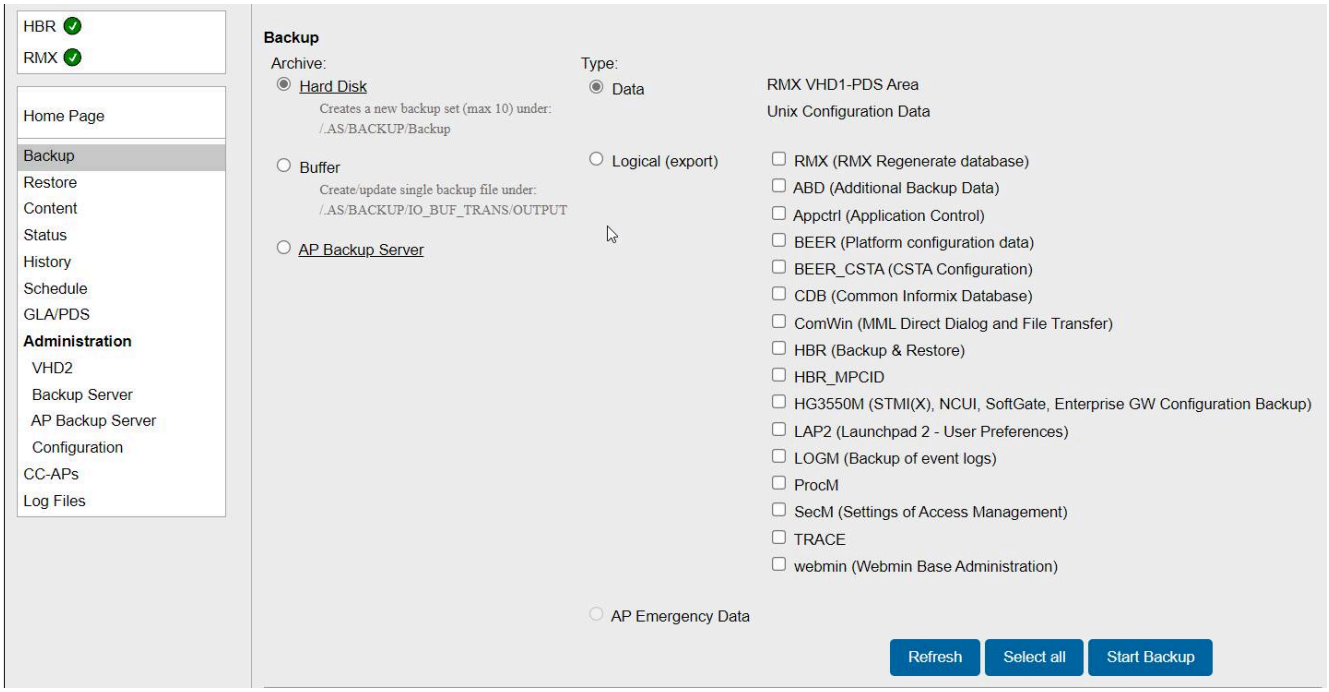


Figure 94: Logical backup with OpenScape 4000 Assistant

Step 2: A message from the webpage will appear announcing the fact that the backup will interfere and you won't be able to use some functionalities until it is finished. Confirm this message box and the next one that will appear. The second one will announce the start of the backup. Press the **OK** button for both.

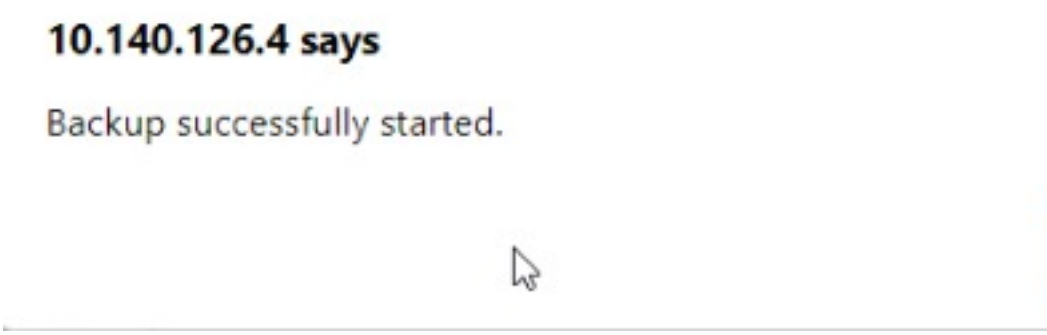


Figure 95: Start of the logical backup

Step 3: After pressing **OK** the page will be redirected to **Status** where you can see the units that will be backed up, their status (Successful, Running or Waiting) and more.

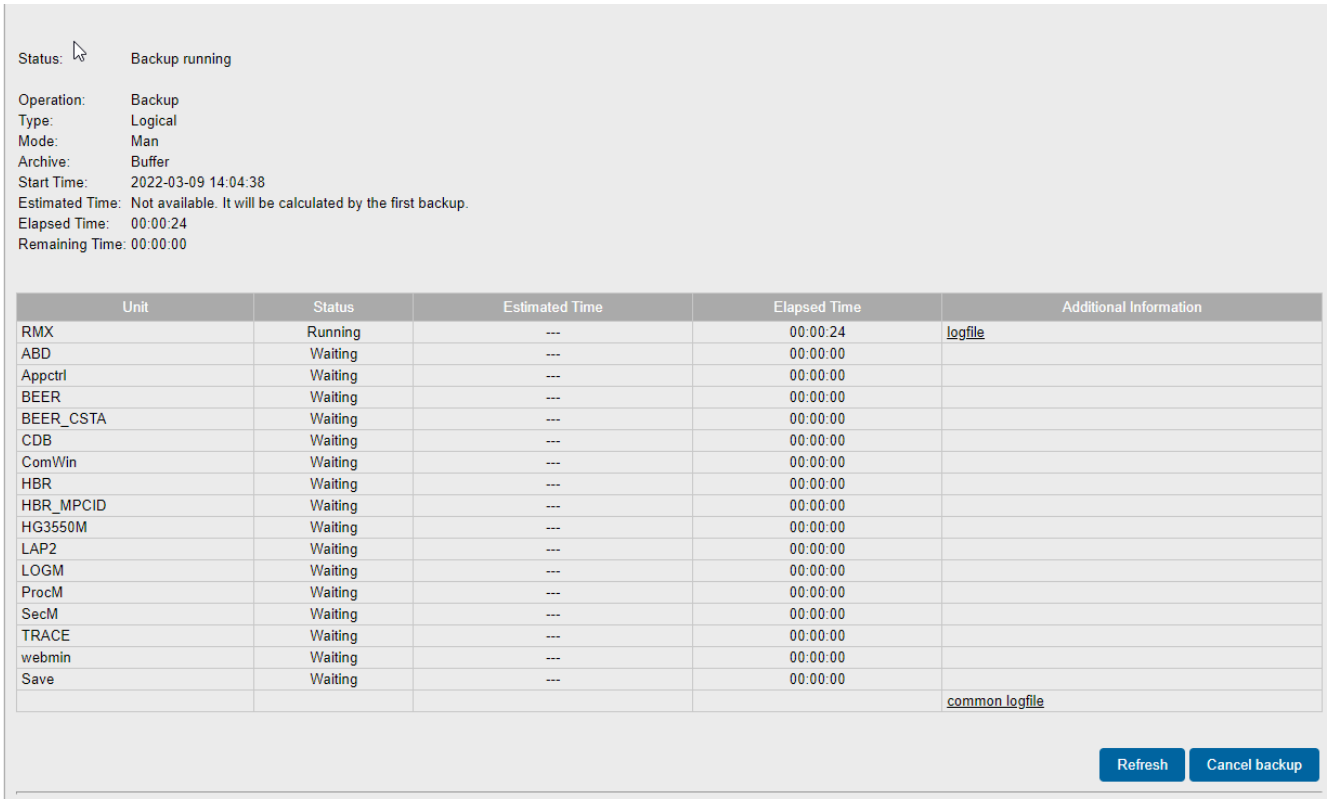


Figure 96: Status of the logical backup

Step 4: After the backup ends check also the **History** tab on the left to make sure that no errors occured during the backup.

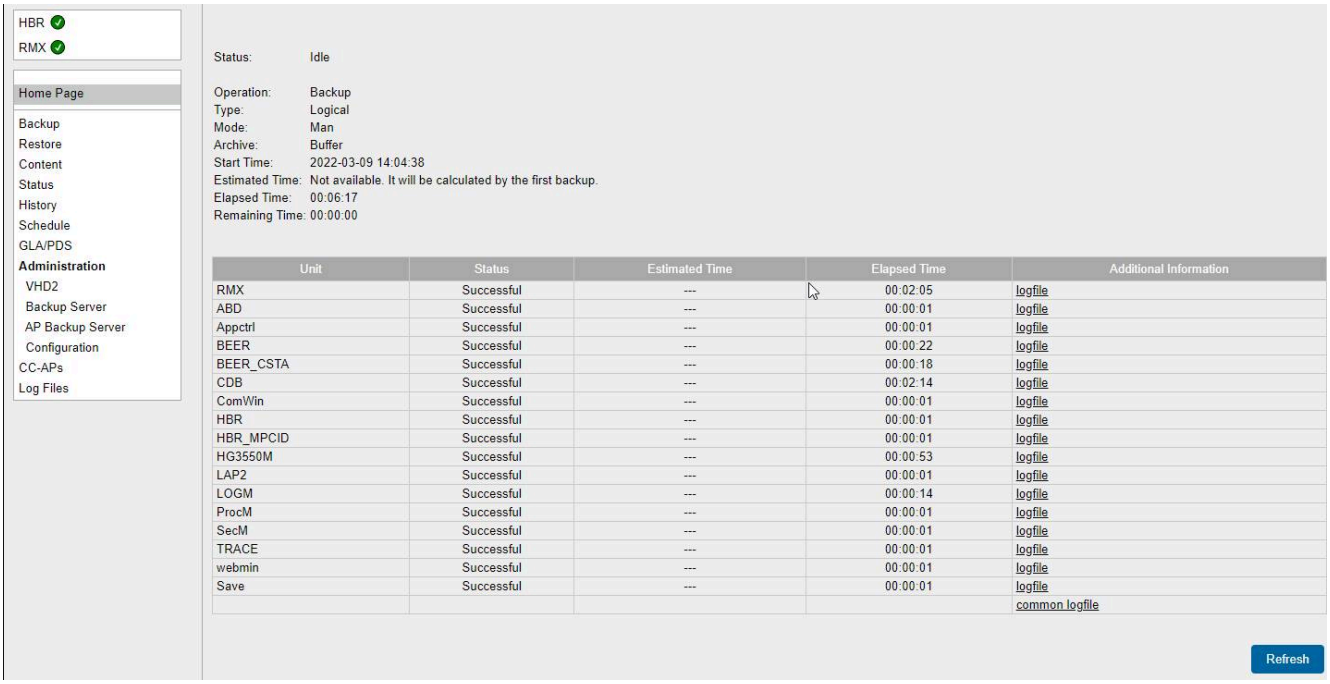


Figure 97: Check history of the logical backup

Then you have to check if the backup file has been created.

Follow these steps to see if the file has been created:

Establish a SSH connection to the linux host system (on Duplex and Separated Duplex Systems connection must be done on the active node).

Go to **/var/opt/Assistant/data/BACKUP/IO_BUF_TRANS/OUTPUT/**.

Check for a file named **backup_set.[date&time_code].Z**.

4.2.3 Save the Logical Backup

The RMX image archive and the logical backup created with OpenScape 4000 Assistant now will be stored on a USB stick.

IMPORTANT: You need to know how about mounting an USB stick on Linux.

---

1) Insert the USB Media Device in your system.
2) Establish a SSH connection to the linux host system (on Duplex and Separated Duplex Systems connection must be done on the active node).
3) Create a mounting point

   Example:

   # mkdir /mnt/pen
4) Mount the USB Media Device.

   Example:

   # mount /dev/sdc1 /mnt/pen

5) Copy the logical backup from the platform to the USB stick.

   Example:

   # cp /var/opt/Assistant/data/BACKUP/IO_BUF_TRANS/OUTPUT/backup_set.[date&time_code].Z /mnt/pen/

   IMPORTANT: Make sure that the [date&time_code] is the one corresponding to the latest backup.

6) Unmount the USB stick.

   Example:

   # umount /dev/sdc1

7) Remove the USB stick.

4.2.4 Final Steps before shutting down the HiPath 4000 V6 Host

- Take care to have the latest APE Backup executed on host and restored to all CCAPs.

  OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration > AP Backup Server

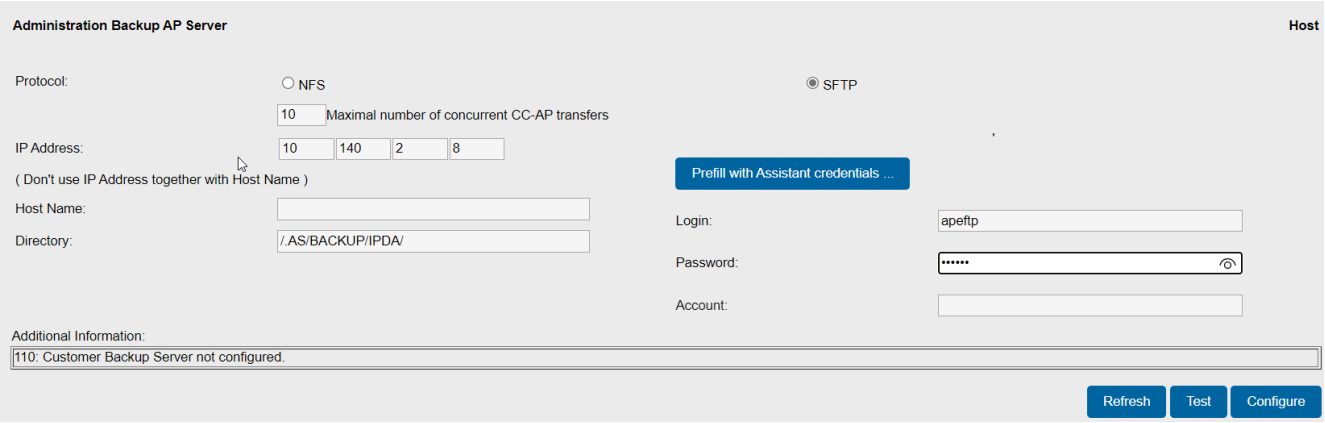


Figure 98: Disable automatic restore on all CC-APs

4.3 Migration of OpenScape 4000 Host System

After performing the OpenScape 4000 first installation and the configuration of OpenScape 4000 Platform Administration (Portal) on your system and the RMX, OpenScape 4000 Assistant and OpenScape 4000 CSTA are running you can start the migration process.

To perform the first installation you need a XML file with the configuration data of your system. This XML file can be created automatically from your "old" system (see Chapter 12, "Appendix D: How to Create a XML File Automatically".

For more information on the first installation please refer to Chapter 2, "First Installation".

4.3.1 Restore RMX Database

Restore the RMX database with GENDB. You need the file you created with PCDACON before the first installation (see Section 4.2.1, "Backup RMX Database").

Activate the system: `ACTIVATE-USSU:UNIT=LTG,LTG=1;`

Wait for all HG35xx boards to load (READY in RMX).

Perform `EXEC-UPDAT:UNIT=BP,SUSY=ALL;`

4.3.2 Restore OpenScape 4000 Assistant from the Logical Backup

NOTICE: After an upgrade, regardless of the old version, the OpenScape 4000 Assistant browser client preparation has to be carried out new on all client PCs. Starting with V10R1, Client Preparation requires openwebstart. For more details, see the Assistant Public Page -> Client Preparation.

Step 1: Upload your Backup set using the **Browse** button you find in **Software Management > Backup & Restore>Restore**. Choose your **backup_set.[date&time_code].Z** and press the **Upload** button. Wait until the upload is finished and then you can continue with step 2.

NOTICE: For the correct restore of component HG3550m the gateways must be already connected to the system of new version.

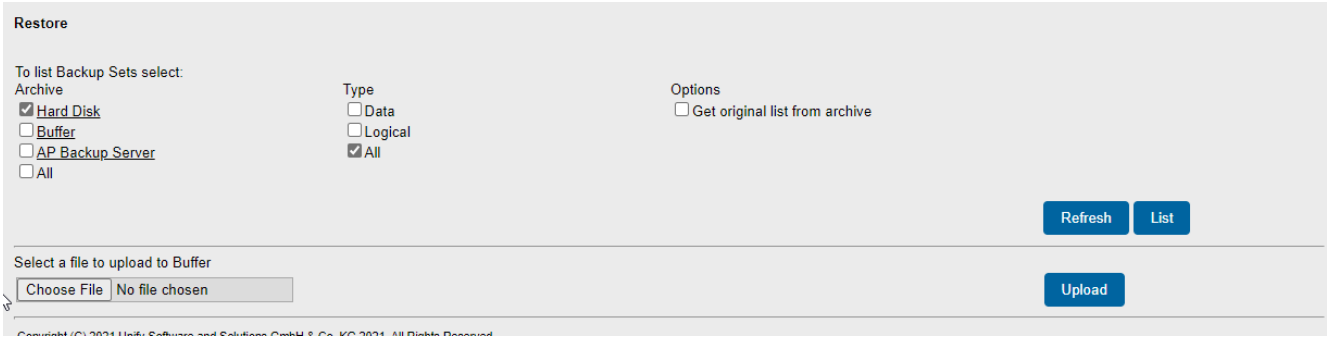


Figure 99: Restore the OpenScape 4000 Assistant

Step 2: Wait for the page to load. Then select from what backup you want to restore by checking the radio button in front of the row. To restore all Units select all checkboxes.

IMPORTANT: If Logical Backup was done correctly the **RMX** and **BEER** (**BEER_CSTA** must not be mixed up with **BEER**) component will not be displayed. In case the RMX and BEER components are displayed make sure they are NOT checked. RMX can not be migrated via logical backup/restore, because the regen syntax is changed between versions.

To start the restore click **Restore Set**.

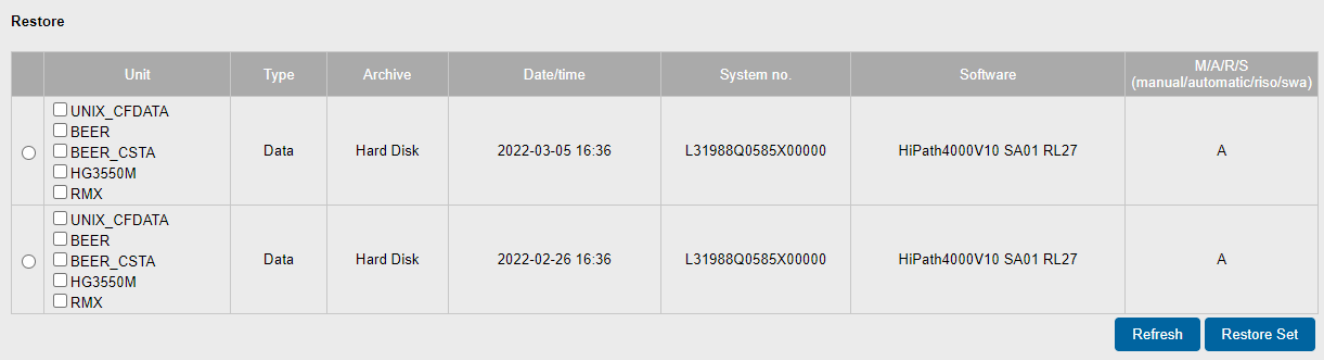


Figure 100: Select the backup file and set the restore options

Step 3: Wait for the restore to be finished and then restart OpenScape 4000 Assistant on the new system. You can do that by navigating to **OpenScape 4000 Assistant > Base Administration > Webmin** and clicking on **Reboot/ Shutdown** link on the left.

Figure 101: Restart OpenScape 4000 Assistant

Step 4: Start an "upload all" on the new system. You can do that by navigating to **OpenScape 4000 Assistant > Configuration Management > Network > System**, click on **Search**. When the system is found, select **Action > Upload** menu item.

Step 5: The new system is now running with grace period license. Import the official license files for OpenScape 4000 with OpenScape 4000 Assistant License Management.

License Management > Browse... > Select the license file **> Send**

IMPORTANT: In case of multi node deployment both licenses for active and standby should be imported!

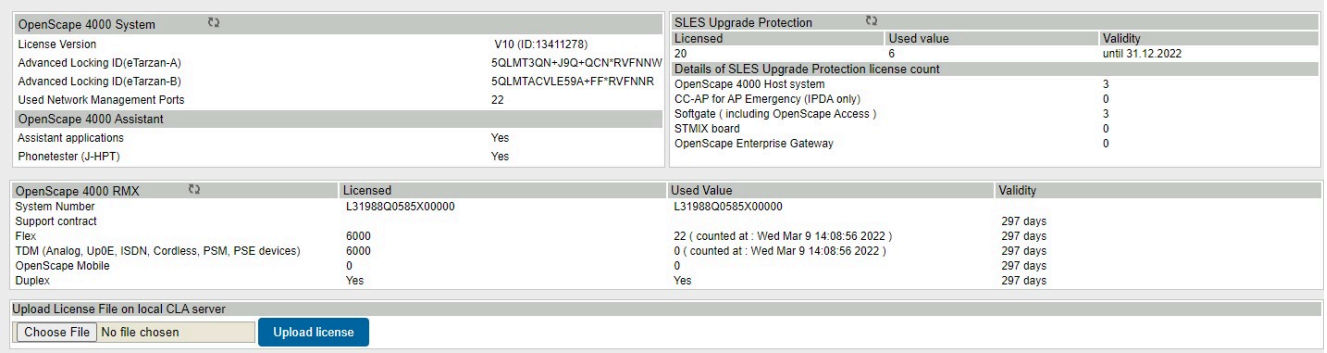


Figure 102: OpenScape 4000 Assistant - License file installation with license management

An automatic CODEW generation is executed after about 15-20 minutes. After that you may check the validity as described before.

Step 6: If web certificates for OpenScape 4000 Assistant have been activated in the previous version, then they are restored into the new version. However the relevant certificate has to be activated manually again. The certificate cannot be activated automatically because the input from the technician is required to insert the password of the certificate.

4.3.3 OpenScape 4000 SoftGate Configuration in Case of Signaling and Payload Encryption is Active

In case of Signaling and Payload Encryption was activated on HiPath 4000 V6/V7 and the OpenScape 4000 SoftGate has been reinstalled using the OpenScape 4000 Installation Media then the Master Encryption Key (MEK) must be manually added with the OpenScape 4000 Platform Administration (Portal):

System > LAN Configuration > SoftGate > under **SoftGate Master Encryption Key (MEK) Management > Master Encryption Key (MEK)**

NOTICE: In case of Standalone OpenScape 4000 SoftGate if OpenScape 4000 Platform Administration (Portal) IP address is not configured in XML file the OpenScape 4000 Platform Administration (Portal) can be reached via the NCUI IP address and port 8443 (e.g.https://NCUI_IP:8443).

NOTICE: For general OpenScape 4000 SoftGate configuration please refer to Section 2.3, "Manual OpenScape 4000 SoftGate Configuration".

NOTICE: After the migration the security checklist should be applied.

NOTICE: If the portal page cannot be accessed, MEK can be added to SoftGate or Enterprise GW via local console or ssh:
`/opt/soco/native/os/linux/mektool --mek=<MEK>`

4.4 Remote Appliance Reinstall/Update (RAR)

4.4.1 Important Hints

- The prerequisite for RAR is to have the central host already upgraded to the target version/release.
- It is not allowed to launch RAR on APE, Quorum, Standalone or Survivable OpenScape 4000 SoftGate.
- With RAR feature, the following remote appliances can be upgraded via host:
  - Standalone OpenScape 4000 SoftGate
  - Survivable OpenScape 4000 SoftGate
  - Enterprise GW
  - Survivable Enterprise GW
  - For Appliances configured as Standalone OpenScape 4000 SoftGate deployment, RAR will transfer and install the same software version as on the host including the last Platform HotFix. For appliances configured as APE or Survivable OpenScape 4000 SoftGate the upgrade to the last Platform HotFix applied the host should be done over the APE Backup and Restore Feature after RAR has completed.
- Host system has to be on target software release.
- RAR uses SSH and SFTP protocols. In order for RAR to work, the Host System (client) needs access to the TCP port 22 of the remote appliance (server).
- The terminal or service PC <-> host system connection can be closed. However, the RAR process is still running in the background.
- Approximately 3 GB will be transferred between host and remote appliance. In case of "Stand Alone OpenScape 4000 SoftGate" deployment only 1,5 GB will be transferred.
- LINUX root passwords of remote appliance are required.
- All remote appliances must use the same software version (Platform & RMX) as the host system. Should remote appliances have different versions to the host for any reason then they must be reinstalled with RAR (or other means) in order to synchronize software version before the next host RLC upgrade to avoid further upgrade issues.
- It is possible to schedule the time of the activation time reboot (activation) (e.g. Saturday, 03:00)) and to limit the bandwidth used by RAR for the transfer activities.
- Platform HotFixes upgraded on the Host System are not being transferred by RAR to targets configured as AP Emergency or Survivable SoftGate deployment. In order to activate the last Platform HotFix on such RAR targets, APE Restore must be used after RAR process has finished.

4.4.2 Process of the Remote Appliance Reinstallation/Update (RAR)

The whole process of the Remote Appliance Reinstallation/Update (RAR) can be divided into 4 parts:

- Part 1: Preparation on the remote appliance

  Preparation on remote appliance meaning disabling APE, checking password etc. This step can be completed before central host upgrade/(re)installation.
- Part 2: Preparation on the central host

  Preparation on the central host meaning HBR configuration. This step can only be completed **after** central host upgrade/(re)installation.
- Part 3: Start of actual RAR process in terminal window via script
- Part 4: Manual verification checks on reinstalled appliance via RAR (after successfully execution on host).

4.4.2.1 Part 1: Preparation on the remote appliance

OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration > AP Backup Server

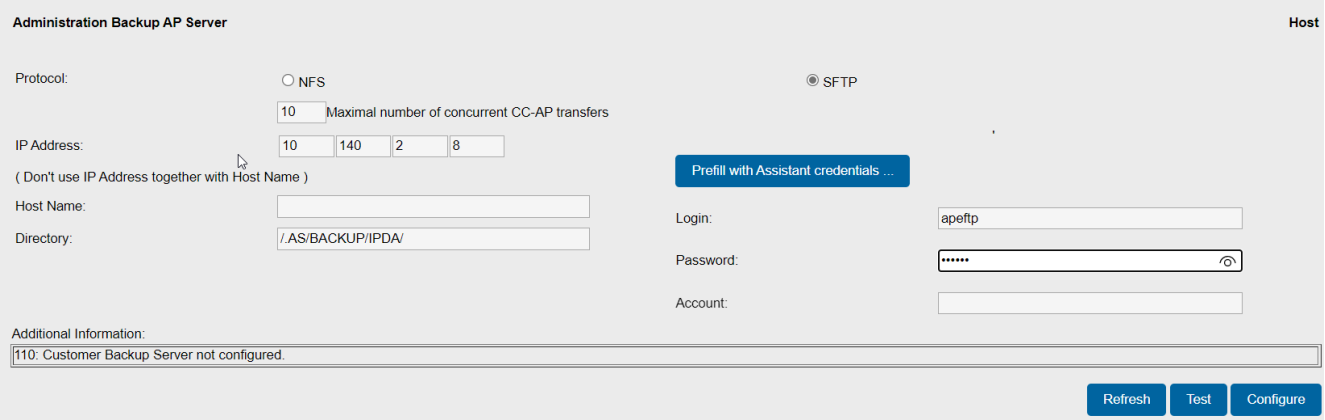


Figure 103: Disable automatic restore on all CC-APs

Password check via SSH:

Since RAR can not change the root password on remote appliance, it should be checked manually that on each remote appliance the password was changed (when you first login as root user you must change password).

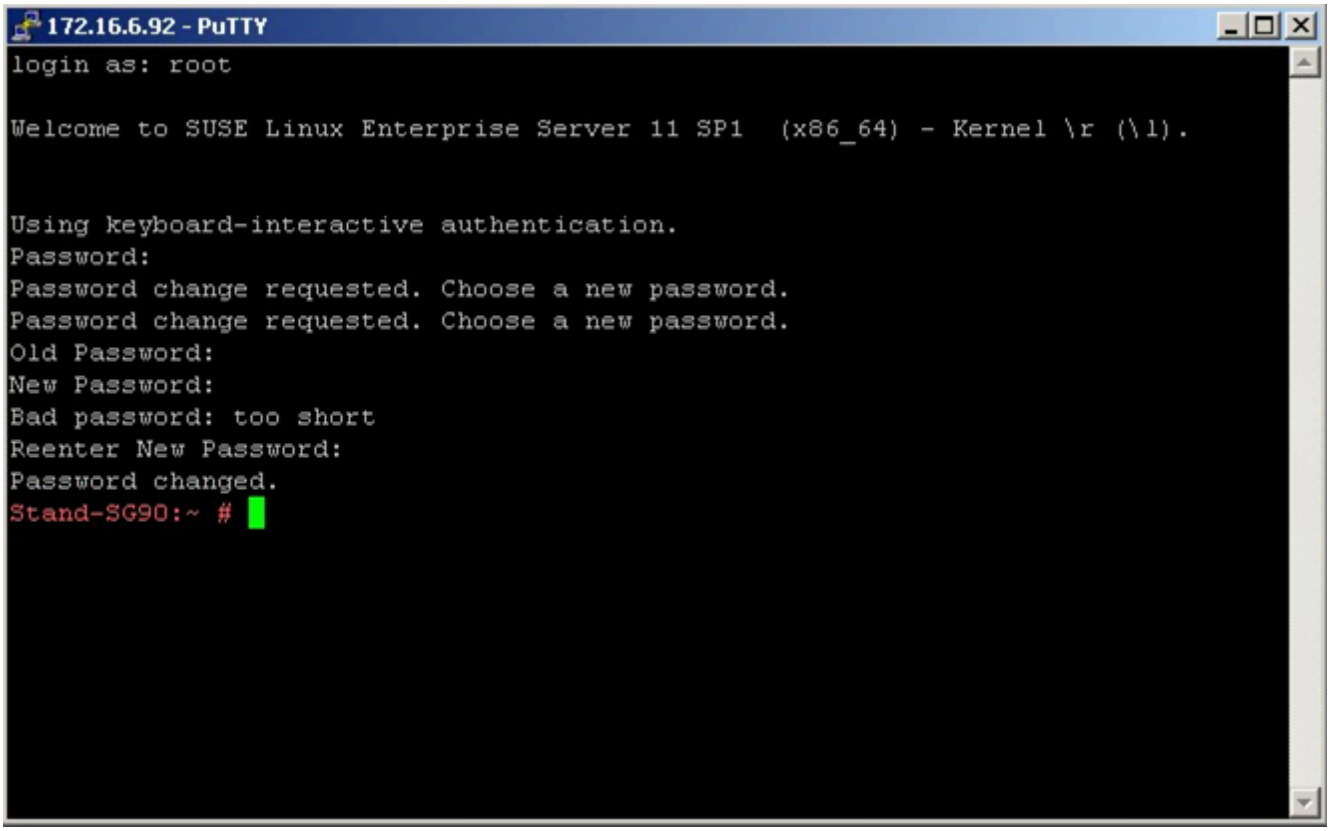


Figure 104: Password check via SSH

4.4.2.2 Part 2: Preparation on the central host

The host installation/upgrade is not described here.

After the completion of installation process on host, AP Backup Server should be configured or restored by HBR logical restore.

OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration > AP Backup Server

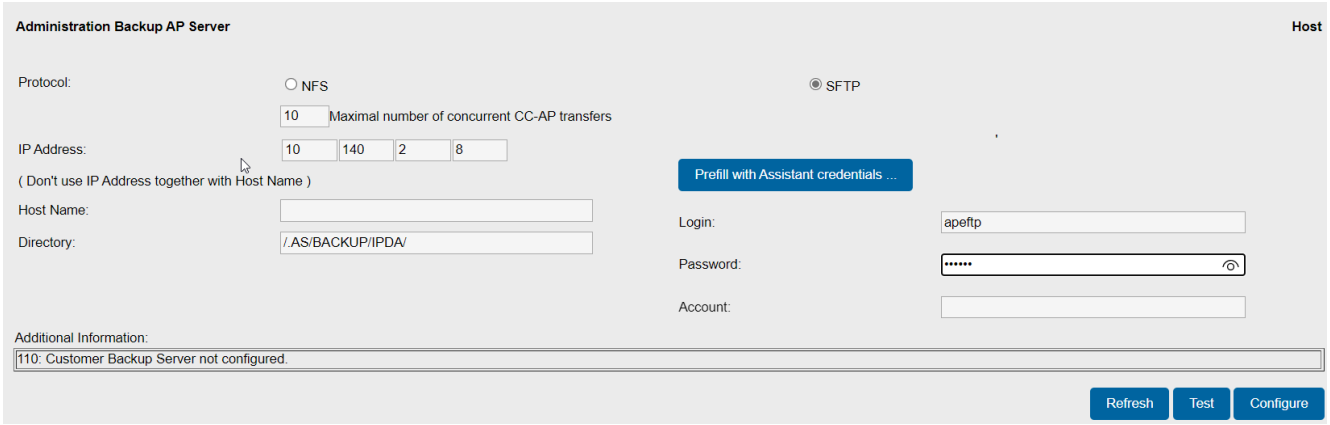


Figure 105: Configure/restore AP Backup Server

AP backup start on host to make sure that a fresh APE backup set exists on the AP backup server.

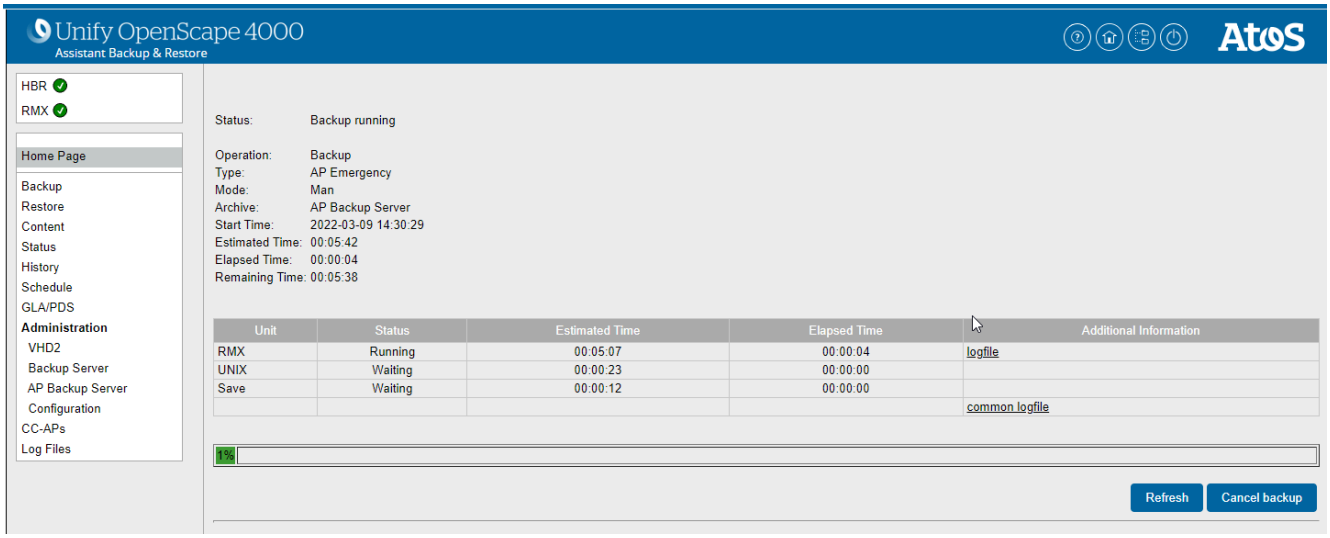


Figure 106: Create APE backup set

4.4.2.3 Part 3: Start of actual RAR process in terminal window via script

On Duplex deployments it is highly recommended to start RAR on standby node.

RAR script is started with the following parameters:

- physical IP (YAST) address of remote appliance (Survivable OpenScape 4000 SoftGate, Standalone OpenScape 4000 SoftGate, APE)
- root password on remote appliance
- scheduled activation time
- Optional parameter **no_version_check** to be used for forcing RAR to override installation on appliances which are already on the same Fix Release software version as the host. Use this for appliances configured as Standalone OpenScape 4000 SoftGate in order to transfer and install the latest Platform HotFix on them.
- By default RAR will install on the SoftGate (standalone or survivable) targets the LW that is contained in the RMX Harddisk of the host from where RAR is started (:A1H1E:APSP/LTG/LGA0/PZKSGW50).
- Optional parameter **keep_sg_version** to be used for forcing RAR to keep the SoftGate version that is already running on the target. However this is possible only if the Softgate was updated at least once with an official or private SG LW. If there was no such update the usage of this option has no effect and the RMX HDD version will be installed.

> **NOTICE:** Call the RAR command without parameters to display all possible parameter commands and options. For all options please refer to the RAR online help or to Section 4.4.3, "RAR Help".

Steps for RAR start from host:

- login as root in SSH session on host
- RAR 172.16.6.72 <root password> scheduled=<date_and_time>

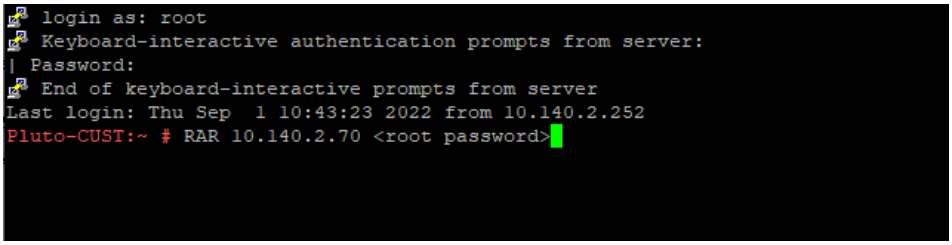


Figure 107: Start RAR on host

Notes regarding password

- If the password contains special characters (anything else then letters and numbers), then the password must be put between single quotes.

  RAR 172.16.6.72 'abc$efg' scheduled=2021.02.18-02:00
- If the ' (single quote) character is part of the password of the appliance, then it must be changed before starting RAR. RAR does not work if the appliance password contains ' (single quote).

Notes regarding scheduled activation

The RAR process consists of the following phases:

- transfer,
- background installation,
- waiting for scheduled activation,
- activation

These phases correspond to the RAR statuses as displayed by the RAR status command described further below: [TRANSFER-RUNNING], [REINSTALL-RUNNING], [SCHEDULED-ACTIVATION-PENDING], [ACTIVATION-STARTED]

During the transfer phase, the OpenScape 4000 software is being transferred from the host to the appliance over SFTP. This can take a variable amount of time depending on the bandwidth available between the two machines.

All other phases are running then on the remote appliance independently and the amount of time needed depends on the harwdare performance of the appliance machine.

The activation of the new software on the remote appliance machine can take place only once the background installation phase has completed.

In order to control the activation time which implies a reboot and thus telephony services downtime, the parameter scheduled activation time should be used. The remote appliance will wait for the scheduled activation time and only then do the activation.

If for some reason the scheduled activation time is reached and the necessary prerequisites are not fulfilled, then RAR will stop with corresponding error message and the RAR process needs to be started again.

If an unexpected reboot or power failure occurs during the waiting for scheduled activation, then the activation of the new software will happen immediately after the appliance is again started. This will spare an extra downtime later since a recent downtime has already occurred. However, if for some reason this is not wanted, then the option "no_activation_on_reboot" can be used to prevent this behavior. For e.g.:

RAR 172.16.6.72 'abc$efg' scheduled=2021.02.18-02:00 no_activation_on_reboot

In the case that the "no_activation_on_reboot" option is specified and an unexpected reboot occurs, then the RAR process will resume waiting for the scheduled activation time and will carry on with the steps as described above.

NOTICE: If option "no_activation_on_reboot" is not specified and RAR has already reached the waiting for scheduled activation phase, the activation can be triggered by the user at any time before the scheduled activation time by just issuing a Linux reboot on the appliance.

The scheduled activation time is expressed in the time zone of the host. If different time zones are configured for the host and for the appliance, the user must calculate the corresponding time difference in order to plan the scheduled activation time correctly.

E.g. host is on GMT+1 and appliance is on GMT+2. Then in order to plan the scheduled activation on the appliance to be done on 24 February 2021 at 2:00 AM local time on the appliance, the scheduled activation time to be passed to the RAR command must be 2021.02.24-01:00.

During the script runs, the terminal window is dedicated for outputs.

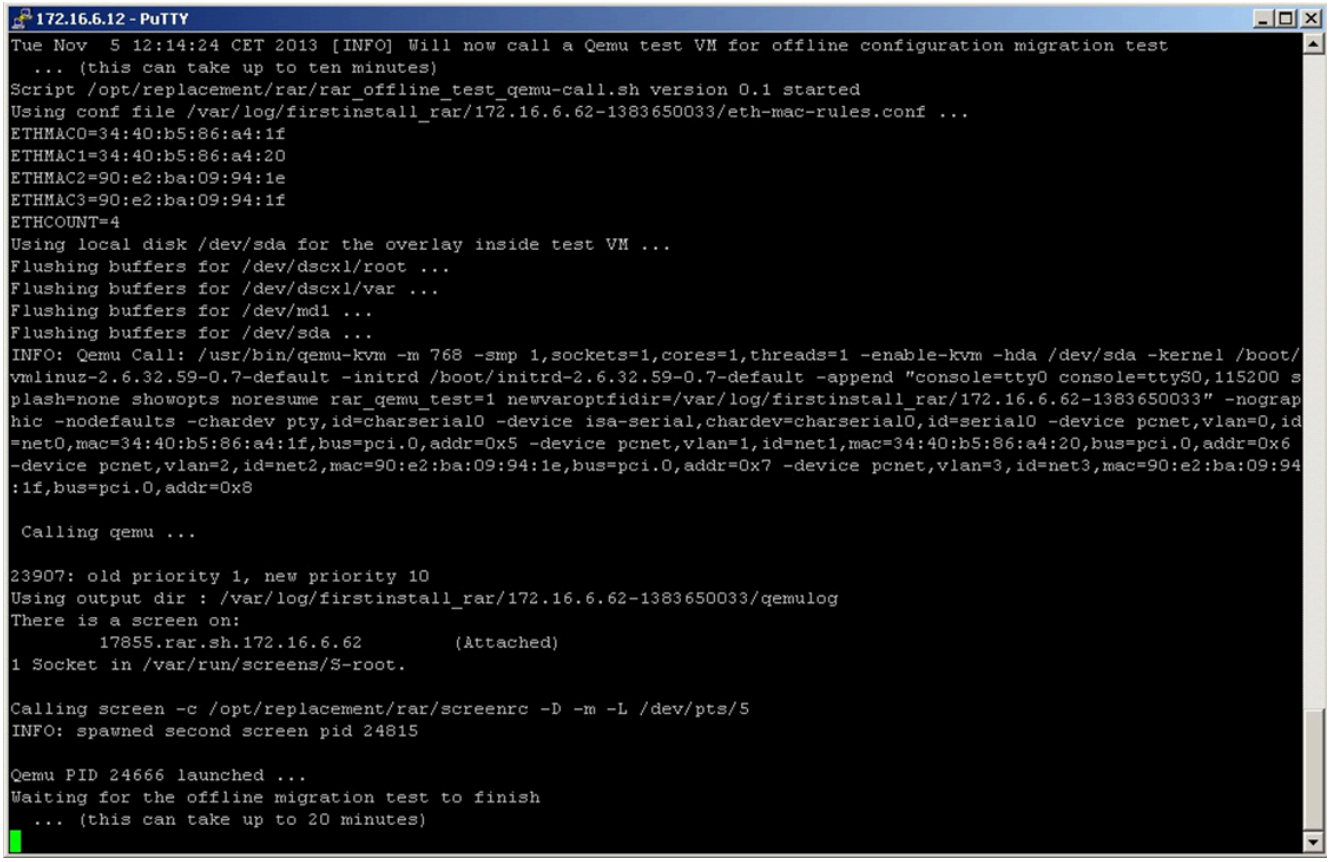


Figure 108: Outputs during RAR process

The RAR script on the host will stop after the transfer to the appliance has completed and the background installation activities are initiated. To continue getting live information from the appliance the monitor command can be used:

RAR monitor 172.16.6.72

It is possible to start RAR activities with scheduled activation time for multiple RAR appliances at the same time. In order not to use too many resources on the host, a maximum number of 5 RAR sessions are allowed to perform transfer activities at the same time. Any RAR session started when this number has already been reached will wait until one of the other running RAR instances finishes the transfer. The RAR appliance status for this case is [WAITING-TO-TRANSFER].

For narrow bandwidth connections between host and appliance the parameter "bandwidth" can be used when starting RAR. For e.g.:

RAR 172.16.6.72 'abc'\'efg' scheduled=2021.02.18-02:00 bandwidth=1000

The bandwidth parameter is expressed in Kilobits per second and must be an integer number.

Cancelling RAR process

If for some reason the user decides to interrupt the RAR process for an appliance then this can be done with the cancel command:

RAR cancel 172.16.6.72

This will initiate the cancellation and the RAR process will be stopped in a nice and safe way during the next minutes. More details can be checked live with the monitor command.

A RAR process cannot be cancelled if the activation has already begun on the remote appliance.

Possible RAR status sequences

Possible RAR status sequences on survivable OpenScape 4000 SoftGate and on CC-AP are:

172.16.6.72 active [STARTING] @ Tue Nov 5 14:54:06 CET 2021

172.16.6.72 active [DATA-COLLECT-PENDING] @ Tue Nov 5 14:54:08 CET 2021

172.16.6.72 active [DATA-COLLECT] @ Tue Nov 5 14:57:06 CET 2021

172.16.6.72 active [WAITING-TO-TRANSFER] @ Tue Nov 5 14:58:00 CET 2021

172.16.6.72 active [TRANSFER-RUNNING] @ Tue Nov 5 14:58:06 CET 2021

172.16.6.72 active [STARTING-REINSTALL] @ Tue Nov 5 15:03:05 CET 2021

172.16.6.72 active [REINSTALL-RUNNING] @ Tue Nov 5 15:07:58 CET 2021

172.16.6.72 active [SCHEDULED-ACTIVATION-PENDING] @ Tue Nov 5 15:29:41 CET 2021

172.16.6.72 active [ACTIVATION-STARTED] @ Tue Nov 5 15:32:33 CET 2021

172.16.6.72 active [HEALTH-CHECK] @ Tue Nov 5 15:48:10 CET 2021

172.16.6.72 active [VERSION-CHECK] @ Tue Nov 5 15:49:11 CET 2021

172.16.6.72 active [ASSISTANT-INSTALLATION] @ Tue Nov 5 15:49:16 CET 2021

172.16.6.72 active [APE-HBR-CONFIG-RESTORE] @ Tue Nov 5 16:10:37 CET 2021

172.16.6.72 active [APE-RESTORE-RUNNING] @ Tue Nov 5 16:12:12 CET 2021

172.16.6.72 .... done [SUCCESS] @ Tue Nov 5 16:12:13 CET 2021

or in case of failed RAR:

13. 172.16.6.72 .... done [ERROR] @ Tue Nov 5 16:12:13 CET 2021

Possible RAR status sequences on standalone OpenScape 4000 SoftGate are:

172.16.6.82 active [STARTING] @ Tue Nov 5 14:40:28 CET 2021

172.16.6.82 active [DATA-COLLECT-PENDING] @ Tue Nov 5 14:40:30 CET 2021

172.16.6.82 active [DATA-COLLECT] @ Tue Nov 5 14:46:43 CET 2021

172.16.6.82 active [WAITING-TO-TRANSFER] @ Tue Nov 5 14:47:40 CET 2021

172.16.6.82 active [TRANSFER-RUNNING] @ Tue Nov 5 14:47:43 CET 2021

172.16.6.82 active [STARTING-REINSTALL] @ Tue Nov 5 14:52:05 CET 2021

172.16.6.82 active [REINSTALL-RUNNING] @ Tue Nov 5 14:52:37 CET 2021

172.16.6.72 active [SCHEDULED-ACTIVATION-PENDING] @ Tue Nov 5 14:58:40 CET 2021

172.16.6.82 active [ACTIVATION-STARTED] @ Tue Nov 5 15:00:52 CET 2021

172.16.6.82 active [HEALTH-CHECK] @ Tue Nov 5 15:06:42 CET 2021

172.16.6.82 active [VERSION-CHECK] @ Tue Nov 5 15:07:14 CET 2021

172.16.6.82 .... done [SUCCESS] @ Tue Nov 5 15:07:22 CET 2021

or in case of failed RAR:

10. 172.16.6.82 .... done [ERROR] @ Tue Nov 5 15:07:22 CET 2021

The RAR status can be checked in another SSH session / window with the command `RAR status`.

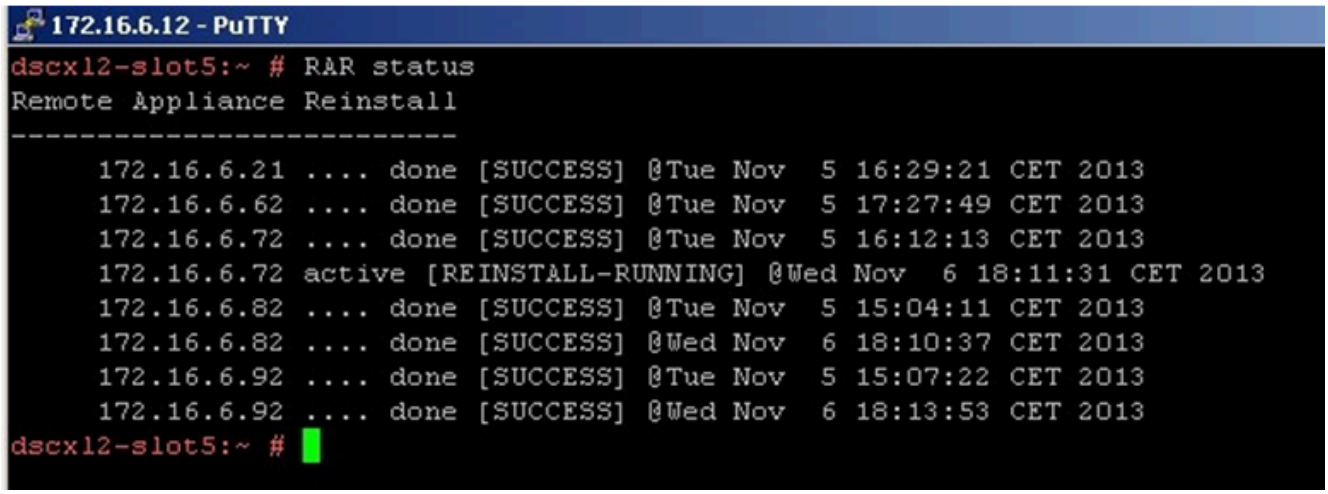


Figure 109: RAR status

Successfully executed RAR script will be ended with:

Tue Nov 5 16:12:13 CET 2021 [PASSED] **Remote Appliance Reinstallation finished OK**.

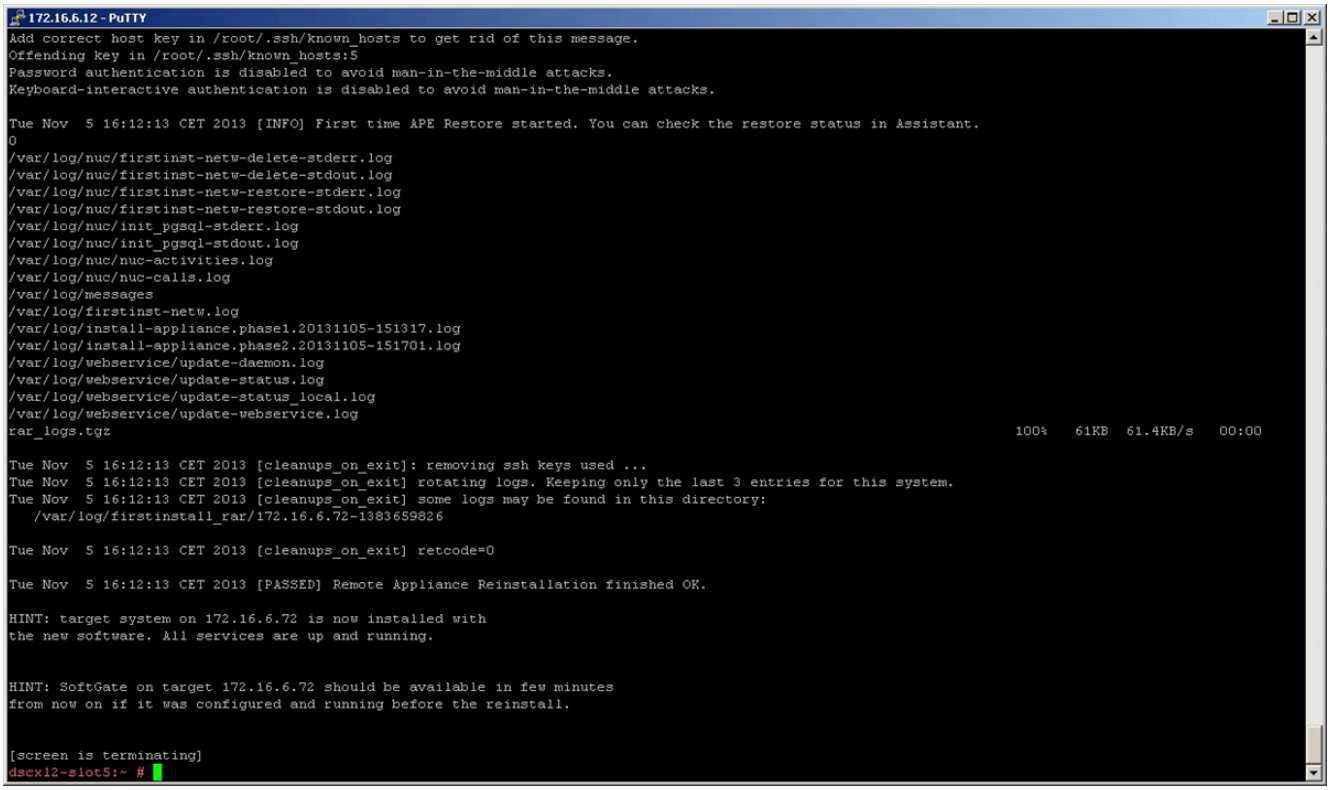
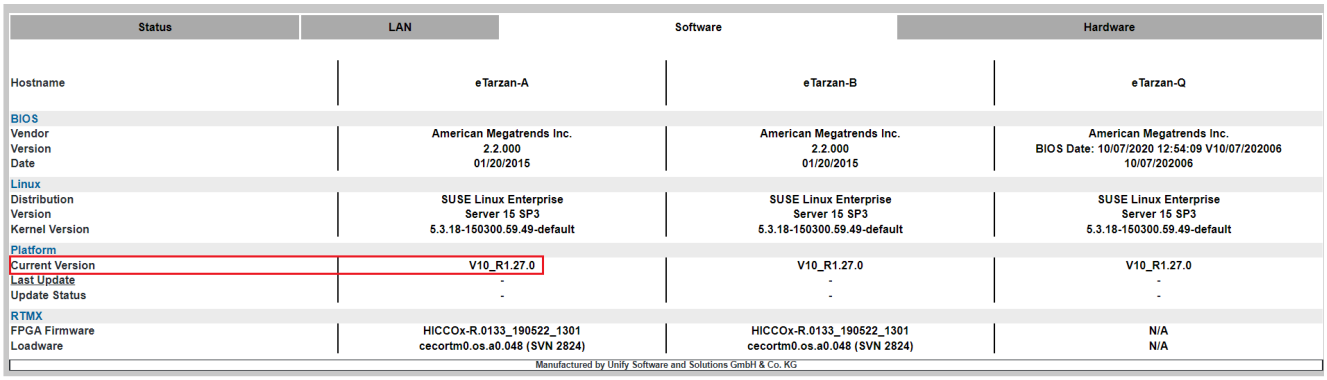


Figure 110: RAR finished successfully

4.4.2.4 Part 4: Manual verification checks on reinstalled appliance via RAR

- on reinstalled appliance **OpenScape 4000 Platform Administration (Portal)**



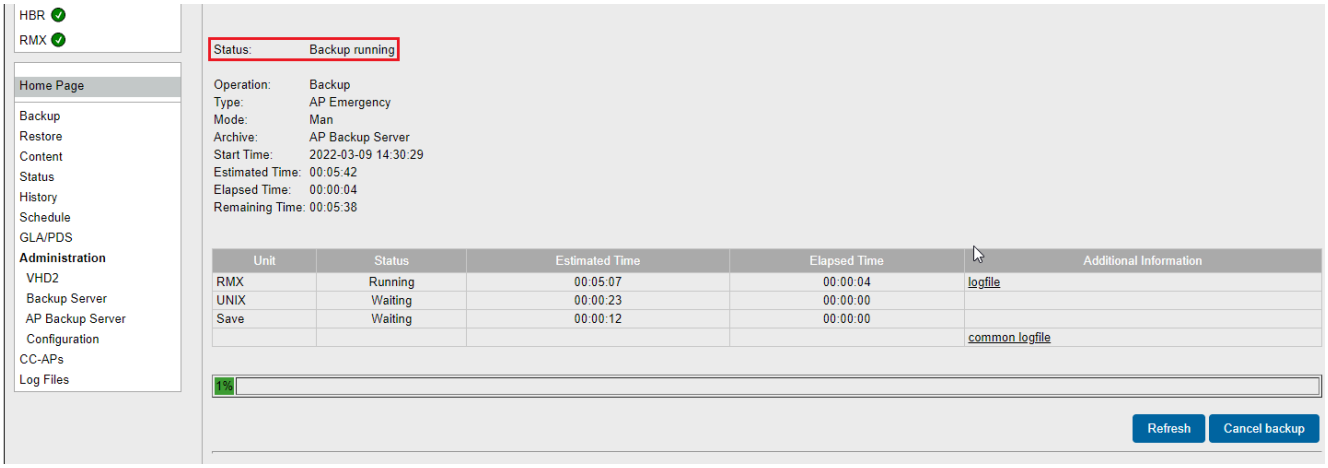
Status	LAN	Software	Hardware
Hostname	eTarzan-A	eTarzan-B	eTarzan-Q
BIOS			
Vendor	American Megatrends Inc.	American Megatrends Inc.	American Megatrends Inc.
Version	2.2.000	2.2.000	BIOS Date: 10/07/2020 12:54:09 V10/07/202006
Date	01/20/2015	01/20/2015	10/07/202006
Linux			
Distribution	SUSE Linux Enterprise	SUSE Linux Enterprise	SUSE Linux Enterprise
Version	Server 15 SP3	Server 15 SP3	Server 15 SP3
Kernel Version	5.3.18-150300.59.49-default	5.3.18-150300.59.49-default	5.3.18-150300.59.49-default
Platform			
Current Version	V10_R1.27.0	V10_R1.27.0	V10_R1.27.0
Last Update	-	-	-
Update Status	-	-	-
RTMX			
FPGA Firmware	HICCOx-R.0133_190522_1301	HICCOx-R.0133_190522_1301	N/A
Loadware	cecortm0.os.a0.048 (SVN 2824)	cecortm0.os.a0.048 (SVN 2824)	N/A

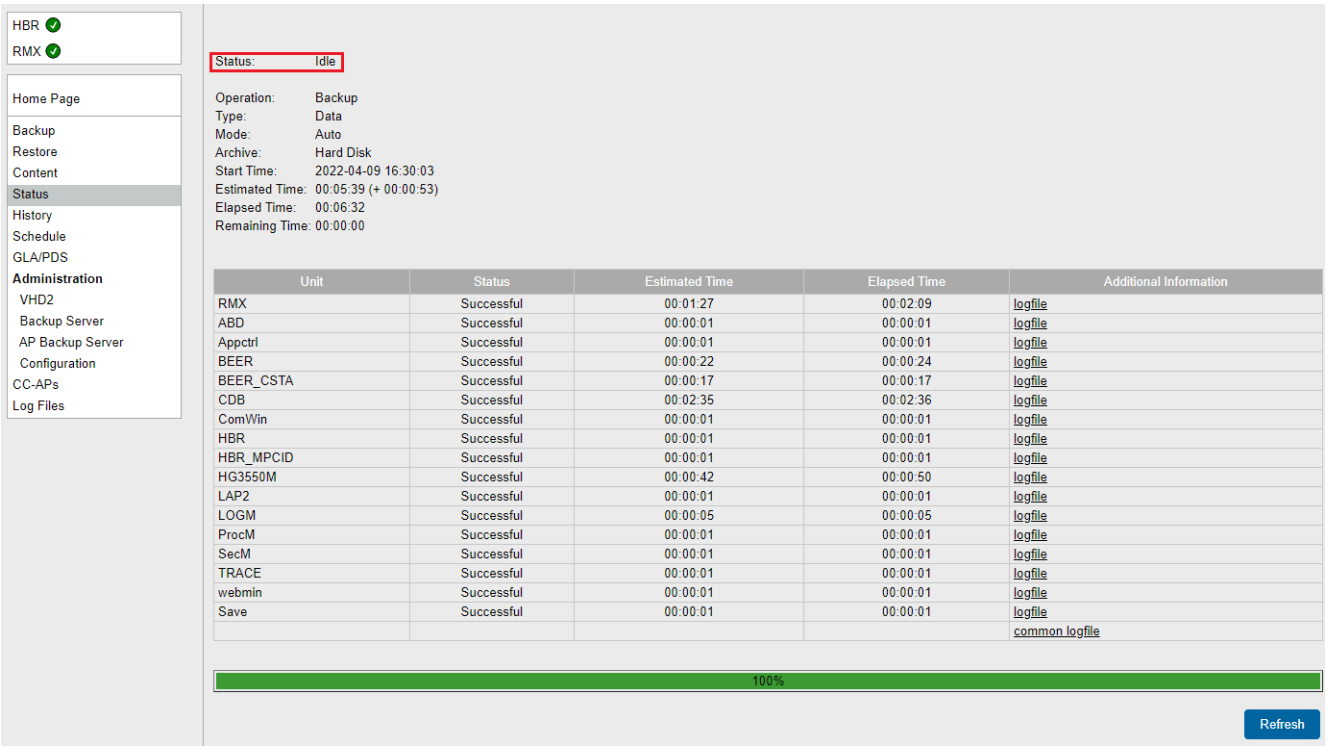
Manufactured by Unify Software and Solutions GmbH & Co. KG

Figure 111: Check software version in Platform Administration (Portal)

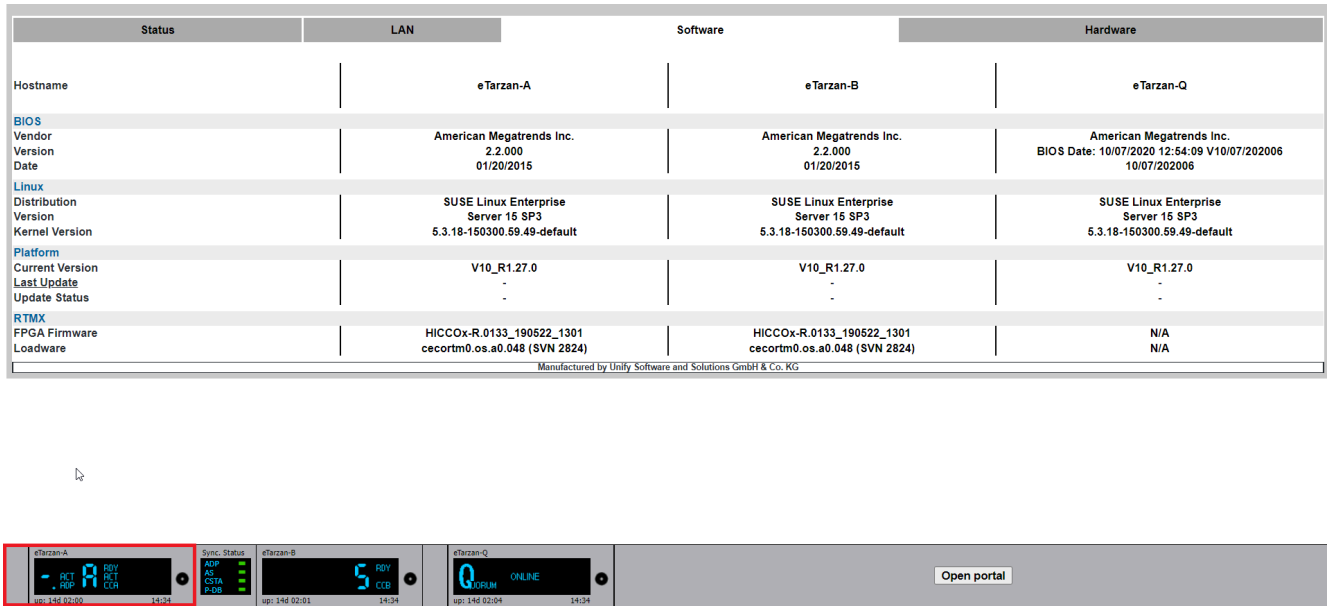
- Survivable OpenScape 4000 SoftGate or an APE EcoServer
- If the reinstalled appliance is a Survivable OpenScape 4000 SoftGate the first APE Restore process will take place automatically, overriding the

deactivation flag in AP Backup Server Configuration web page. The Restore status can be checked in APE's OpenScape 4000 Assistant as usual:





When the AP Restore is finished, CC-AP should be in "A" status:



Status	LAN	Software	Hardware
Hostname	eTarzan-A	eTarzan-B	eTarzan-Q
BIOS			
Vendor	American Megatrends Inc.	American Megatrends Inc.	American Megatrends Inc.
Version	2.2.000	2.2.000	BIOS Date: 10/07/2020 12:54:09 V10/07/202006
Date	01/20/2015	01/20/2015	10/07/202006
Linux			
Distribution	SUSE Linux Enterprise	SUSE Linux Enterprise	SUSE Linux Enterprise
Version	Server 15 SP3	Server 15 SP3	Server 15 SP3
Kernel Version	5.3.18-150300.59.49-default	5.3.18-150300.59.49-default	5.3.18-150300.59.49-default
Platform			
Current Version	V10_R1.27.0	V10_R1.27.0	V10_R1.27.0
Last Update	-	-	-
Update Status	-	-	-
RTMX			
FPGA Firmware	HICCOx-R.0133_190522_1301	HICCOx-R.0133_190522_1301	N/A
Loadware	cecortm0.os.a0.048 (SVN 2824)	cecortm0.os.a0.048 (SVN 2824)	N/A

Manufactured by Unify Software and Solutions GmbH & Co. KG

Figure 112: Check status in CC-AP

OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration AP Backup Server

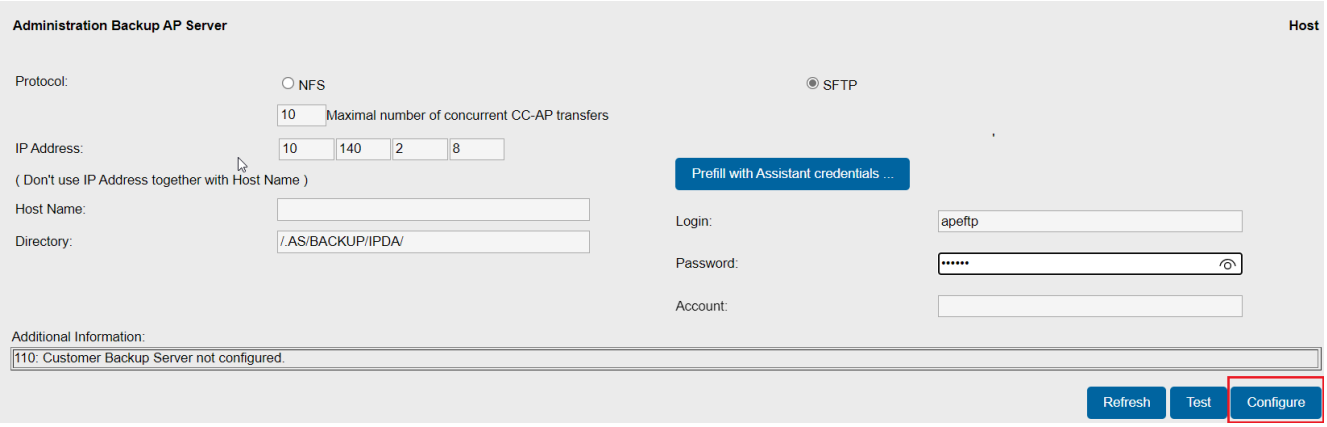


Figure 113: Allow automatic APE restore

- Standalone OpenScape 4000 SoftGate

- If the reinstalled appliance is a Standalone OpenScape 4000 SoftGate the OpenScape 4000 Assistant will not be installed and AP Restore will not be started.

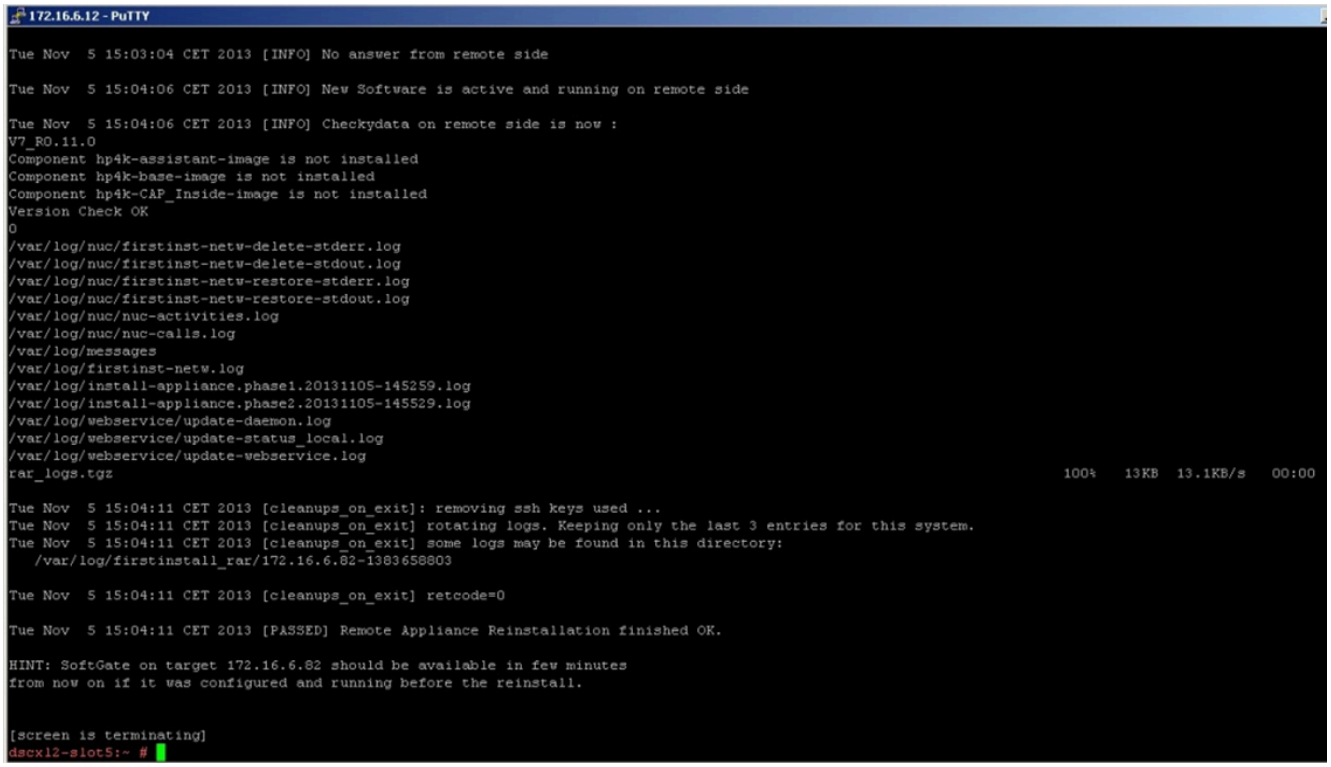


Figure 114: RAR finished successfully on a Standalone OpenScape 4000 SoftGate

OpenScape 4000 SoftGate status can be checked manually in SSH session on OpenScape 4000 SoftGate linux machine:

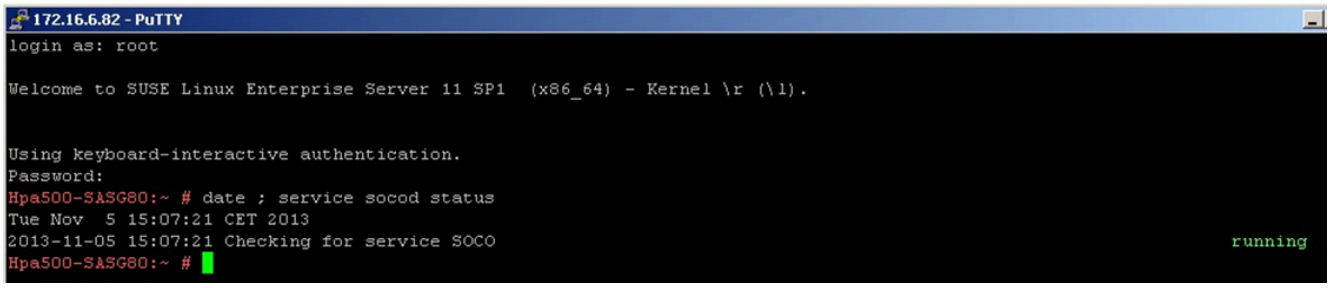


Figure 115: Check status of OpenScape 4000 SoftGate

Platform status on OpenScape 4000 SoftGate can be checked using linux command `checkydata`.

4.4.3 RAR Help

sys1:~ # RAR

Remote Appliance Reinstall 6.1

Usage:

RAR <IP_Address> <root_pasword> [<option1> <option2> ...]
- start RAR on given target system including automatic APE restore
launching at the end of RAR. Please read carefully the RAR
documentation in case the password contains special characters like $
- possible options are (space separated) :
no_version_check - forces RAR to perform the reinstall
wihtout checking target SW version
no_ape_restore - start RAR on given target system WITHOUT
automatic APE restore launching at the end
of RAR. User must do restore manually.
keep_sg_version - use current SoftGate LW version
in the newly installed Linux platform.
To be used in case the latest LW HotFix
or a private LW was applied prior to starting
the RAR process. If there was no previous
LW update, then the LW from RMX Harddisk
will be installed on the SG appliance.
scheduled=<date_and_time> - do all reinstall actions except for
the activation reboot which will happen at the
moment given by <date_and_time>. The format
is : YYYY.MM.DD-HH:mm where :
YYYY is the year
MM is the month
DD is the day
HH is the 24-hours format hour
mm is the minute
Note: the time is considered in the timezone
of the Host system from which RAR is started.
no_activation_on_reboot - do not activate new software in case an
unexpected reboot occurs during waiting for
scheduled activation moment to come
bandwidth=<bandwidth_in_Kbits> - limit used bandwidth to the given
amount expressed in Kbits.
RAR status [<IP_Address>|--active|--long]
- print overall status of RAR activities. If IP address is given
then show detailed information for given target system
- the "--active" option displays just active running instances

- the "--long" option displays the complete history

RAR cancel [<IP_Address>]

- interrupt and abort the execution of given RAR instance

RAR attach <IP_Address>

- re-attach to the terminal of an active running RAR

To dettach just close the terminal window or press CTRL-ad

!! Do NOT use CTRL-c to dettach since this will interrupt RAR !!

RAR monitor <IP_Address>

- monitor execution of remote RAR after it has started reinstall

RAR clear <IP_Address>|all

- clear run history for given target system or for all

4.5 Reinstallation from Recovery ISO image

The Recovery ISO feature including the reinstallation process is described in the "OpenScape 4000 Assistant, Appliance Management, Administrator Documentation" in Chapter Reinstallation of an appliance from Recovery ISO image.

5 Update/ Upgrade Process of OpenScape 4000

OpenScape 4000 supports updating the central system components (host system including OpenScape 4000 Assistant, OpenScape 4000 CSTA, etc.) and the peripheral system components (access points, Survivable units) in a single procedure.

Please see Chapter 4, "Migration and Reinstallation of legacy systems" for information about migration to OpenScape V10.

IMPORTANT: The whole update process can be performed from remote. No on site assistance is necessary.

The update process is done in two phases:

- Preparation Phase

  The preparation is started automatically after the RLC package has been transferred to the hard disk. During the preparation phase the software is copied to the directory `var/newdisk` and the loadware of the IP boards is distributed.

  During preparation phase there is no telephony downtime.

- Activation Phase

  In the activation phase the new loadware will be loaded, backup of all data is done and then the installation takes place followed by a restore of all backed up data.

  For the update process only the OpenScape 4000 Assistant applications Software Manager and Software Activation are needed.

  The update process is performed in the following sequence:

  1) Quorum (if available)
  2) Standby node (if available)
  3) Active node

  During the update process different timers are installed to "monitor" the process. In case one of these timers is exceeded, a roll back to the former system version is initiated. For an updated node the timer is 20 minutes.

IMPORTANT: Starting with V8R1, for Duplex and Geo-Separated Duplex deployments the Standby node is upgraded in the background, resulting in substantial less telephony downtime. The telephony downtime of these deployments is now comparable to a power on loading of the system.

Deployment	Expected Total Upgrade Time [1]		Expected Time until RMX Downtime [1]		Expected Total RMX Downtime [1]
	GenDB during upgrade (default)	Without GenDB during upgrade	GenDB during upgrade (default)	Without GenDB during upgrade	
Simplex [2]	[3]	Up to 1:30 hours	[3]	Up to 25 min [3]	Approx. 20 min +

Deployment	Expected Total Upgrade Time [1]		Expected Time until RMX Downtime [1]		Expected Total RMX Downtime [1]
	GenDB during upgrade (default)	Without GenDB during upgrade	GenDB during upgrade (default)	Without GenDB during upgrade	
Duplex [2]	[3]	Up to 2:00 hours	[3]	Up to 25 min [3]	Approx. 5 min + [4]
GSD [2]	[3]	Up to 2:00 hours	[3]	Up to 25 min [3]	Approx. 5 min + [4]

[1] Times are based on previous lab tests and are only for reference. They **are not** guaranteed.

[2] Times are based on ECO Servers/EcoBranch HW.

[3] The total duration depends on customer’s HW configuration.

[4] Time comparable to a normal system reload of the customer.

These times are based solely on system upgrade and **do not** include transfer and activation times for GW loading. To minimize Transfer times (in addition to SWA Reduced Downtime feature), the GW LWs versions can already be distributed and activated before starting the upgrade where the GW LW APS variant is compatible (i.e. the same GW versions are usually available for the previous FR as a LW HF!).

These times depend on customer's network. In case of a large IPDA system, it might take longer until every IPDA is fully back in service.

IMPORTANT:

Within the same Minor Release (e.g. V10 R1.34 to V10 R1.42), only for Duplex deployments (GSD not supported), when RMX versions are compatible, the RLC update will take place with no telephony downtime. From RMX SWU point of view, the RLC upgrade looks like a soft restart, meaning that the already connected calls will be preserved.

To benefit from “no telephony downtime”, on the SWA page the “Activate the OS on Standalone SoftGate, STMIX, STMIY and Enterprise GW after Transfer” option has to be unchecked and later the user/admin has to manually update the LW and OS via Gateway Manager.

NOTICE: The ADP is fully reloaded, and all CTI/CSTA/... applications (e.g. UC or ContactCenter) will lose connection (same situation as for previous RLC updates).

The log files for the update process can be found in the directory `var/log/nuc` and are included in the OpenScape 4000 Administration Platform (Portal). All NUC Upgrade logs can be collected from the **OpenScape 4000 Administration Platform (Portal)** in both success and failure situations by selecting all together the "Update", "messages", "Webservice" and "Firstinstall" check boxes.

5.1 Update process

The HotFix package is transferred to the system via Software Manager (SWM) and subsequently activated via Software Activation (SWA). In the next step, the RLC V10 is uploaded via SWM and activated via SWA.

After successful HotFix application and RLC upload, follow the process described in the chapters below to upgrade to the Major Release:

Major Release upgrade

Update/ Upgrade Process of OpenScape 4000 on page 146

5.1.1 Prerequisites

When upgrading from OpenScape 4000 V8 R2/ V10 R0, it is recommended that all the latest Hotfixes are transferred and applied on the system before the V10 upgrade.

- Parameter **NOIPBLWL** in AMO ZANDE

  To reduce telephony downtime the parameter **NOIPBLWL** (**No IP B**oard **L**oad**w**are **L**oad) in AMO ZANDE must be set to **YES**. If this parameter is set to **YES** then the new loadware of an IP board is not loaded in case of a restart/reboot.

  ```
  CHANGE-ZANDE:TYPE=ALLDATA2,NOIPBLWL=YES;
  EXEC-UPDAT:UNIT=BP,SUSY=DELTA;
  ```

  IMPORTANT: Perform an APE Backup to be sure that the setting on the access points is also correct.

  In case the recommended **NOIPBLWL** parameter is not used the sequence of events will look like this:

  1) During the Update, NCUIs/CGWs and OpenScape 4000 SoftGates will receive OpenScape 4000 V10 R0/ V10 R1 loadware via reduce down time feature via https (default).
  2) Then the system will go down and NCUIs/CGWs and OpenScape 4000 SoftGates will switch to APE if configured.
  3) Since APE/Survivable unit has at least OpenScape 4000 V8 R2 loadware, it will overwrite the OpenScape 4000 V10 R0/ V10 R1 loadware which has been downloaded in step 1 and the switch over to APE will be extremely slow because the loadware will be transferred by FTP to the NCUIs and STMIs.
  4) When the RLC is finished, NCUIs/CGW and OpenScape 4000 SoftGate will switch back from APE to host and NCUIs/STMIs will download

OpenScape 4000 V10 R0/ V10 R1 loadware via FTP (which is again slow).

In case the recommended **NOIPBLWL** parameter is used (set to **YES**) we will avoid the FTP download in steps 3 and 4, which will make the switch to APE and from APE to host (startup after NUC) extremely fast.

Remarks:

– If no APE is used then the **NOIPBLWL** parameter setting is not needed.
– If the OpenScape 4000 V10 R0/ V10 R1 loadware has been updated manually before the RLC on host and APE then **NOIPBLWL** parameter setting is not needed.

- Open sysinfo on the active node

With sysinfo you can monitor the update process of all nodes.

https://<portal_ip_address>/sysinfo

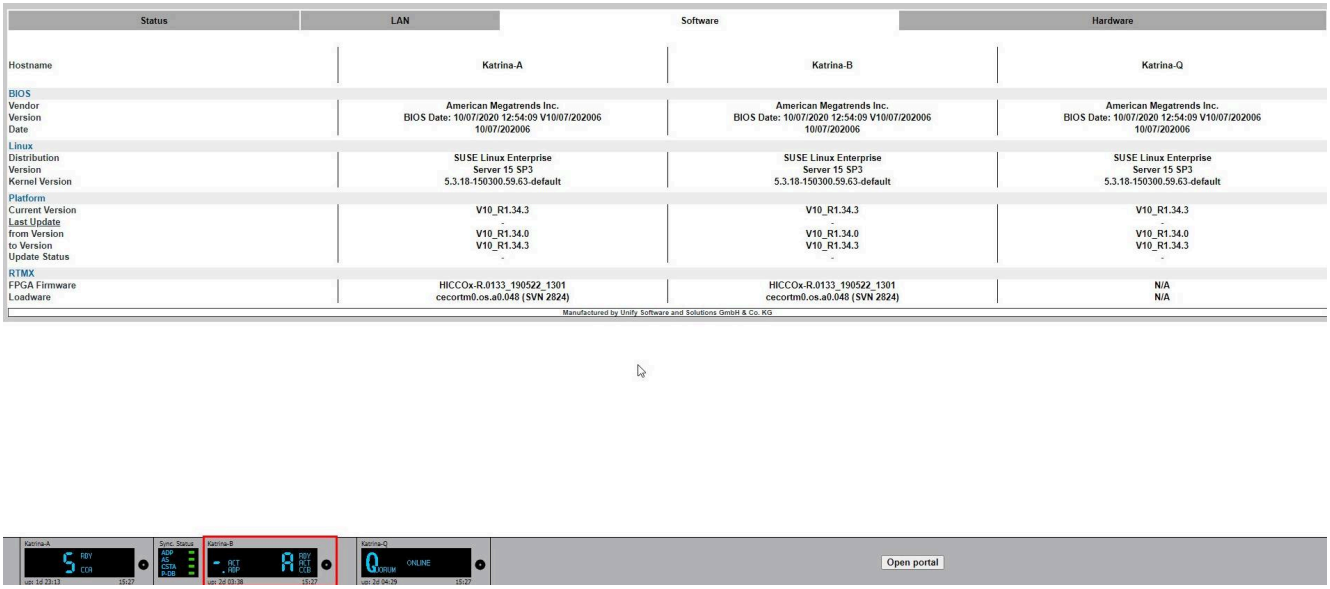


Figure 116: sysinfo

- All nodes of the system must be up and running.

  You can check this in sysinfo (see picture above) or in the front panel in the OpenScape 4000 Platform Administration (Portal).

  OpenScape 4000 Platform Administration (Portal) > System > Frontpanel

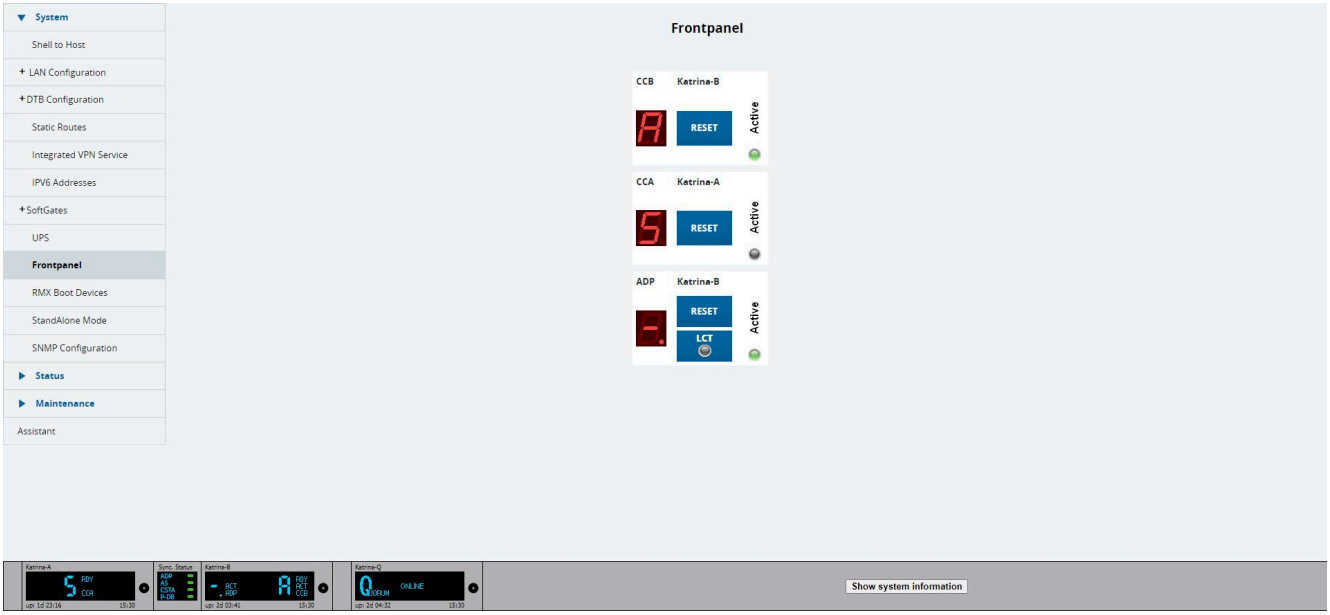


Figure 117: OpenScape 4000 Frontpanel

- OpenScape 4000 CCAPs/Survivable units must be synchronized before starting the update process.>

  The status of the host system and all CC APs/Survivable units can be checked in the OpenScape 4000 Assistant Backup & Restore

5.1.2 Preparation

1) **Check version of the OpenScape 4000 components (Platform, Assistant, etc.)**.

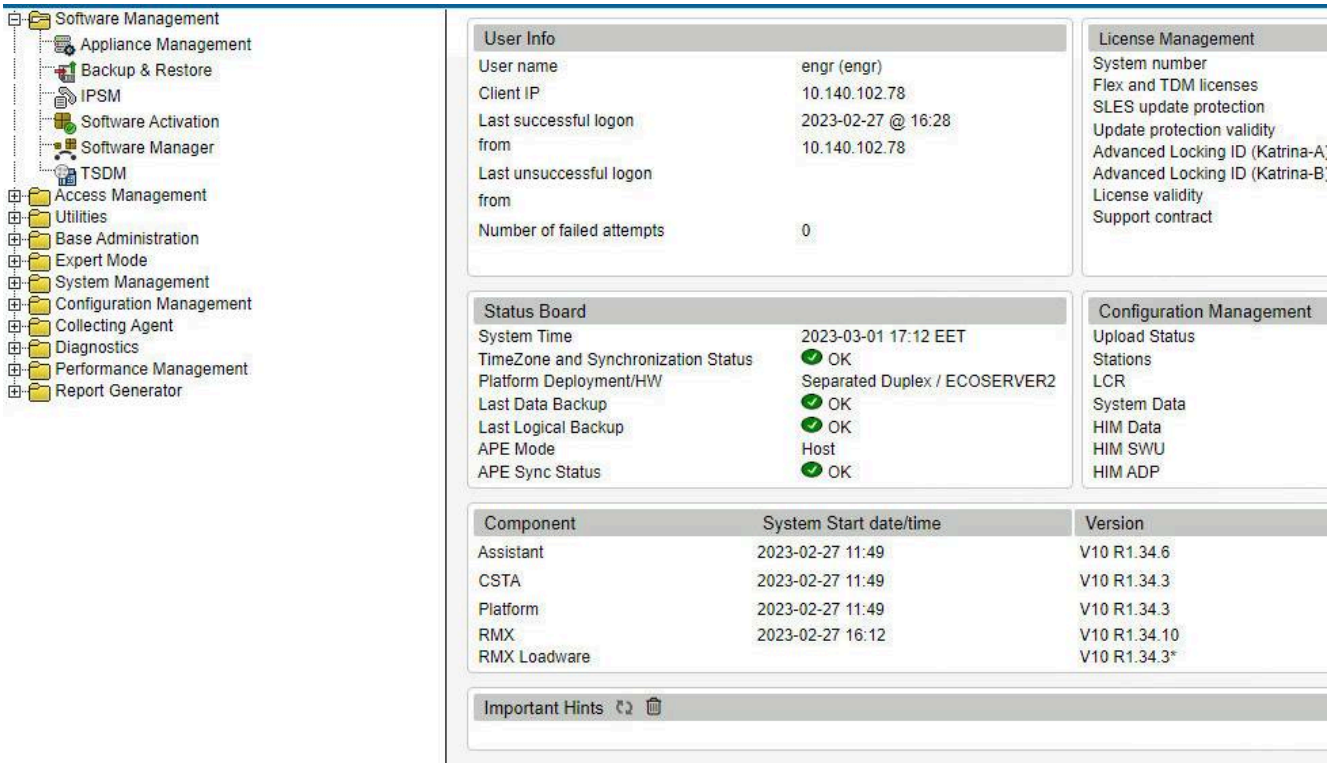


Figure 118: OpenScape 4000 Assistant start page

2) **Controlled Reboot for Survivable units**

Any Survivable units will automatically reboot during HBR (APE Restore) process.

This default behavior can be modified on the host..

Software Management > Backup & Restore > Configuration > Automatic OS Update Activation

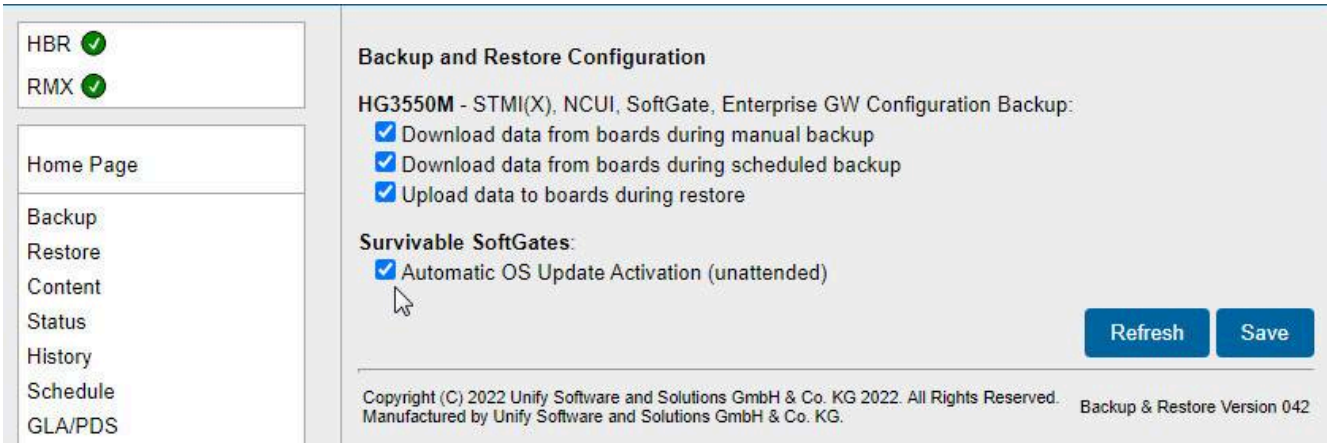


Figure 119: Survivable units - Disable automatic OS update activation

Perform an APE Backup to be sure that the setting on the Survivable unit.

In case of **Automatic OS Update Activation (unattended)** disabled (controlled) the operating system activation on the Survivable unit must be confirmed from the OpenScape 4000 SoftGate/ Enterprise GW WBM when the APE Restore process has reached the point when the system would make the activation reboot. This is displayed by the Software Activation. The menu inside the OpenScape 4000 SoftGate/ Enterprise GW WBM to be used for confirming the operating system update activation reboot is the following:

WBM: Maintenance > SW Update > OS Update > OS Update Actions > Activate OS Update

3) **Transfer the RLC package using OpenScape 4000 Assistant Software Manager**

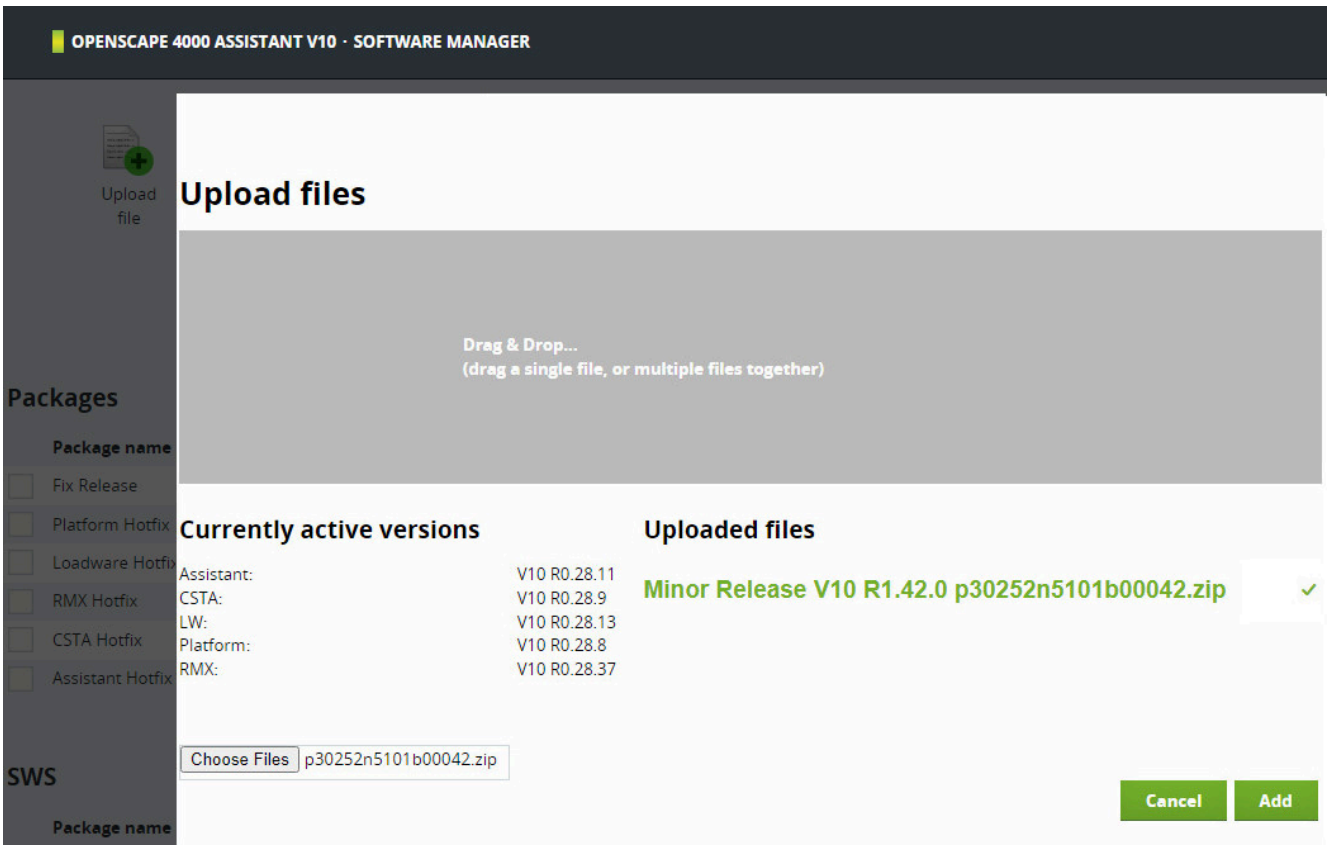


Figure 120: Add files for transfer

Select the RLC package (and Hotfixes) by navigating to Software Management > Software Manager > Upload file > Choose Files.

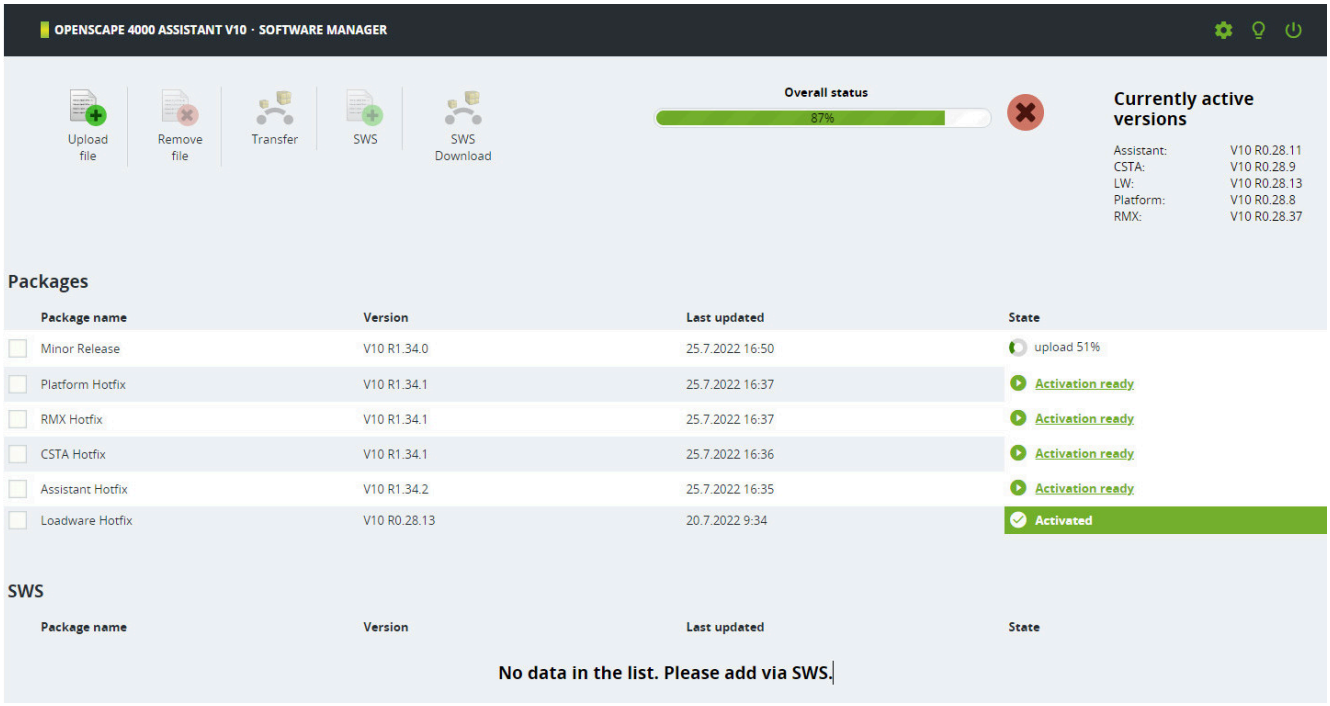


Figure 121: Transfer of RLC package

Once the transfer is completed, automatic RLC preparation will be triggered and if finished successfully, **Auto REGEN&GENDB** will start.

Preparation phase of the update has finished.

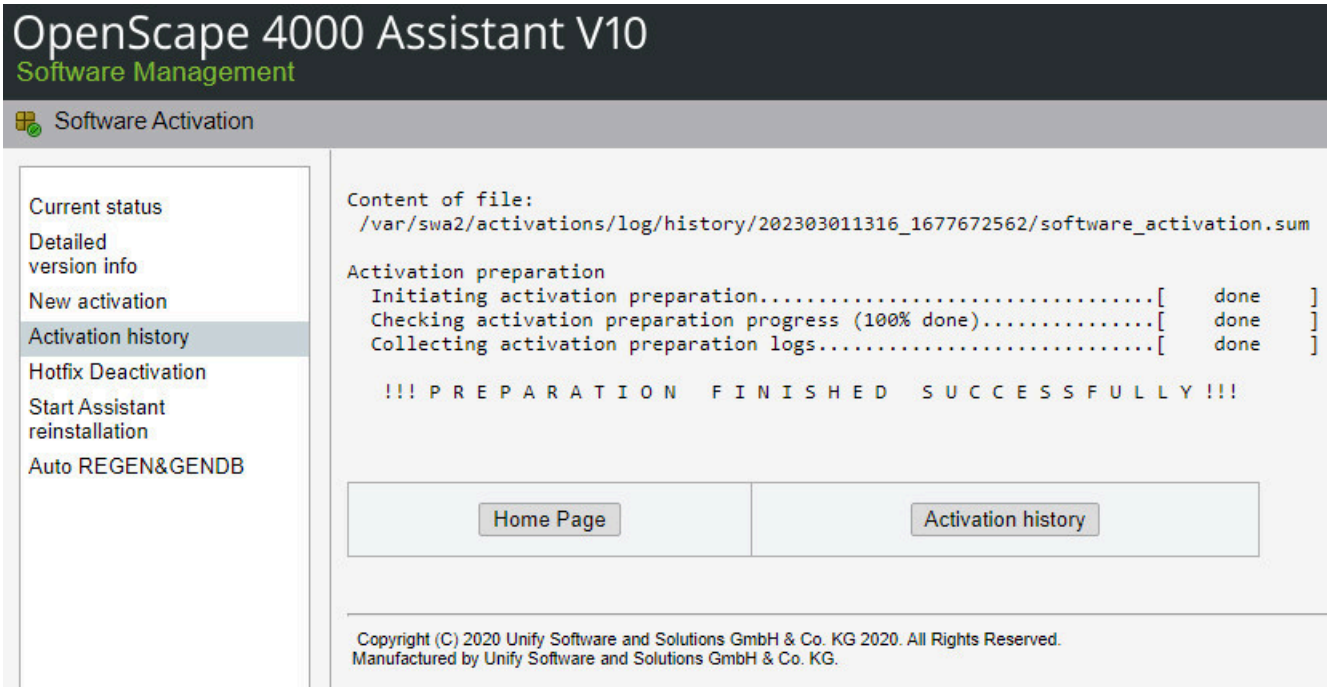


Figure 122: Details of RLC Preparation

4) **Check the activation status in OpenScape 4000 Assistant**

Software Activation > Activation history

Figure 123: Activation history and status of the activation

5) **Check the REGEN&GENDB status in OpenScape 4000 Assistant**

Software Activation > Auto REGEN&GENDB

See:

OpenScape 4000 Assistant / Manager V10, Software Activation, Administrator Documentation

6) **Optional: Open the Gateway Manager**

If you want to monitor the distribution of the loadware of the IP boards you can do this with the Gateway Manager in the OpenScape 4000 Assistant.

OpenScape 4000 Assistant > Expert Mode > Gateway Manager

Status of IP boards in the Gateway Manager before activation:

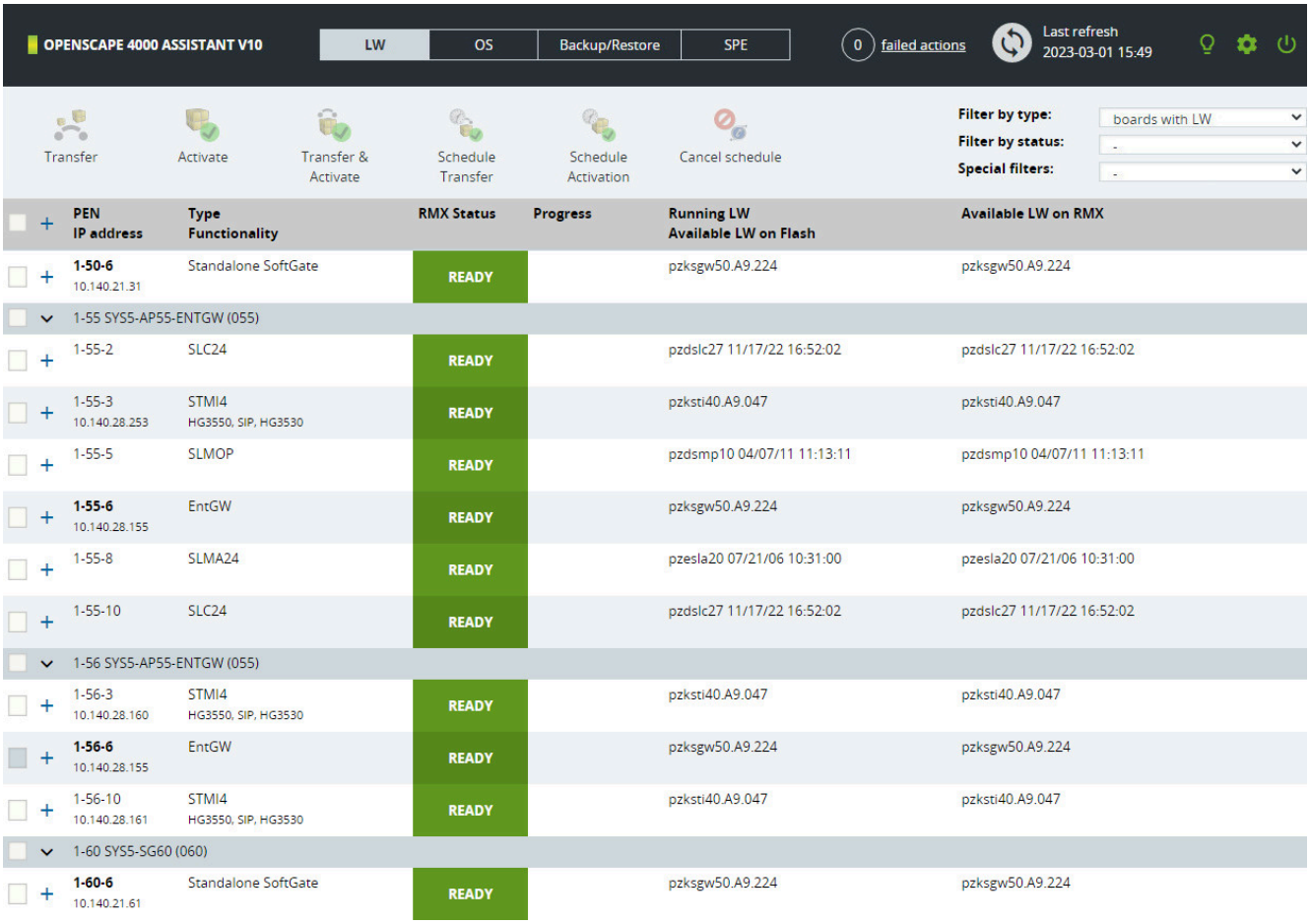


Figure 124: Status of IP boards

5.1.3 Activation

Start the activation phase:

OpenScape 4000 Assistant Software Management > Software Activation > New activation

Select the **Minor/Major Release OpenScape 4000 V10 R0.x/ V10 R1.x**.

To reduce the downtime of the system it is highly recommended to select the following **LW update options**:

- **Enable reduce downtime LW update during activation (enabled by default)**
- **Update SoftGate**

IMPORTANT: In case of upgrade from V8 R2/ V10 R0, to prevent the restart of the Standalone SoftGates, uncheck the "Activate the OS on Standalone SoftGate, STMIX, STMIY and Enterprise GW after Transfer" option before starting the RLC Activation. In this case, only OS transfer and preparation for OpenScape 4000 SoftGate, STMIX, STMIY and Enterprise GW are performed. The activation of the

OS should be done manually using **OS Update** tab in GW Manager.

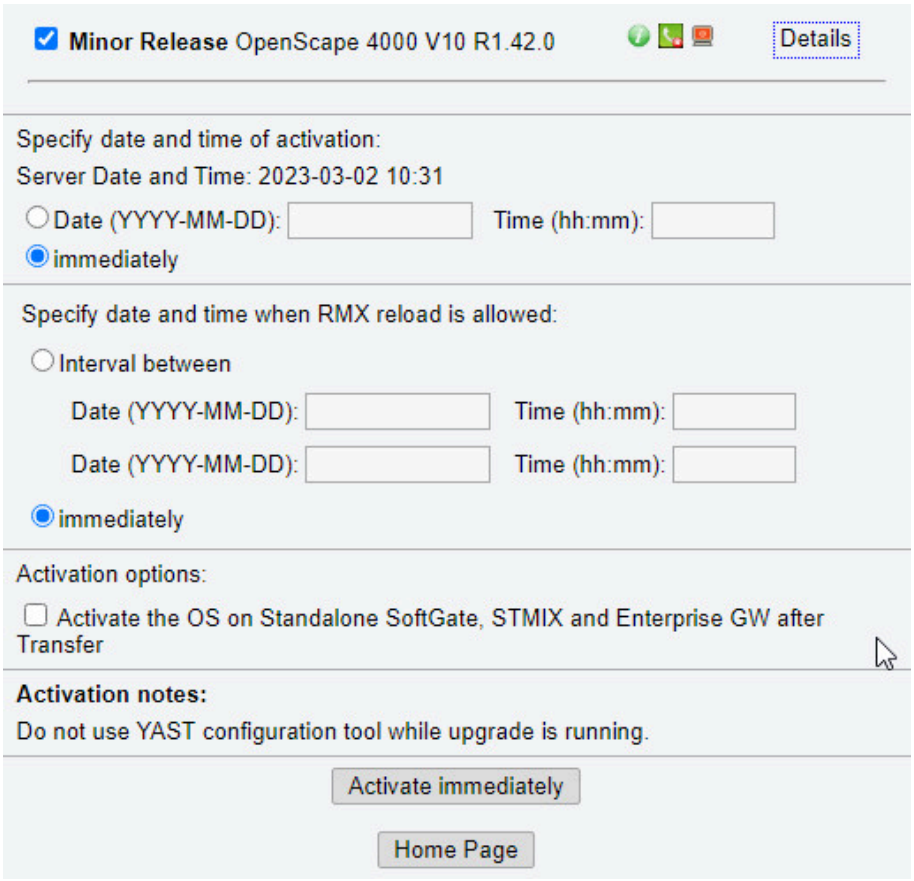


Figure 125: Activate standalone SoftGate

- **Continue with activation if LW activation fails (enabled by default)**

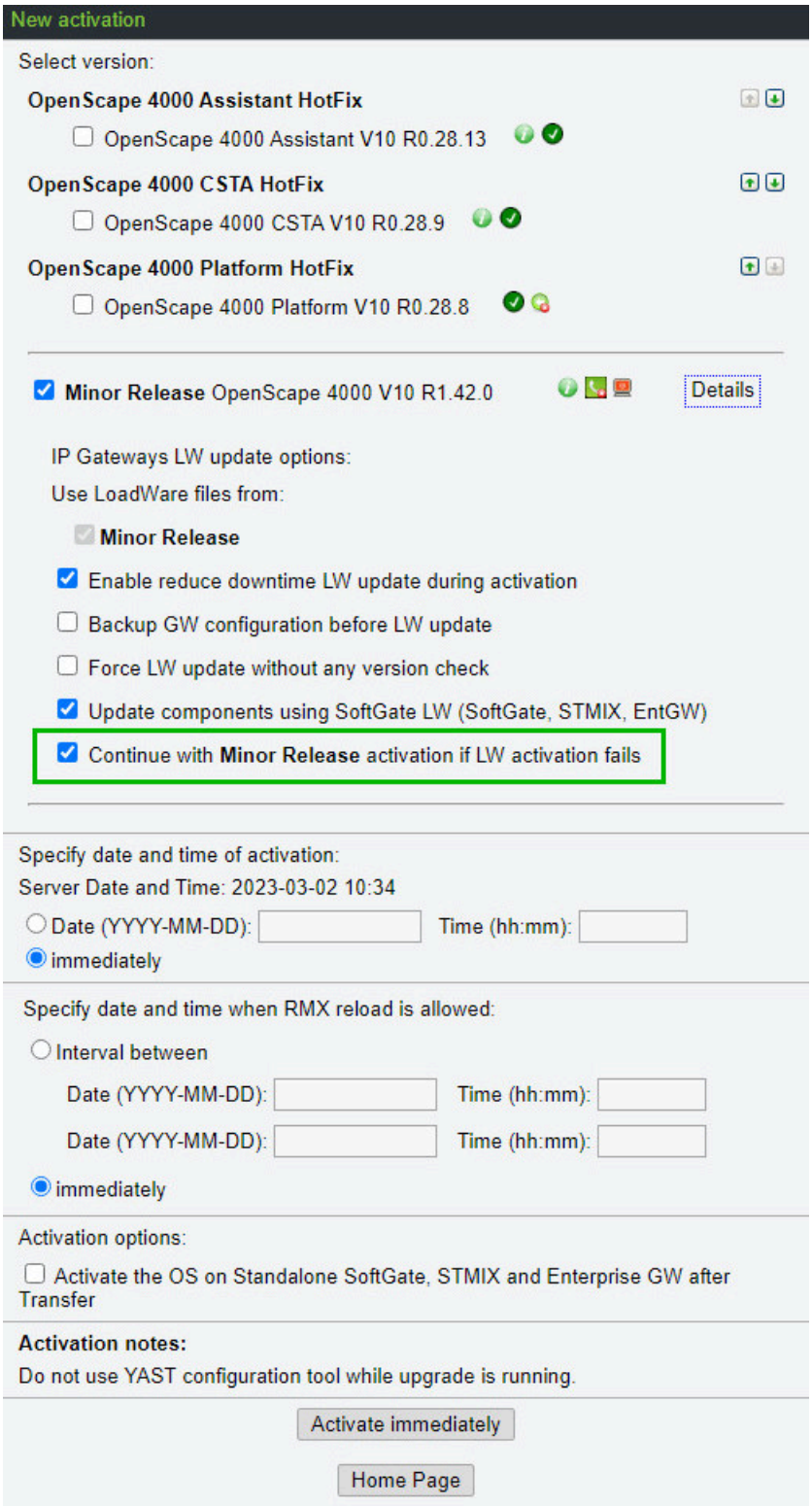


Figure 126: Activation of RLC package- start update

Click on **Activate immediately** to start the update process now.

An overview of all tasks that will be done during activation is shown.

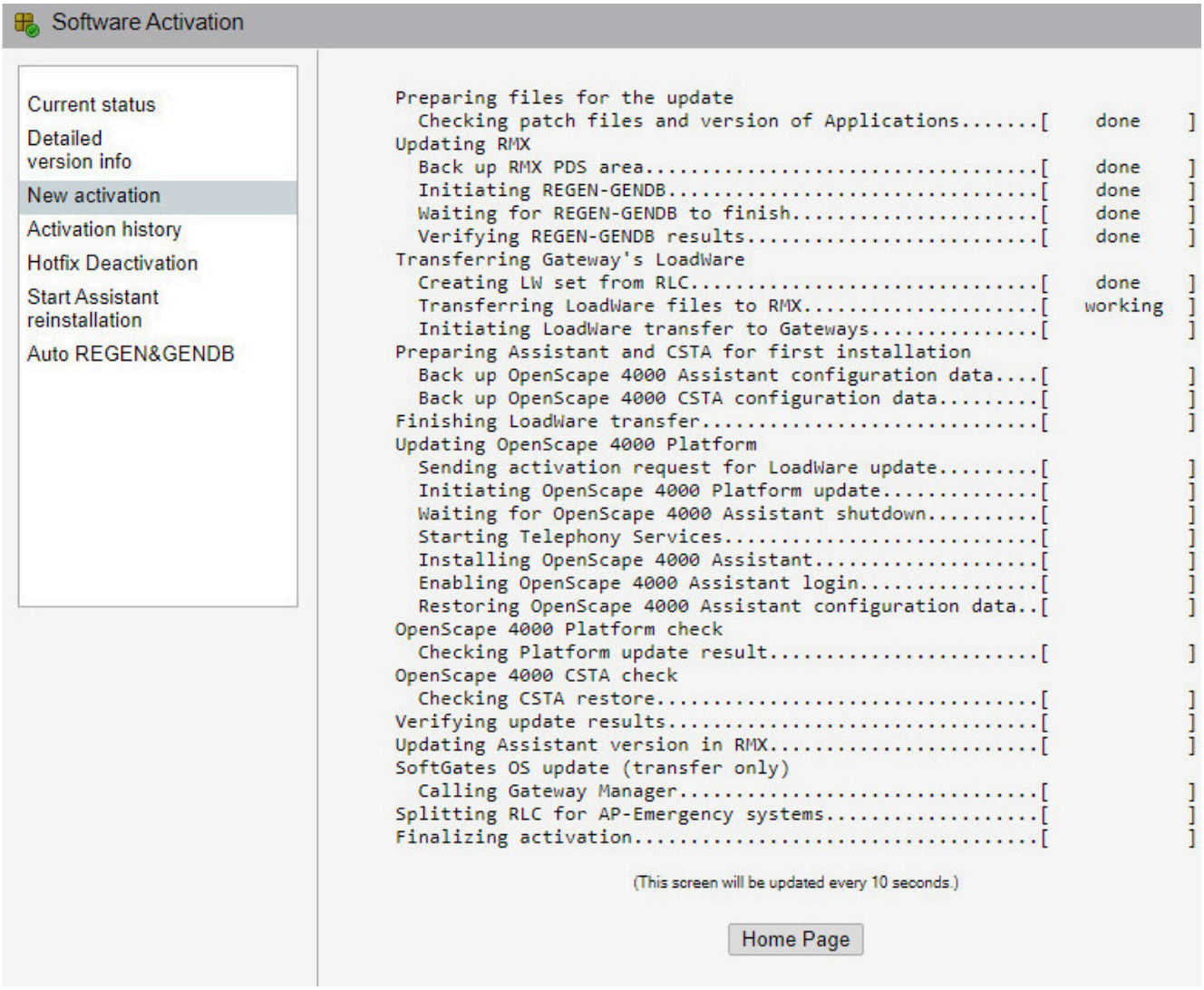


Figure 127: Tasks during update

You can monitor most of the tasks in the OpenScape 4000 Assistant.

E.g: Loadware update in **Gateway Manager**.

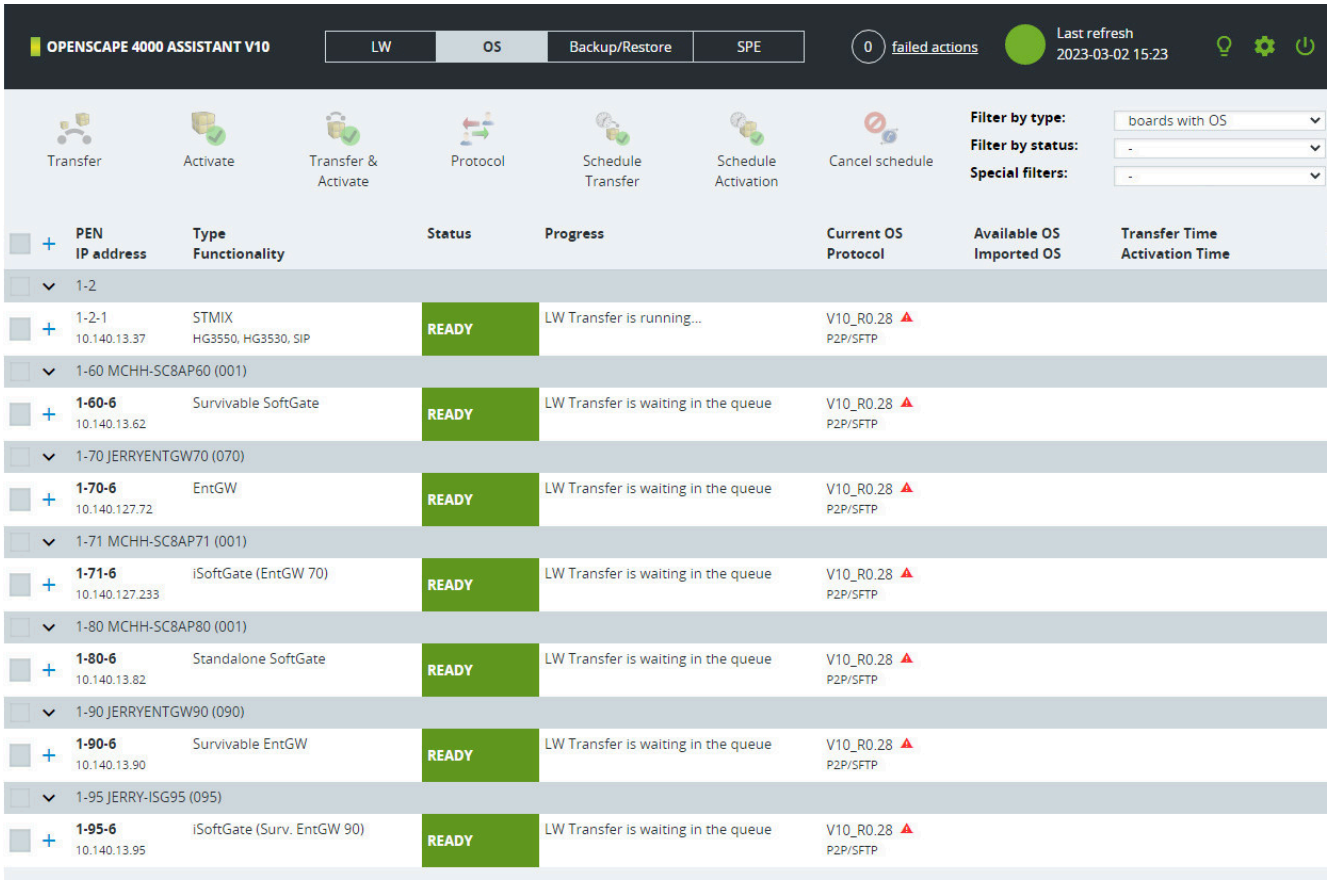


Figure 128: Loadware transfer during update

or the progress of the Backup of OpenScape 4000 Assistant in **Backup & Restore**.

Figure 129: Backup of OpenScape Assistant during update

Also on the OpenScape 4000 Assistant start page, you can see that the update in general takes place (see **Important Hints**) and that at the moment a logical backup is running.

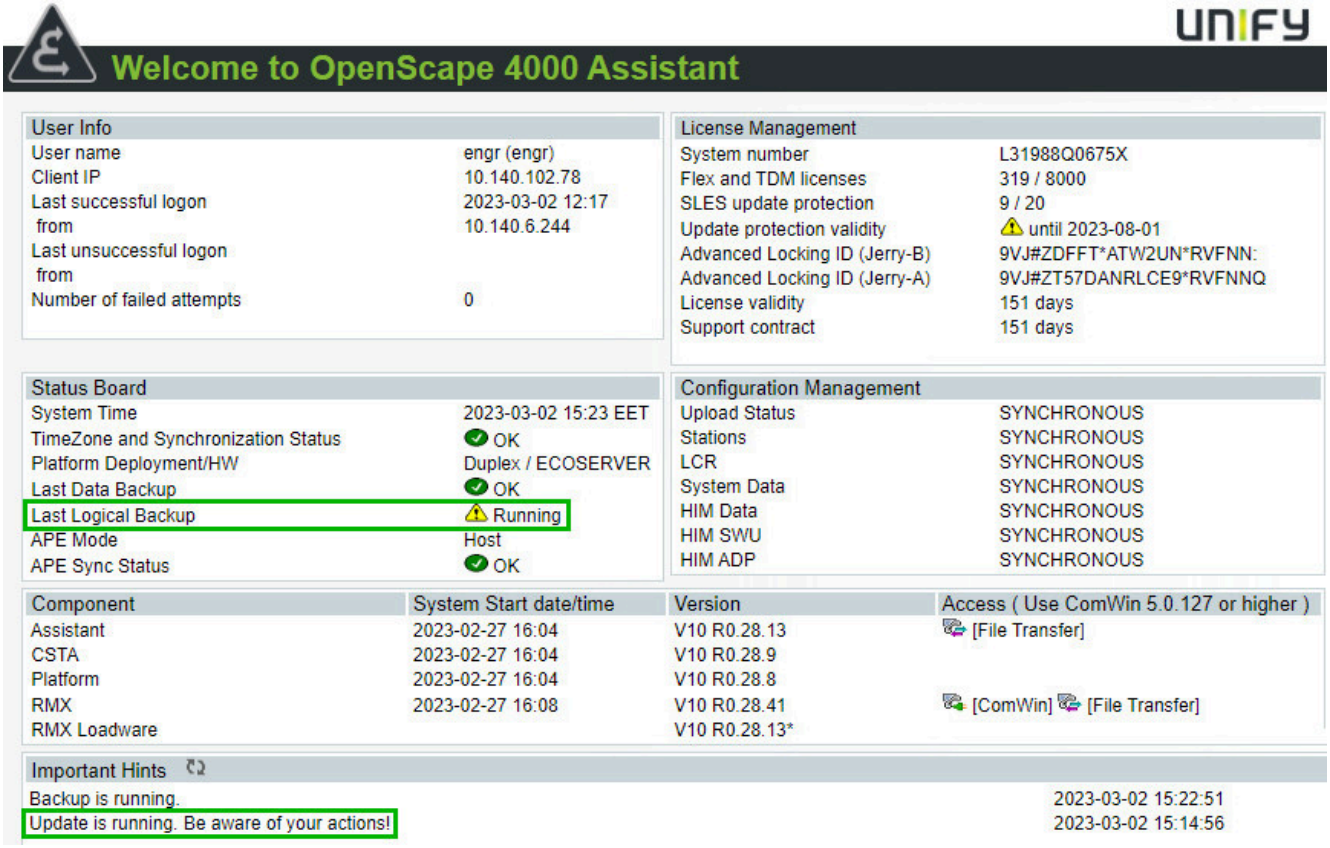


Figure 130: Monitoring the update

In the **Software Activation** in the menu **Current status** you can see what activation has been currently started.

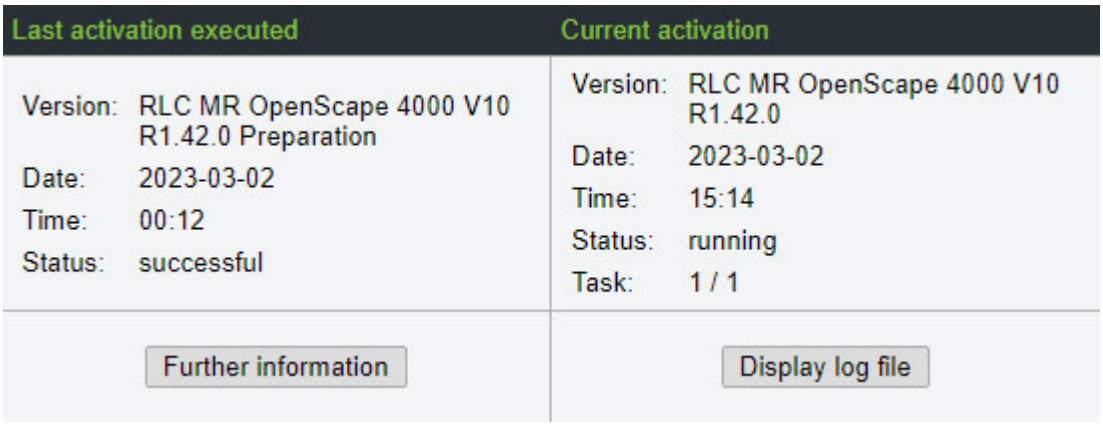


Figure 131: Software Activation > Current status

When the loadware transfer has finished, all IP board loadware has been transferred to the flash memory of the board.

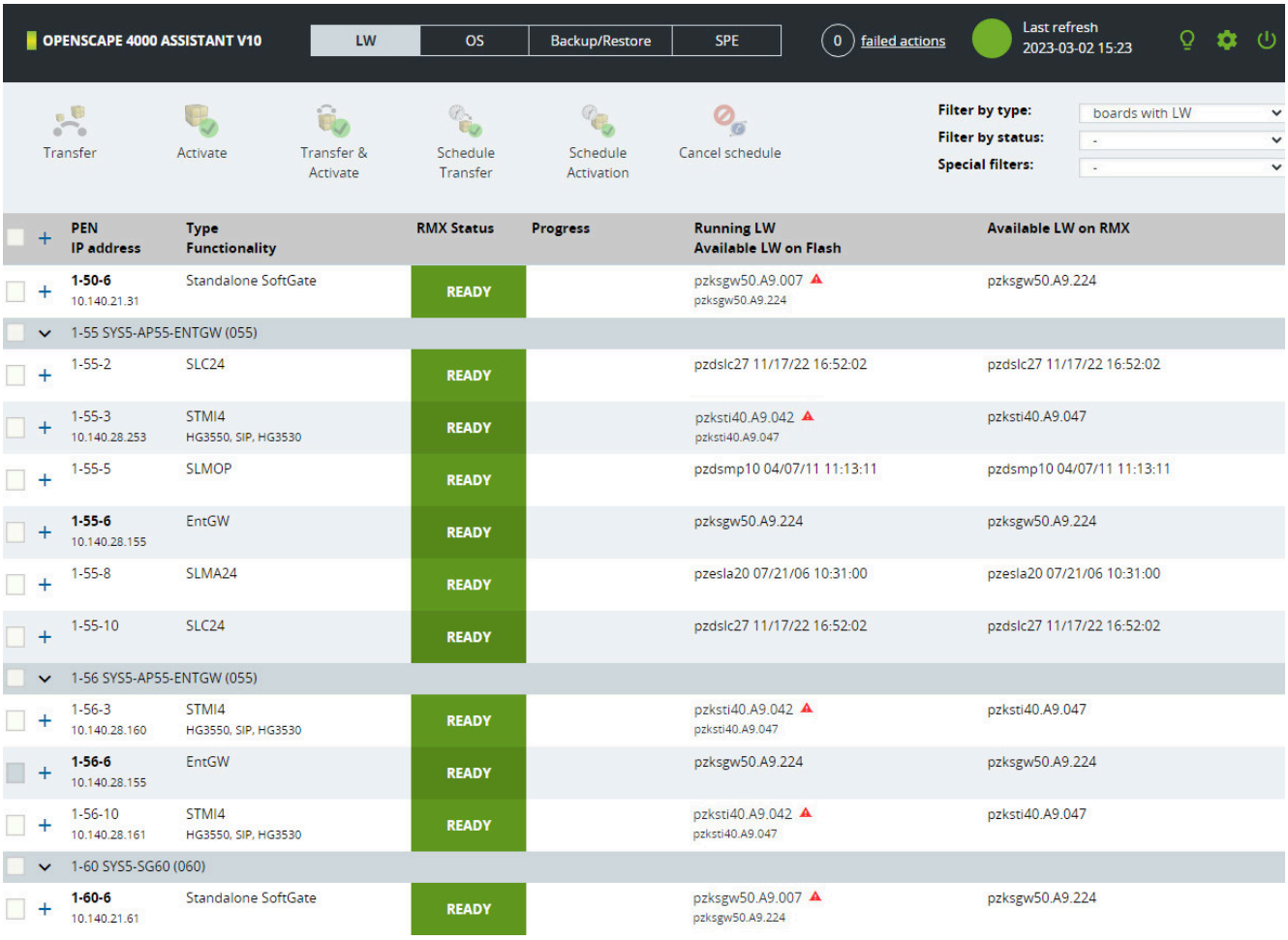


Figure 132: Loadware transfer has finished

Between the tasks **Waiting for OpenScape 4000 Assistant shutdown** and **Starting Telephony Services** the telephony is down. The loadware is now updated shelf by shelf and all services and applications will be stopped.

IMPORTANT: The phones should be configured to switch to emergency mode now.

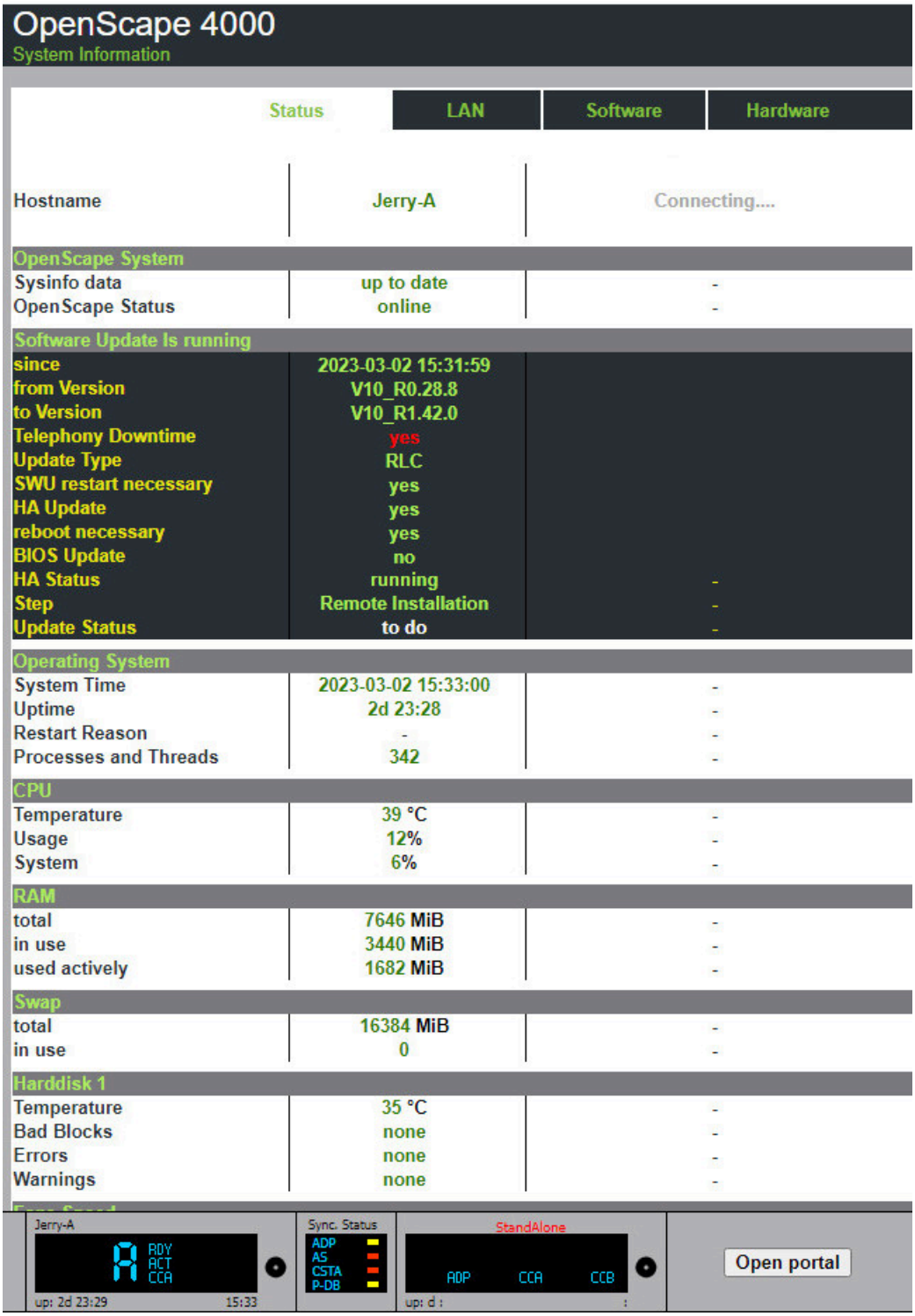


Figure 133: sysinfo - All services have been stopped (Duplex)

After some reboots the OpenScape 4000 Assistant installation will start, followed by a logical restore. Telephony is running again. Waiting for RLC activation to be completed.

The duration of the update can be seen in the detailed log file in the OpenScape 4000 Assistant:

Software Activation > Current status

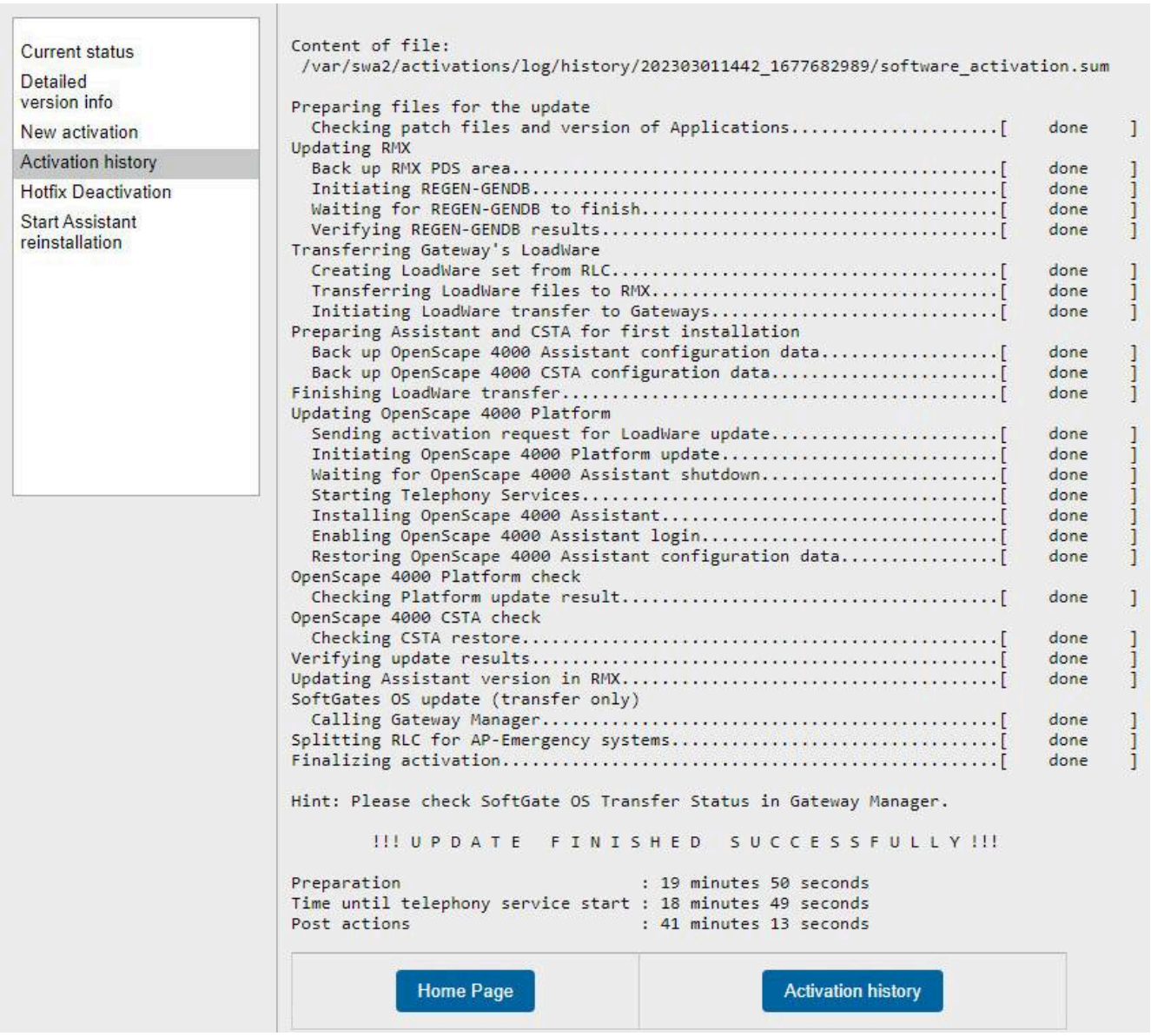


Figure 134: Software Activation - Duration of the update

IMPORTANT: After first AP backup on host and after CC-AP's AP restores, the following commands must be executed:

```
CHANGE-ZANDE:TYPE=ALLDATA2,NOIPBLWL=NO;
EXEC-UPDAT:UNIT=BP,SUSY=DELTA;
```

IMPORTANT: When upgrading from OpenScape 4000 V8, the system will run under grace period license. The system will require a new V10 license. For more information about the V10 license generation procedure, see the Licensing on page 189 chapter.

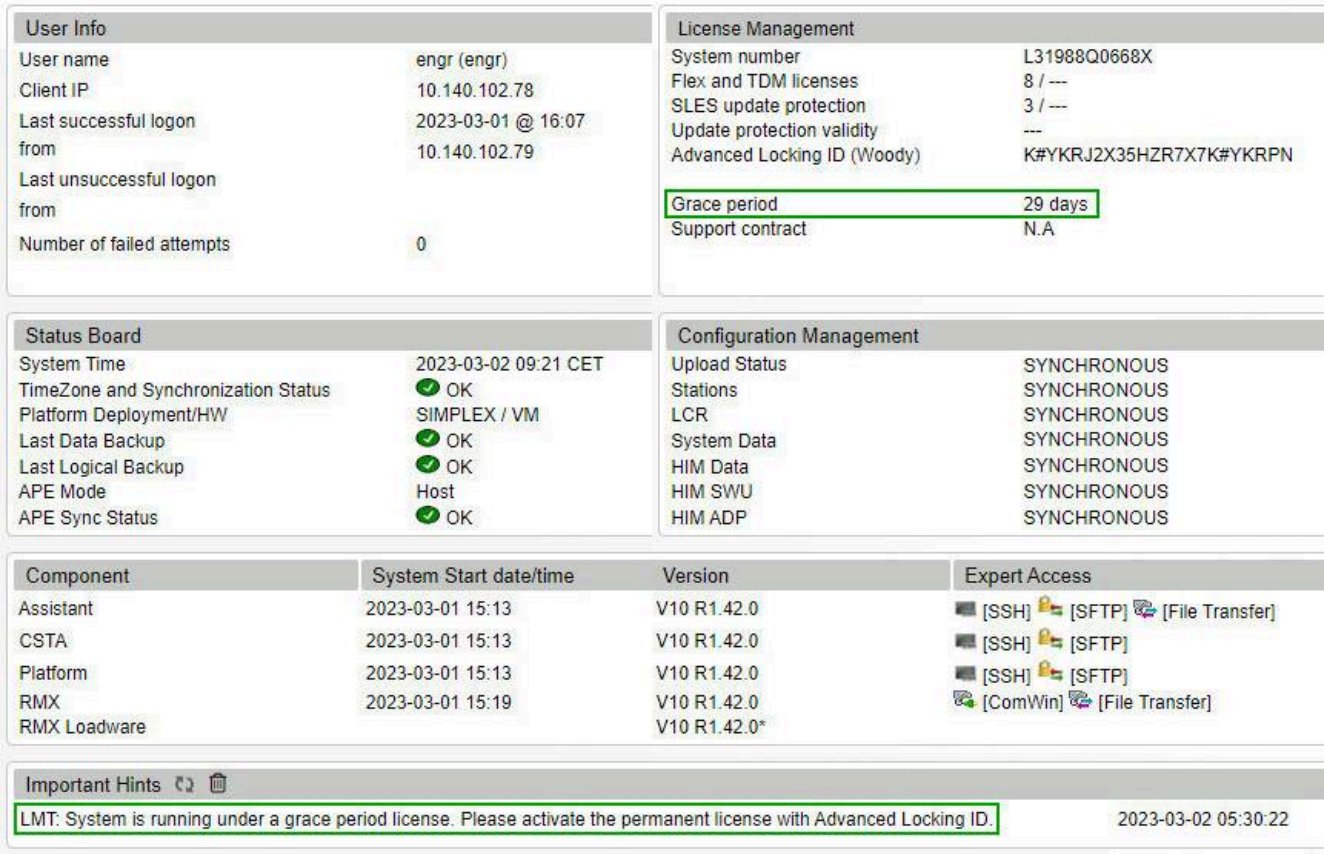


Figure 135: System under grace period license

5.1.3.1 APE and Survivable units Update

After the host has been updated an APE Backup must be initiated for the APEs.

In case of **Automatic OS Update Activation (unattended)** is disabled (controlled) the operating system activation on the Survivable units must be confirmed from the SoftGate/Enterprise GW WBM when the APE restore process has reached the point when the system would make the activation reboot (see **Software Activation > Current status**).

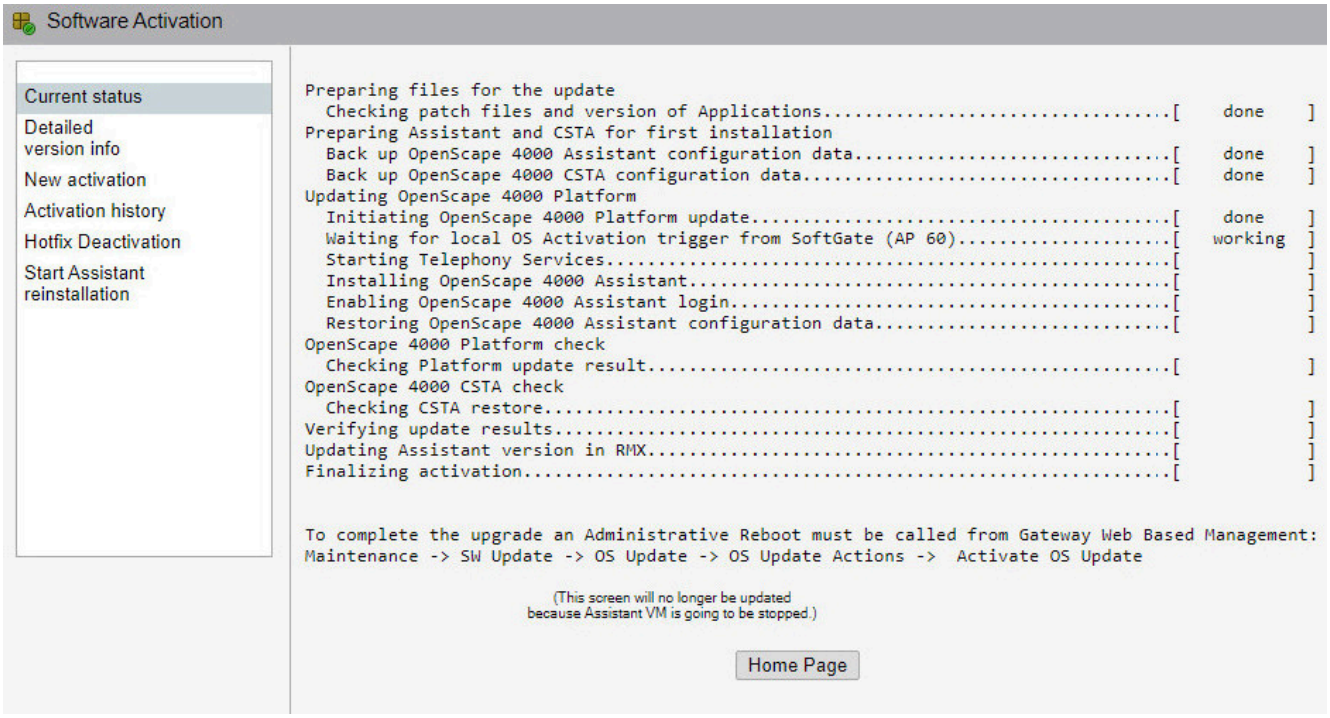


Figure 136: Software Activation - Waiting for reboot of Survivable OpenScape 4000 SoftGate

The menu inside the SoftGate/Enterprise GW WBM to be used for confirming the operating system update activation reboot is the following:

WBM > Maintenance > SW Update > OS Update > OS Update Actions > Activate OS Update

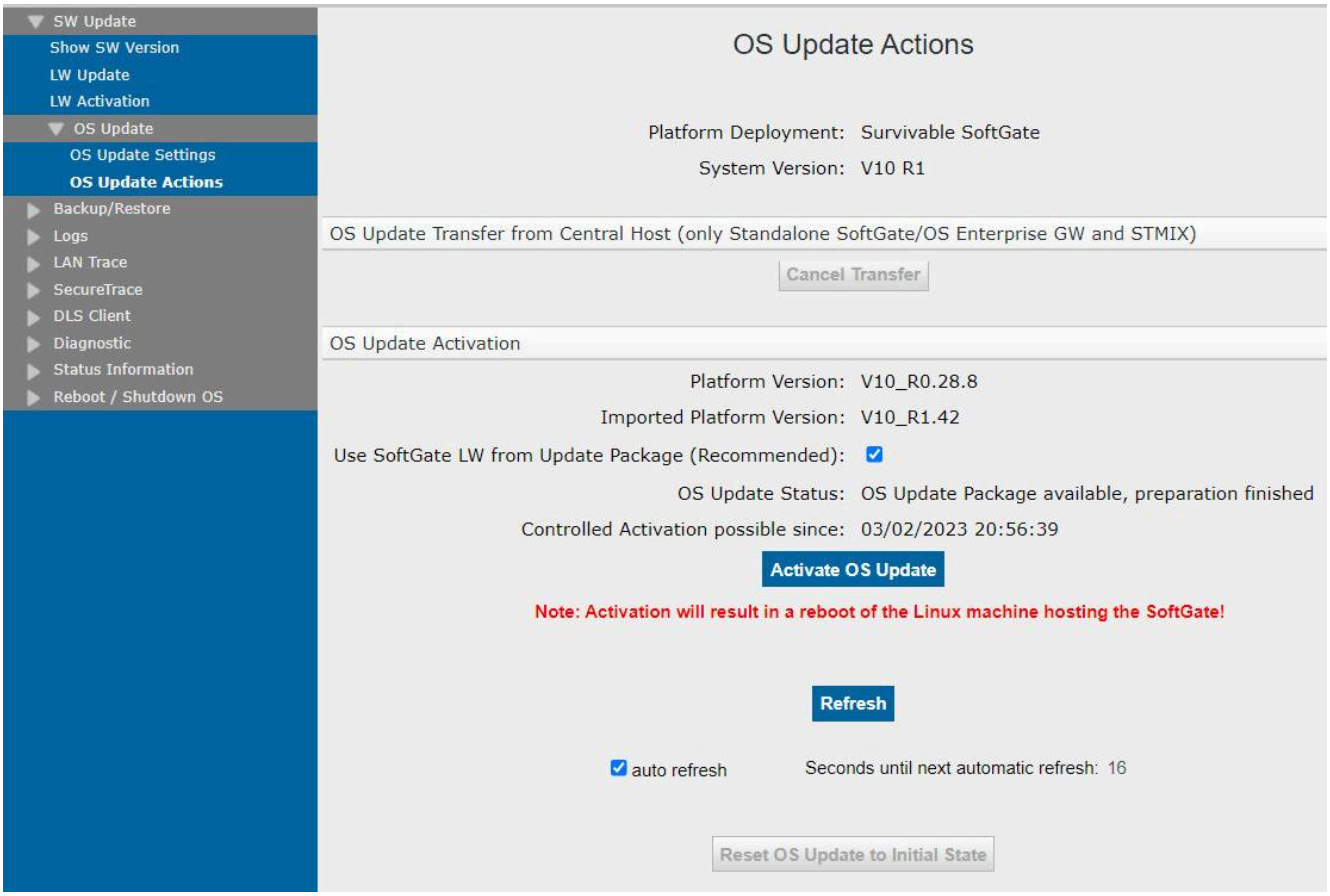


Figure 137: WBM - Operating system update for Survivable units

After rebooting the Survivable unit, the RLC activation continues. The final status can be checked on the WBM and OpenScape 4000 Assistant.

WBM: **Maintenance > SW Update > Show SW Version**

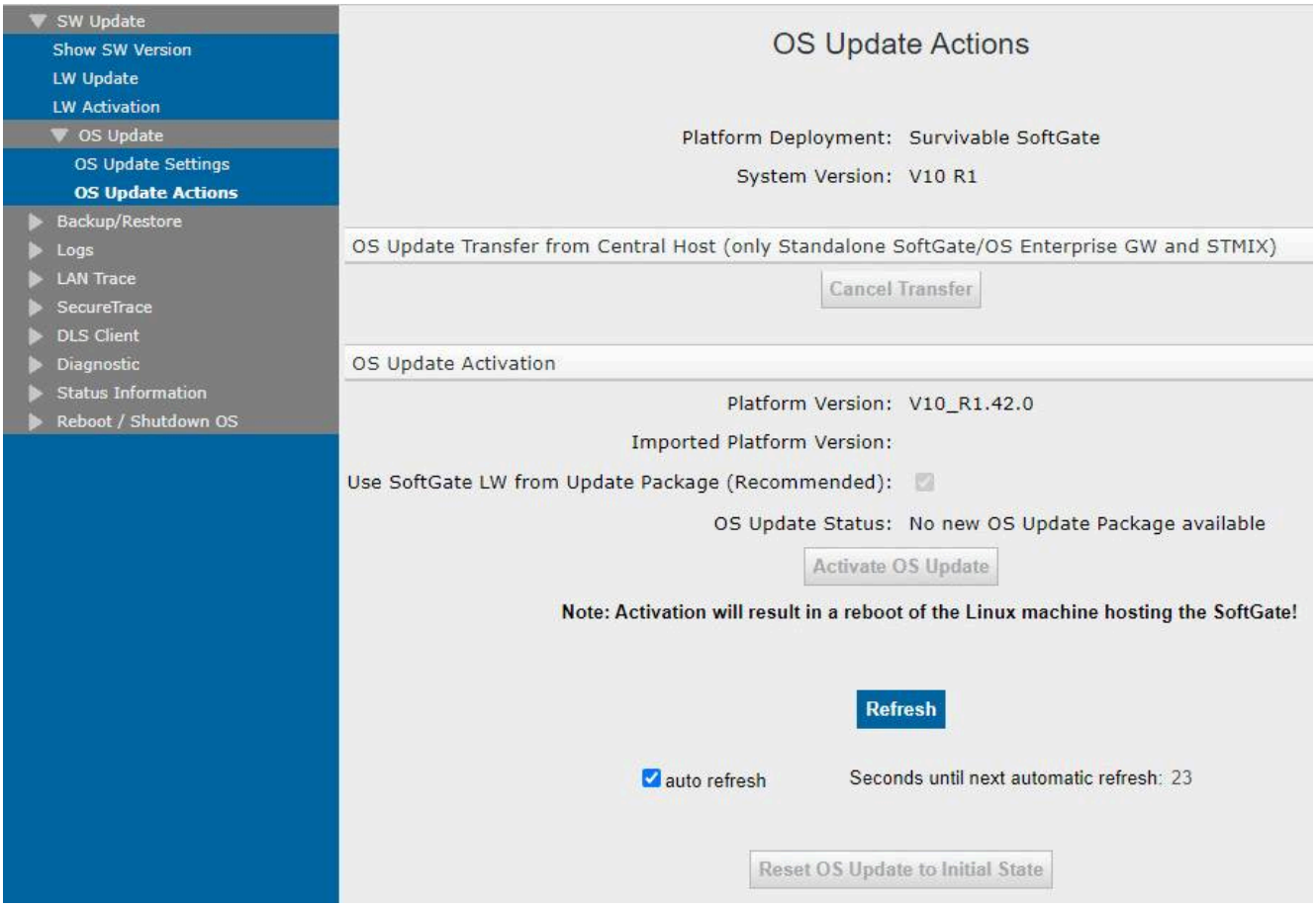


Figure 138: WBM - Software version after update

OpenScape 4000 Assistant: **Software Activation** > **Activation history**

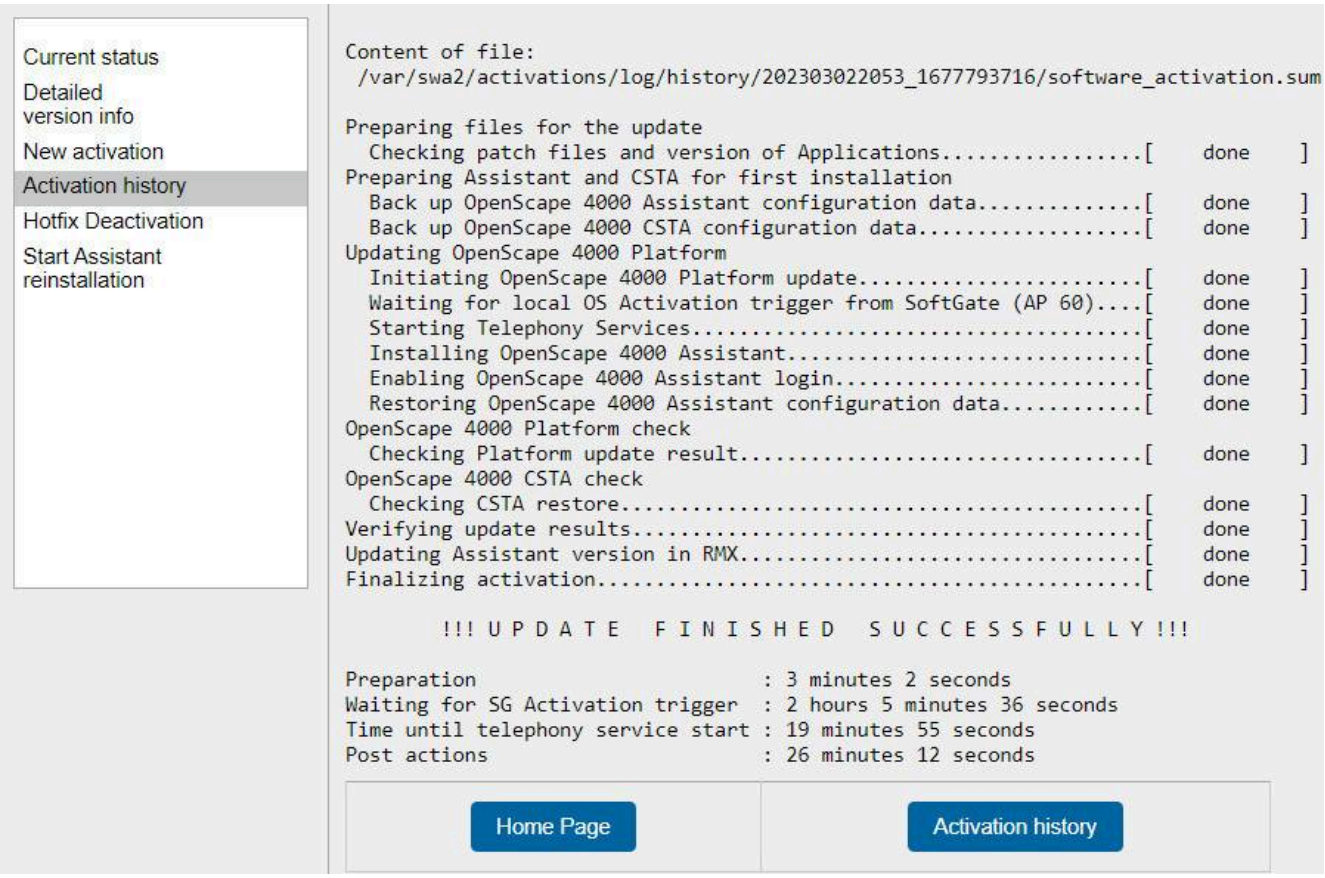


Figure 139: OpenScape 4000 Assistant - Software version after update

5.1.3.2 Standalone SoftGate, STMIX, STMIY and Enterprise GW update

The operating system activation on the Standalone SoftGate, STMIX, STMIY and/or Enterprise GW must be confirmed from the OpenScape 4000 Assistant:

Expert Mode -> Gateway Manager -> OS tab -> Transfer & Activate

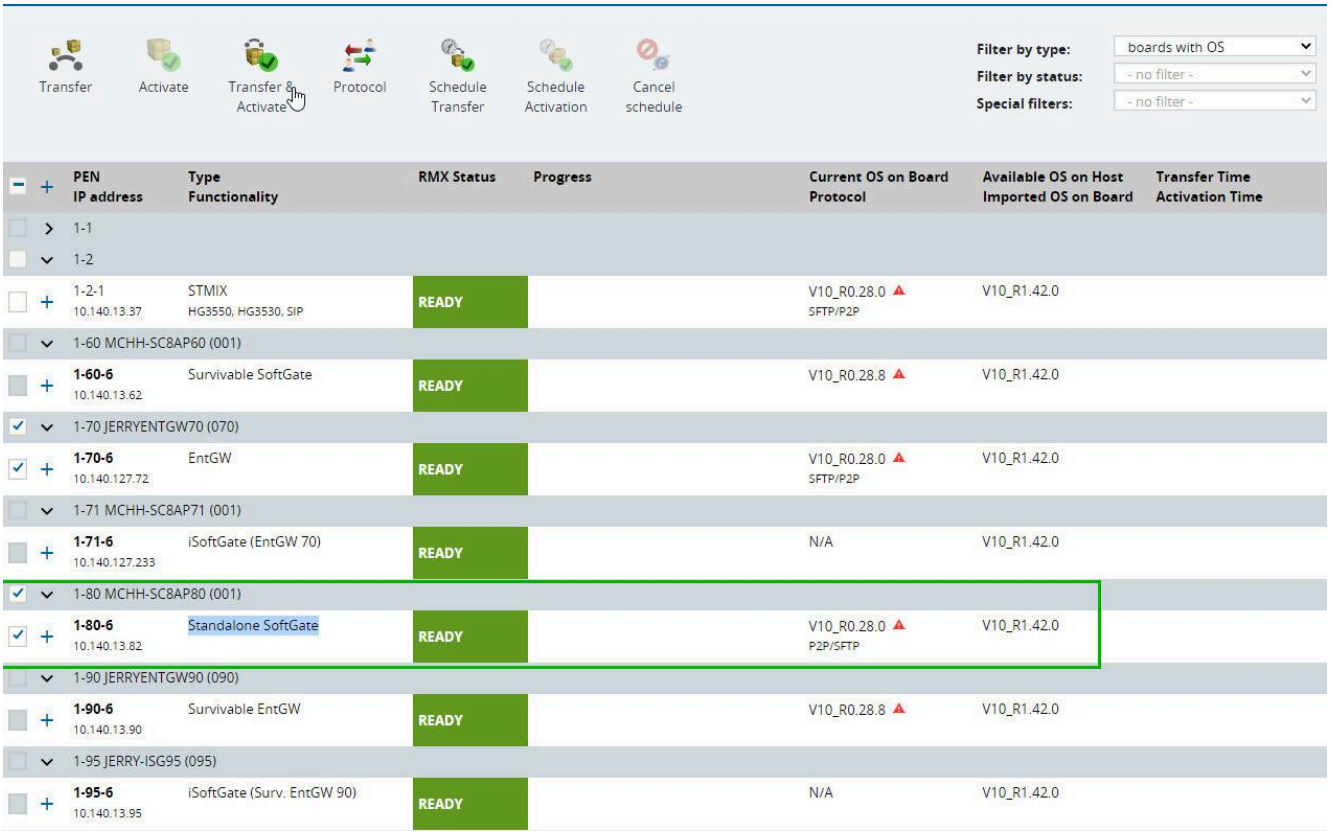


Figure 140: Activate SG OS GW Manager

After the reboot of the Standalone SoftGate, STMIX, STMIY and/or Enterprise GW, the new operating system will become active.

5.2 Reduced Downtime for Loadware Hotfixes

The feature can be utilized during the upgrading process.

Software Update Packages (RLC) contain new LoadWare files, which can be activated via the "reduce downtime" feature.

Loadware (LW) Hotfixes can be released while the RLC is about to be activated.

In such situations service had to activate the RLC package and the Loadware (LW) Hotfix, which means double telephony downtime. This feature allows the merging of both updates.

You can transfer the RLC and LW HF together via Software Manager and activate them.

The OpenScape 4000 Assistant uses the LoadWare (LW) Hotfix with newer content rather than Loadwares from the RLC. This way, only one downtime is needed. The difference between this update scenario and the previous one is that the Loadware HotFix is not displayed in the Software Activation GUI.

- Transfer LoadWare Hotfix to the OpenScape 4000 Assistant.
- Transfer the Minor/Fix Release (RLC).
- Activate Minor/Fix Release

6 Changing Platform Configuration

6.1 Important Information

This document should be used for a system that has been already installed and now some IP addresses/interfaces must be changed.

All IP address configuration changes should be made using the **Recovery/ Reconfiguration Tool**.

OpenScape 4000 Platform Administration (Portal)

There is still the possibility to use the OpenScape 4000 Platform Administration (Portal) for IP address changes but only if the new IP address is in the same IP subnet as the old one. Changing the IP address using the OpenScape 4000 Platform Administration (Portal) will not cause telephony downtime if the new IP address is in the same IP subnet as the old one. (exception: IPDA Network IP address change, see Section 6.4.2, "IPDA Network IP Address Change".

Examples of changes that do not cause telephony downtime when using OpenScape 4000 Platform Administration (Portal):

- Change the IP address of OpenScape 4000 Platform Administration (Portal) (old and new IP address are in the same subnet)
- Change the IP address of OpenScape 4000 Assistant (old and new IP address are in the same subnet)
- Change the IP address of OpenScape 4000 CSTA (old and new IP address are in the same subnet).
- Atlantic interface (if the target interface is already configured with IP 0.0.0.0/0)

Recovery/Reconfiguration Tool

The Recovery/Reconfiguration Tool must be used if the new IP addresses that will be assigned are from a different subnet than the old ones or if new interfaces need to be configured.

IMPORTANT: Please be aware that using the Recovery/ Reconfiguration Tool causes a telephony downtime (like a normal system reload), regardless on the changes that are made on the nodes.

For more information on the Recovery/Reconfiguration Tool please refer to Section 6.3, "Recovery/Reconfiguration Tool".

First installation script called with -s option

Script called with the option **-s** and a second parameter makes only the following configurations from the XML file, without removing/reinstalling the network configuration.

Table 34: firstinst-netw.sh, option -s

./firstinst-netw.sh **-s keyboard**	--> Configures only the keyboard layout
./firstinst-netw.sh **-s timezone**	--> Configures only the timezone
./firstinst-netw.sh **-s dns**	--> Configures only the DNS server(s)
./firstinst-netw.sh **-s ntp**	--> Configures only the NTP server(s)
./firstinst-netw.sh **-s all**	--> Configures only the 4 parameters above

Any existing configuration will be replaced with the values from the XML file, which corresponds to the server.

IMPORTANT: If DNS entries are changed directly via YAST, all IP interfaces will be restarted causing an outage to the system!

6.2 Using OpenScape 4000 Platform Administration (Portal)

6.2.1 Customer LAN IP Address Change

6.2.1.1 OpenScape 4000 Platform Administration (Portal)

For changing the IP address of the OpenScape 4000 Platform Administration (Portal) open the **OpenScape 4000 Platform Administration (Portal) > System > LAN Configuration** and replace the existing IP address with the new IP address in the field **IP Address of Portal**.

Then press **Next** and **Submit**.

6.2.1.2 OpenScape 4000 Assistant IP Address Change

For changing the OpenScape 4000 Assistant IP address open the **OpenScape 4000 Platform Administration (Portal) > System > LAN Configuration > System** and replace the existing OpenScape 4000 Assistant IP address with the new one.

Then press **Next** and **Submit**.

6.2.1.3 OpenScape 4000 CSTA IP Address Change

For changing the OpenScape 4000 CSTA IP address open the **OpenScape 4000 Platform Administration (Portal) > System > LAN Configuration >**

System and replace the existing OpenScape 4000 CSTA IP address with the new one.

Then press **Next** and **Submit**.

6.2.2 Atlantic Interface Change

NOTICE: Atlantic interface can be changed without telephony downtime only if the target interface is already configured with IP 0.0.0.0/0.

Open the **OpenScape 4000 Platform Administration (Portal) > System > LAN Configuration > System** and replace the existing Atlantic interface with the new one.

Then press **Next** and **Submit**.

6.2.3 OpenScape 4000 SoftGate IP Address Change

NOTICE: This section is valid for all deployments with OpenScape 4000 SoftGate.

Open the **OpenScape 4000 Platform Administration (Portal) > System > LAN Configuration** page and update the data accordingly.

NOTICE: The changes performed this way apply only to the local server (SoftGate). Of course, changing an access point IP address means that also the host system has to be reconfigured accordingly – please see the IPDA section in OpenScape 4000 V10, Volume 4: IP Solutions, Service Documentation.

6.3 Recovery/Reconfiguration Tool

IMPORTANT: Please be aware that using the Recovery/Reconfiguration Tool causes a telephony downtime (like a normal system reload), regardless on the changes that are made on the nodes.

With the Recovery/Reconfiguration Tool you can recover or reconfigure an already installed OpenScape 4000 system. It deals with every deployment.

The Recovery/Reconfiguration Tool uses the script **recover-H4K.sh** that is included in the directory `/opt/soco-common`.

The following two scripts are also necessary for the tool in order to work properly:

- `/opt/soco-common/firstinst-netw.sh` with a version minimum V1.66.

- The version of this script can be get with the command `firstinst-netw.sh -v`.
- `/opt/ha/bin/mount_drbd_partitions.sh`

> **NOTICE:** The recovery script will exit with an error message if these two scripts are not available or don't have the appropriate versions.

The script **recover-H4K.sh** uses the XML file that has been already used for installing the system (for more information see Section 10.3, "XML Configuration File").

The XML source file can be an existing file or a newly generated file when running the script. Then it contains the current node configuration. Updating the XML file can be done during the execution of the Recovery/Reconfiguration Tool using "vi".

During recovery/reconfiguration all network parameters will be deleted and installed new according to the XML file. Then the OpenScape 4000 will be started again.

Scenarios

- **Recovery**
- If the node crashes or is running in an undefined/incorrect state.

> **IMPORTANT:** In case of **recovery** the Recovery/ Reconfiguration Tool should be executed **only on the affected node**.

- **Reconfiguration**
- In the case that you need to change some parameters.

> **IMPORTANT:** In case of **reconfiguration** the Recovery/ Reconfiguration Tool needs to be executed on **all nodes** (e.g. in Separated Duplex deployments the Recovery/ Reconfiguration Tool needs to be executed on Quorum, standby node and active node).

6.3.1 Prerequisites on the System

The script automatically knows for which situations a stop of telephony services is necessary and will prompt the user for a confirmation before completing the action:

Figure 141: Stop services message

The recommend order for reconfiguration on multi node systems using the recovery tool is:

- Duplex Nodes

Current standby node (where ADP/OpenScape 4000 Administration Platform (Portal)/OpenScape 4000 Assistant/OpenScape 4000 CSTA are not running).

Current active node

- Separated Duplex Nodes

Quorum node

Current standby node (where ADP/OpenScape 4000 Administration Platform (Portal)/OpenScape 4000 Assistant/OpenScape 4000 CSTA are not running)

Current active node

For simplex node systems (including Simplex with Integrated OpenScape 4000 SoftGate/Survivable OpenScape 4000 SoftGate/APE/OpenScape 4000 SoftGate) there is no reconfiguration order possible because of only one node.

6.3.2 Script Execution

6.3.2.1 Common Execution Steps

Change to the directory `/opt/soco-common` and call the script **recover-H4K.sh**.

cd /opt/soco-common

./recover-H4K.sh

The script looks into the configuration directory **/var/opt/firstinstall** to find the XML file **firstinst-netw-XXXXX.xml** with a corresponding Mac address for the node.

If the script finds more than one XML file with a corresponding Mac address,the user gets a list of these files and must choose one of them for configuring the node. The other files will be moved into the directory `/var/opt/firstinstall/tmp`.

With the option **Create from server** it is possible to automatically create a XML file. In this case, all listed files will be moved into the directory `/var/opt/firstinstall/tmp`.

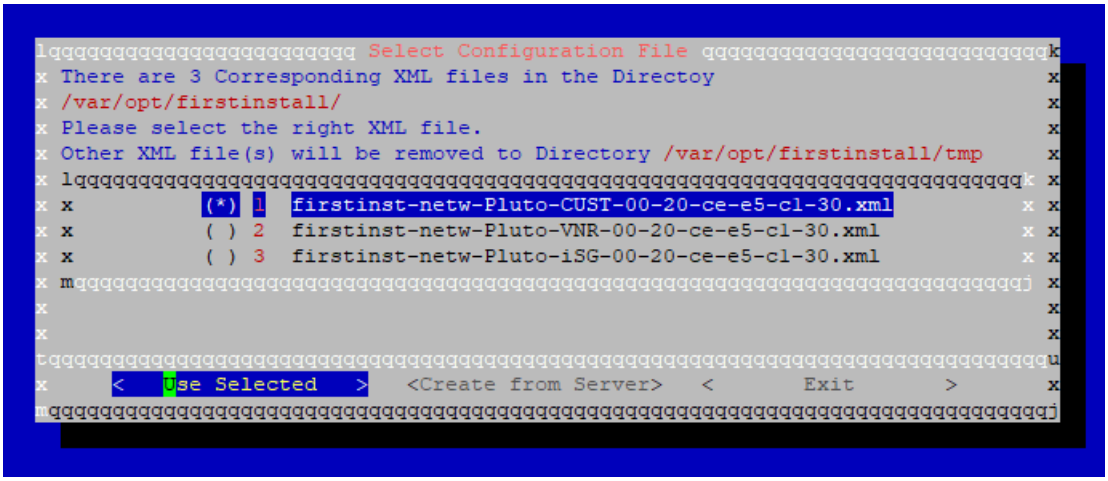


Figure 142: Recovery - Select XML file

The next screen offers the user the function **Call Editor:vi**. With this function you have the possibility to view/edit the XML file.

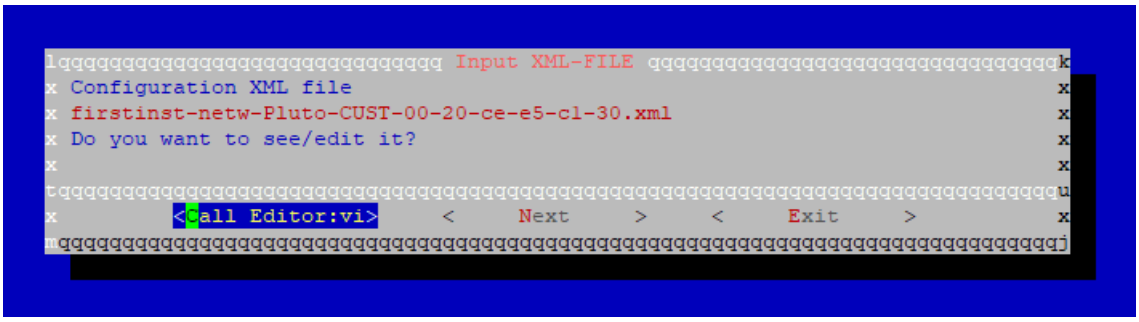


Figure 143: Recovery - View/edit XML file

If the user selects **Call Editor:vi** then the next screen shows a short description of standard "vi" commands.

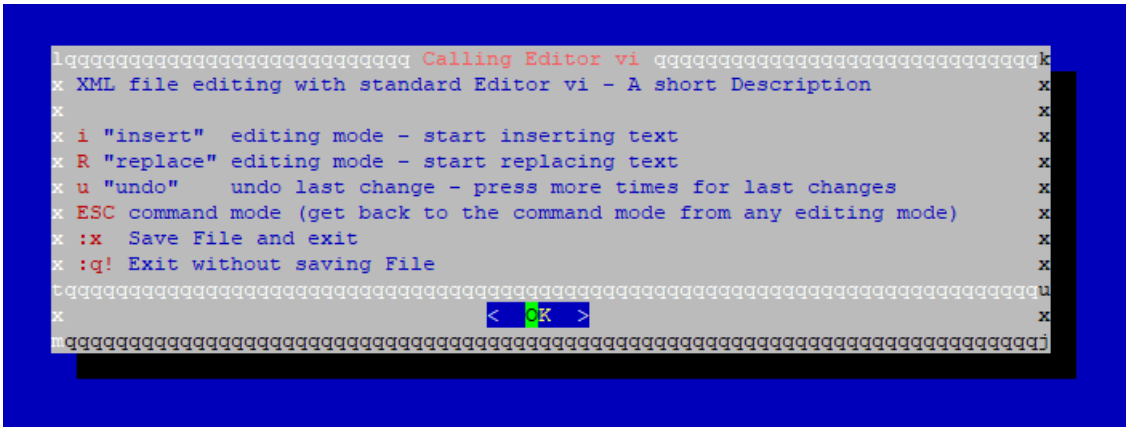


Figure 144: Recovery - Standard vi commands

By clicking **OK** the XML file is opened in the "vi".

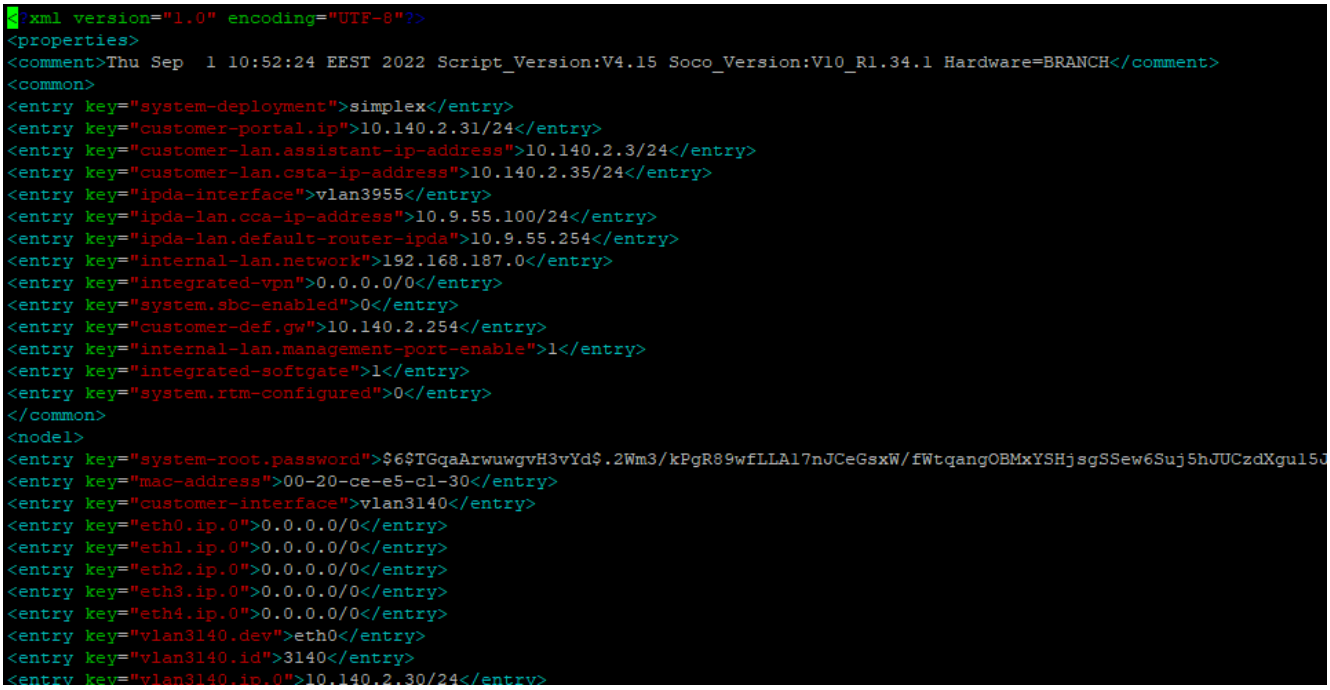


Figure 145: Recovery - XML file in vi editor

Now you can edit the XML file.

IMPORTANT: Changing the deployment is not allowed. You can recover/reconfigure only the already installed deployment. If the deployment has been changed in the XML file an appropriate message is shown on the next screen, similar to the one below. The only exception to this restriction is the change from Survivable Softgate to Standalone Softgate.

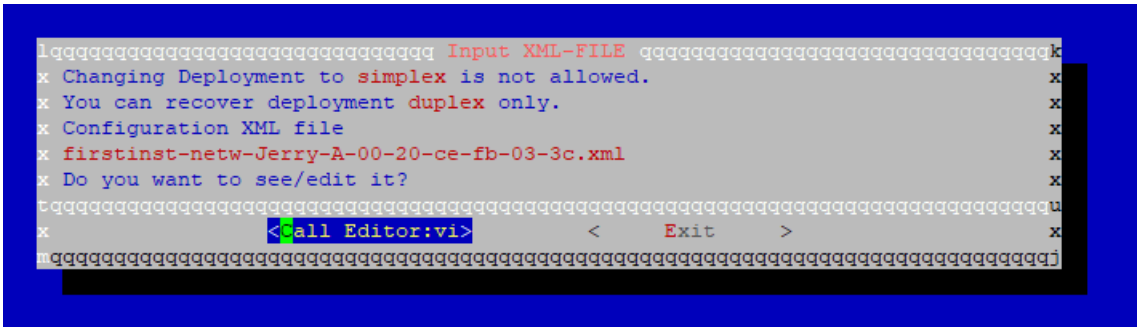


Figure 146: Recovery - Message in case deployment has been changed

In case the deployment has been changed the user must edit the XML file again and correct the deployment in order to proceed with the next step.

Now, the consistency of the XML file is checked. The user can only go on with the configuration, if there is no error message.

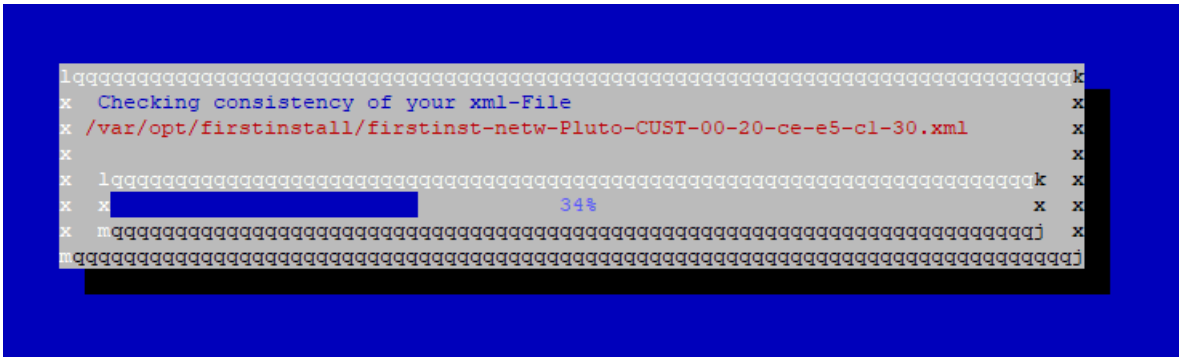


Figure 147: Recovery - Consistency check of XML file

In a case of warning(s) the user can decide if he/she wants to continue with the recovery/reconfiguration or not.

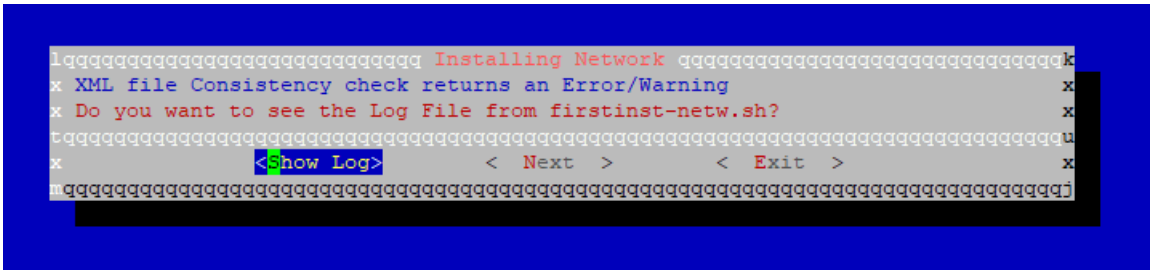


Figure 148: Recovery - Consistency check with error/warning

In the log file the user can find more information about the errors/warnings.

If there are error messages in the log file the user has to correct the XML file accordingly.

If there are no errors or only warnings the user can proceed further by pressing the **Next** button.

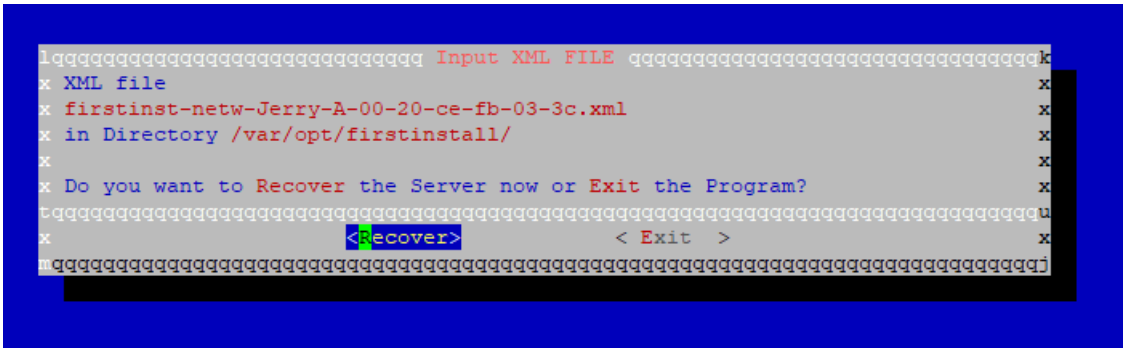


Figure 149: Recovery - Start recovery

For single node deployments please continue with Section 6.3.2.2, "Single Node Deployments".

In case of a multi node deployment (like Duplex or Separated Duplex) please continue with Section 6.3.2.3, "Multi Node Deployments".

6.3.2.2 Single Node Deployments

- User connected to the node via network - SSH
- If the user is connected to the node via network -SSH, the connection will be lost for a couple of minutes, because of deleting/reconfiguring the network parameters. The IP address displayed for reconnecting is taken from the Customer LAN configuration of the XML file.

  Select **Yes** to continue.

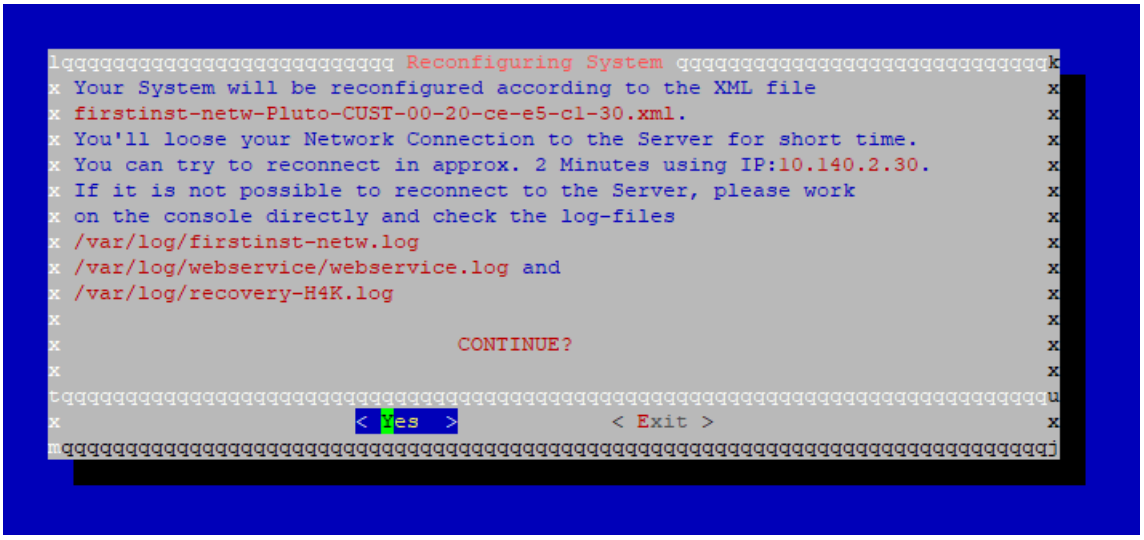


Figure 150: Recovery - Stopping all services

- User is working directly at the console

  If the user is working directly on the console, the following screen is displayed instead of the previous one.

  Select **Reconfigure** to continue.

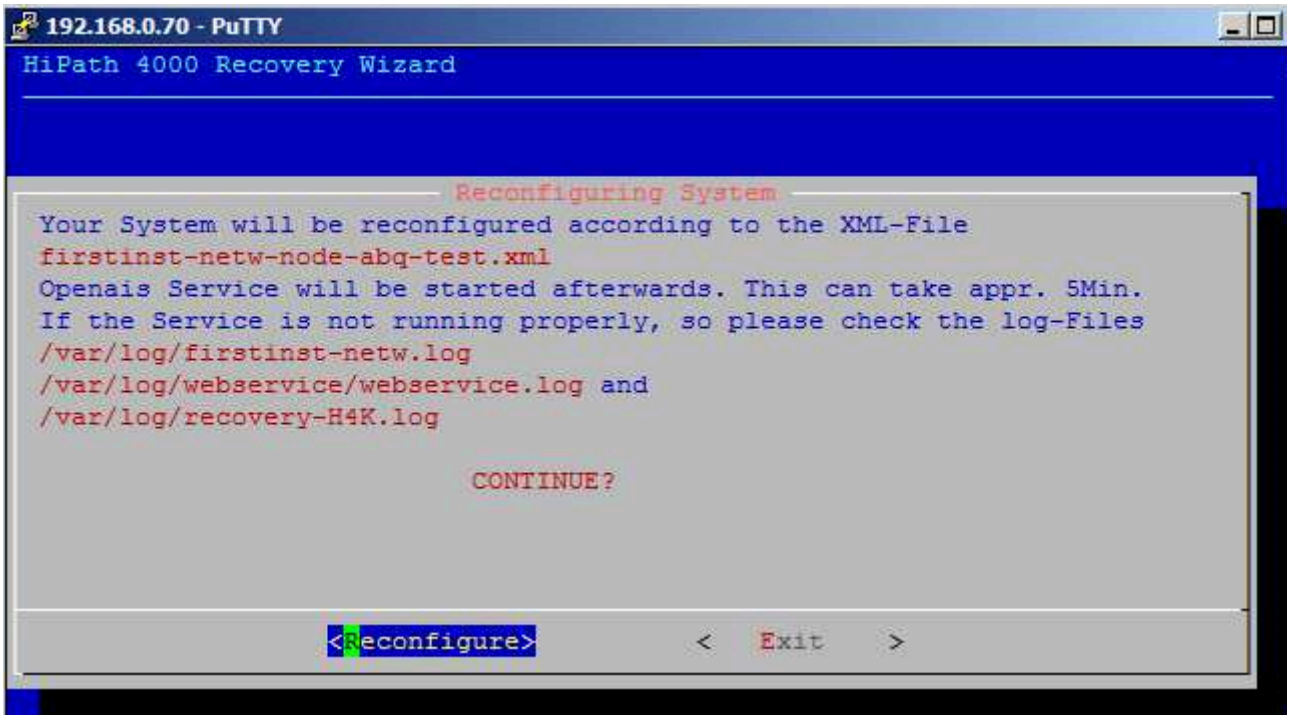


Figure 151: Recovery - Start recovery/reconfiguration

Script checks if any services on the local node are stopped. If not a screen appears where the user can confirm stopping the machines which means starting the recovery/reconfiguration or exit the Recovery/Reconfiguration Tool. If OpenScape 4000 SoftGate is configured and running on the node, the related services will be stopped also.

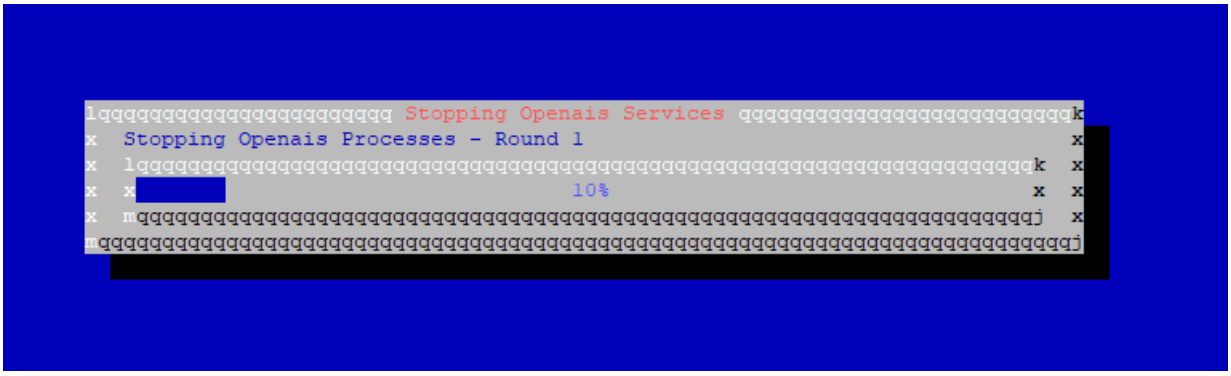


Figure 152: Recovery - Stopping all services

After stopping OpenScape 4000 services the recovery/reconfiguration job starts. If services will not be started (by the script or by the user) in 15 minutes since the time they were stopped, they will be started automatically.

6.3.2.3 Multi-node recovery functionality

To avoid system destruction for duplex or separated duplex (multi-node deployments) recovery, the recover-H4K.sh script can only run on each node individually and should be started in the correct order:

- Quorum Node (GSD)
- Stand-By Node
- Active Node

The functionality is dependent on following scripts (additionally to current recover-H4K.sh dependencies):

- `/opt/webservice/scripts/swupdated`
- `/opt/webservice/scripts/gethaipsetupentry.sh`

Step 1. Login on all 3 nodes, start the recovery script and select **Single node** (select "**Recover only this node**"),

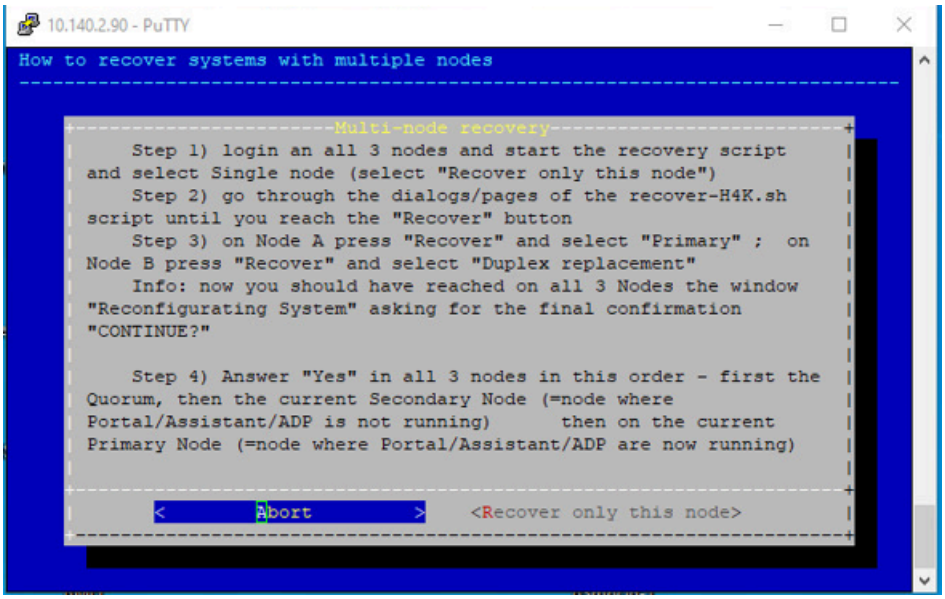


Figure 153: Recovery node order

User is asked to select First Install XML file that will be used during recovery.

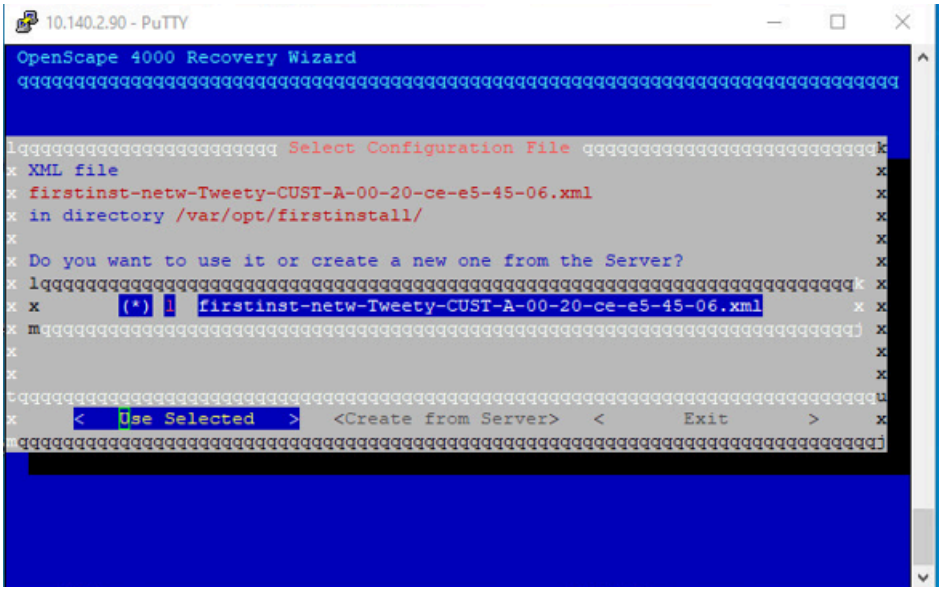


Figure 154: Recovery Wizard

Step 2. Go through the dialogs/pages of the recover-H4K.sh script until you reach the "**Recover**" button

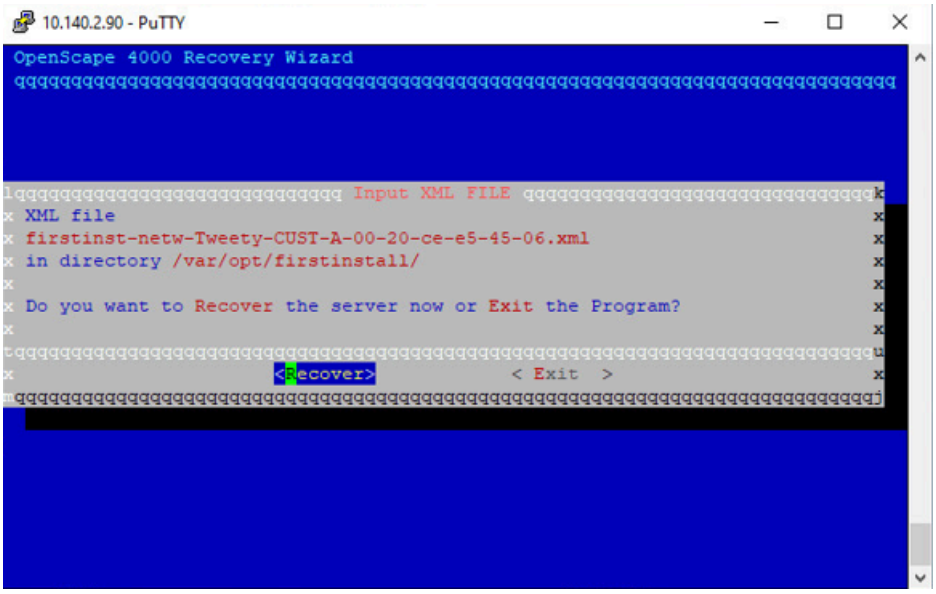


Figure 155: Recover

Step 3. On Node A press "**Recover**" and select "**Primary**"; on Node B press "**Recover**" and select "**Duplex replacement**"

NOTICE: Now you should have reached on all 3 Nodes the window "**Reconfiguring System**" asking for the final confirmation "**CONTINUE?**"

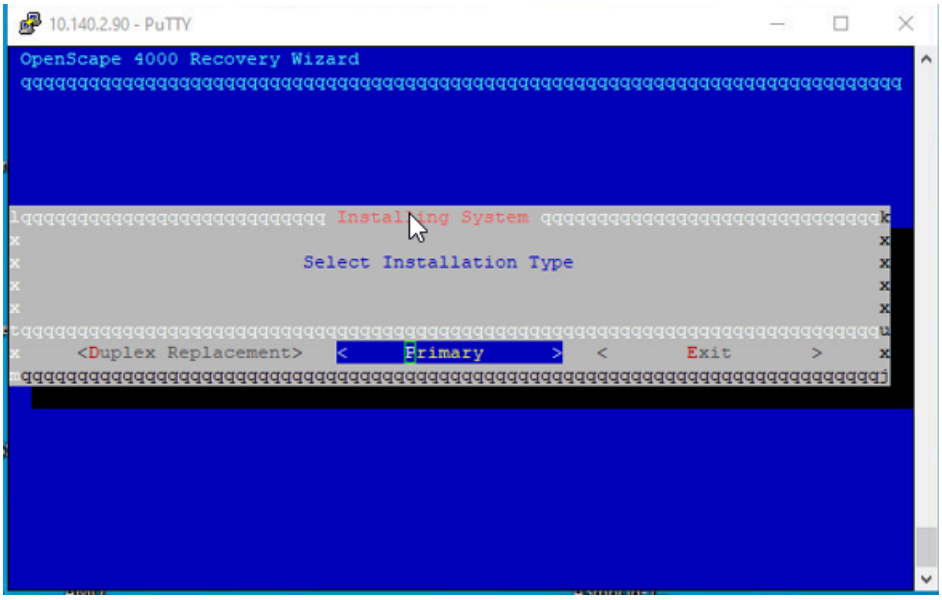


Figure 156: Recovery Node Primary

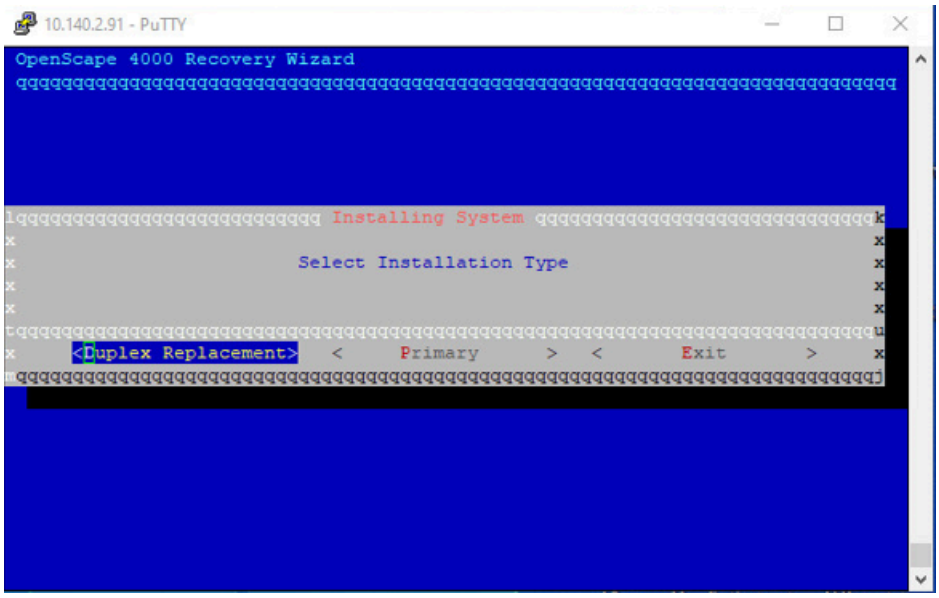


Figure 157: Recovery Node Secondary

For Primary Node we have a window **Attention**

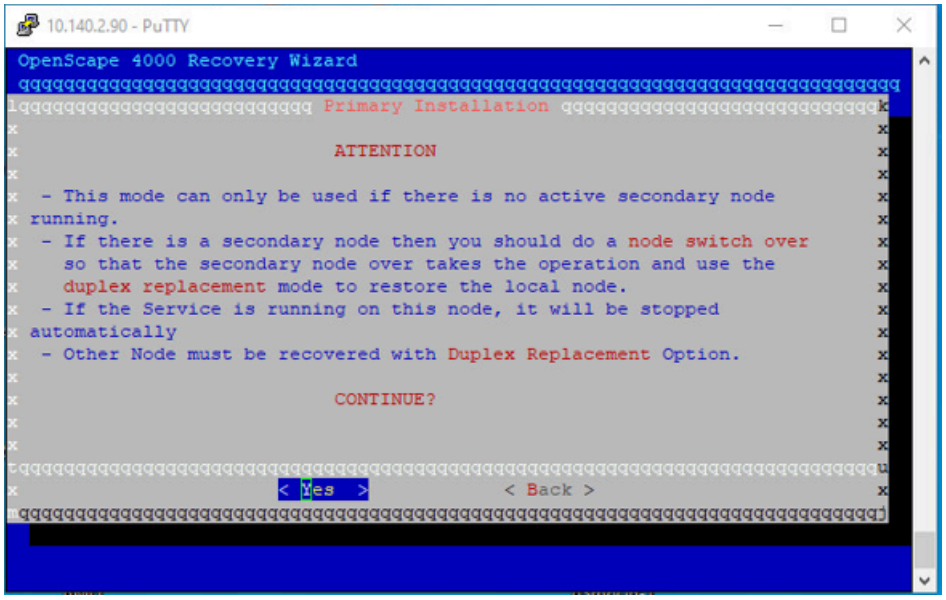


Figure 158: Attention

Step 4. Answer "**Yes**" in all 3 nodes in this order - first the Quorum, then the current Secondary Node (= node where Portal/Assistant/ADP is not running), then on the current Primary Node (= node where Portal/Assistant/ADP are now running)

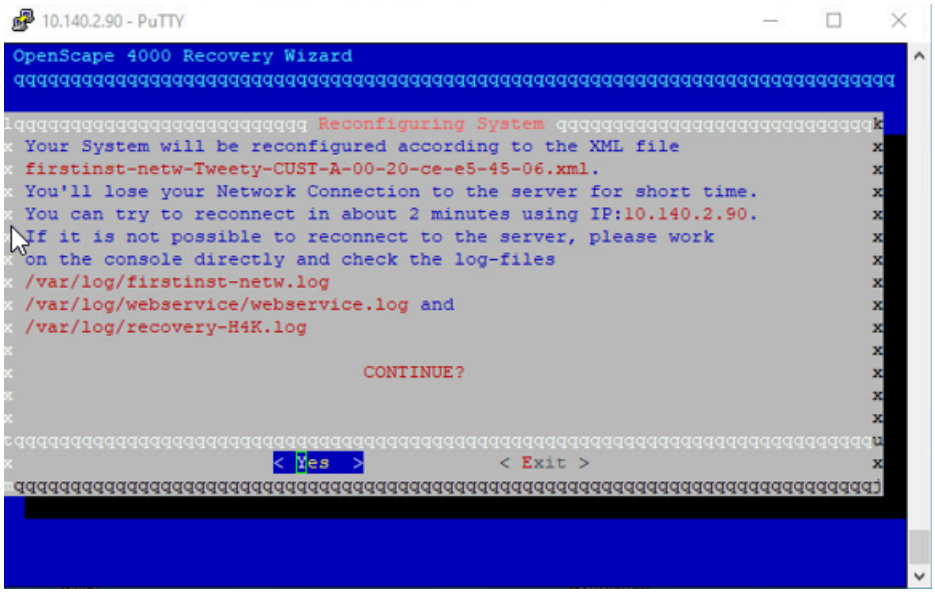


Figure 159: Reconfiguration system & Logs

If no error has been found and user wishes to proceed, OpenAIS services are stopped on all nodes in correct order (first quorum if present, then stand-by node, then active). If services will not be started (by the script or by the user) in 15 minutes since the time they were stopped, they will be started automatically.

Figure 160: Stopping OpenAIS services

In case of troubleshooting, the logs to be checked are:

- `/var/log/firstinst-netw.log`
- `/var/log/webservice/webserive.log`
- `/var/log/recovery-H4K.log`

If services will not be started (by the script or by the user) in 15 minutes since the time they were stopped, they will be started automatically.

6.3.3 Default Gateway

Use the Recovery/Reconfiguration Tool (see Section 6.3, "Recovery/ Reconfiguration Tool") on each node.

6.3.4 IPDA Network IP Address Change

NOTICE: This topic is treated for both cases (changing the IP address within the same network or in different networks) since changing the CCA/CCB addresses will cause a telephony downtime regardless of what case is chosen.

Step 1:

In case of changing the IP addresses **using IP addresses from the same network** (subnet), change the RMX configuration via AMO commands for CCA, CCB, direct link access points/OpenScape 4000 SoftGates and all other necessary IP addresses (e.g. STMI4).

In case of changing the IP addresses **using IP addresses from a different network** (subnet), modification needs to be done also for network link access points/OpenScape 4000 SoftGates.

- Change the IP addresses of CCA/CCB with AMO SIPCO.

- Change the IP addresses of the access points with AMO UCSU.
- Change the signalling IP addresses with AMO APRT.
- Update the configuration with AMO UPDAT.

Step 2: : (or alternatively use AMO USSU, parameter UPDATAP)

Change the configuration on each NCUI via V24.

Then modify the access point/OpenScape 4000 SoftGate data with the OpenScape 4000 Platform Administration (Portal):

Open the **OpenScape 4000 Platform Administration (Portal) > System > LAN Configuration** page and update the data accordingly.

After Step 1 and Step 2 were executed and verified that all changes were made successfully, execute Step 3.

Step 3:

Use Recovery/Reconfiguration Tool (see Section 6.3, "Recovery/ Reconfiguration Tool") on each node.

NOTICE: First after the minimum of a soft restart will a new HSR connection be made (if the Recovery/Reconfiguration Tool may have already requested a restart during part of its steps another soft restart must not be initiated).

6.3.5 Corosync Host Name and IP Address Change

Use the Recovery/Reconfiguration Tool (see Section 6.3, "Recovery/Reconfiguration Tool") on each node.

6.3.6 Atlantic Interface

If the new interface that you want to use does not already have IP address configured as 0.0.0.0 /0 you have to use the Recovery/Reconfiguration Tool to change it.

6.3.7 OpenScape 4000 SoftGate / Enterprise GW Changes

NOTICE: This section is valid for all deployments with OpenScape 4000 SoftGate or Enterprise Gateway.

If you want to change:

- the physical LAN interface (e.g. from eth0 to eth1)

or

- the IP address of the physical interface to IP address from another subnet

then you must use the Recovery/Reconfiguration Tool (see Section 6.3, "Recovery / Reconfiguration Tool").

It is not possible to configure LAN redundancy for SoftGate / Enterprise GW WAN or Signaling Survivability from Portal. Use the **XML Config** file generator to configure bonds during the installation, then assign the bond as the interface to be used instead of the eth.

If the SG is already installed, then use the **recover-H4K.sh** tool to configure the bond and then assign the bond in the WBM.

NOTICE: The changes performed this way apply only to the local server (SG / Enterprise GW). Of course, changing an access point IP address means that also the host system has to be reconfigured accordingly – please see the IPDA section in OpenScape 4000 V10, Volume 4: IP Solutions, Service Documentation.

NOTICE: The Recovery/Reconfiguration Tool may be used also to change other IP addresses on the SoftGate (e.g. Assistant / CSTA).

---

7 Licensing

IMPORTANT: Please check OpenScape 4000 Assistant/ Manager, License Management, Administrator Documentation for detailed information regarding licensing of OpenScape 4000 software. All documents that are available on E-Doku are also available on the Unify Partner Portal. If you don't have access to E-Doku please use the Partner Portal.

7.1 Overview

As of HiPath 4000 V6 the license concept is based on the **H**iPath **L**icense **M**anagement (HLM). The SIM card is no longer needed.

Licensing will not change for the older OpenScape 4000 systems (V5 and before).

Instead of MAC address the licenses will be locked to Advanced Locking Identifier (ALI). This identifier is a text string generated by Central License Agent based on system configuration. The CLA is using following configuration parameters of system to generate ALI:

Host Name

Host IP Address

Gateway IP Address of the same network interface as Host IP Address

Primary DNS IP Address

Time Zone (GMT Offset)

All the above items are mandatory for generation of ALI string. If some of them is not configured ALI cannot be generated.

Since V8 the trunks will be without the license fee. This means the RMX will not count the configuration of trunks into number of used FLEX licenses.

However the number of B-channels used by trunks will still be counted as number of managed ports by OpenScape 4000 Manager. This means the counting of the number of managed ports per V8 system (required by OpenScape 4000 Manager) will same as in V7.

For which license is to be used please refer to the sales information of OpenScape 4000 V10.

A grace period license is created automatically with the first portal configuration, which remains valid for 30 days.

A customer license must be created by specifying the ALI number and the system number in the Central License Server (CLS). The number of licenses required is specified here. The generated ".lic" file can be loaded into the OpenScape 4000 Assistant using the "License Management" application. The OpenScape 4000 Assistant generates a codew from this for the RMX.

Licenses can be loaded and displayed in the OpenScape 4000 Assistant in the **Access Management > License Management** menu. Click **Browse** to search for and select the license file on your PC or drives. Then confirm your selection with **Upload license**. The license file is thereby copied to the predefined directory.

Information on the number of purchased, used, free and blocked licenses is available as before in AMO CODEW.

For more information on the License Management Tool (LMT) please refer to the online help or the administrator documentation **OpenScape 4000 Assistant/Manager, License Management**.

For more information on the License Management please refer to the Partner Portal: https://enterprise-businessarea.unify.com/hlm/default.aspx

For more information on the central license server please refer to the Partner Portal: https://www.central-license-server.com/license-management/session/login.htm

7.2 Grace Period and License File Installation

After the OpenScape 4000 Assistant first installation was successful, the system is in the grace period license (30 days).

You may check it in OpenScape 4000 Assistant under:

Access Management > License Management

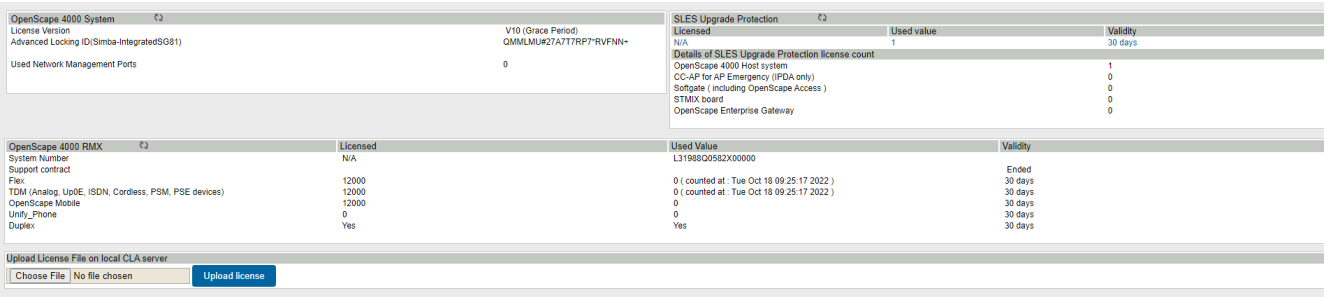


Figure 161: OpenScape 4000 Assistant - Display installed licenses

Add exception in OpenScape 4000 Assistant Firewall in order to connect with Expert Access:

Base Administration > Webmin > WAN Configuration > Firewall > New Entry Properties CLAN Host / Net

In RMX you can check the grace period with `DIS-CODEW;`.

The license is associated to the Switch Number. It is part of the license file name.

Before the import of the license, the Switch Number has to be configured with AMO ANUM.

IMPORTANT: It is only possible to do it once! It can not be changed for security reasons. A new generation would be necessary.

ADD-ANUM:TYPE=SYSNO,UNIT=A1,SYSNO=<switch-no.>;

EXEC-UPDAT:UNIT=A1,SUSY=ALL;

Now it is possible to activate the official license.

Import the official license files with OpenScape 4000 Assistant License Management:

License Management > Browse... > Select the license file **> Upload license**

IMPORTANT: In case of multi node deployment both licenses for active and standby should be imported!

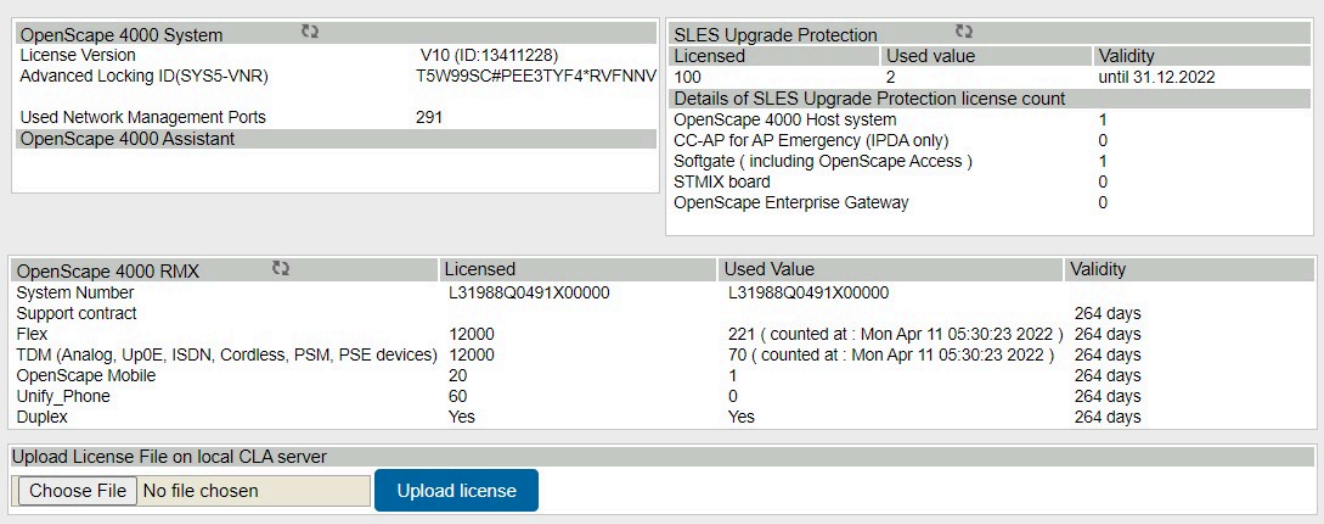


Figure 162: OpenScape 4000 Assistant - License file installation with license management

An automatic CODEW generation is executed after about 15-20 minutes.

After that you may check the validity as described before.

7.3 Installing the License for OpenScape 4000 SoftGate and OpenScape Enterprise Gateway

IMPORTANT: The OpenScape Access/EcoBranch modules are covered by the normal Flex license!

The license can be downloaded from the CLS server.

After installing the license you can find it in the directory `opt/cla/license`.

You have three possibilities to install the license:

1) Install the license via CLM (Customer License Manager).

CLM can be installed on another computer in the network or on the local host after CLA installation.

2) The license can alternatively be imported by copying the license file to the CLA import directory `opt/cla/import` (see CLA release note).

When the license is installed with copying it to the import directory, it will be read from the import directory, checked and then copied to the directory `opt/cla/license`. After this the license file will be deleted from the import directory.

3) Starting with V10R1, the license can be installed via Web based management (Configuration - > Basic Settings -> License Import).

When the license file is loaded a confirmation message is displayed showing that the file was correctly imported. The status can be seen on the License Information page. Establishing a new licensing session may take some time.

For integrated SoftGate on Enterprise GW use the WBM of the Enterprise Gateway itself to upload the SoftGate License file.

Important Notes

- The "Advanced Locking ID" replaced "Locking ID". The string is now generated from several parameters instead of IP address. The "Advanced Locking ID" can be found in Web based management or Gateway Dashoboard (Configuration -> Basic Settings -> License Information).
- The 30-day grace period begins when OpenScape 4000 SoftGate is started, when the license has not been installed before.
- If within the 30-day grace period no valid license has been activated the OpenScape 4000 SoftGate can no longer be administered.
- If there is a CLM installed locally before the CLA is installed, then the CLA installation does not create a CLA admin account. In this case, you can either just use the local CLM (with no account) or create an account via the local CLM.
- In case integrated SoftGate (iSG) is configured, no secondary SLES update protection license is required in the host, but nevertheless a normal SoftGate Base license is needed for the iSG.
- In case an integrated SoftGate (iSG) is deleted or not configured on RMX, deactivating it from the Portal is necessary to keep the SLES update protection accurate and synchronized.

7.4 OpenScape 4000 Appliance Software License JeOS

7.4.1 Operating System SUSE Linux Enterprise JeOS for OpenScape 4000

The SUSE Linux Enterprise JeOS (Just enough Operating System based on SLES JeOS) will be used as operating system for the following solution:

- OpenScape 4000 Communication Server (Simplex, Duplex und Separated Duplex)
- OpenScape 4000 SoftGate Application with or without AP-Emergency Software
- OpenScape Enterprise GW Application with or without AP-Emergency Software
- OpenScape Access 500/ OpenScape 4000 EcoBranch with or without AP-Emergency Software
- AP-Emergency Server for IP Access Points (AP3700 IP)
- Survivable deployments
- STMIX

The operating system SLES JeOS is sold as Software Appliance Model together with above's OpenScape 4000 solution components.

The SLES JeOS operating system software and fixes (Fixed Release, Hot Fixes), will be provided by the software server.

The operating system must not be provided separately by the customer. Additional maintenance agreements are not necessary.

After 6 years a new contract has to be formed otherwise software fixes (Fix, Minor and Major Release) and security patches for the SLES JeOS cannot be updated.

The license agreement is stated in EULA.

7.4.2 Basics of JeOS Licensing

The SUSE provided Software Appliance Model for usage of the operating system is divided into: Reporting and Run down of licenses and checking.

7.4.2.1 Reporting

Ordering a OpenScape 4000 V10, SoftGate, STMIX and STMIY cards will automatically trigger the ordering of appropriate amount of JeOS license (update protection keys).

7.4.2.2 Run down of Licenses and Checking

The JeOS licensing for the OpenScape 4000 family is handled the following way. A combined license position will cover the basic system, the duplex unit and the OpenScape 4000 SoftGate, OpenScape Access/EcoBranch. Hence verification of the OpenScape 4000 SoftGate license has been shifted to the OpenScape 4000 Assistant of the basic system.

7.4.3 OpenScape 4000 - JeOS

NOTICE: Within the following chapters only the OpenScape 4000 will be mentioned, however the same will hold true for OpenScape Access/EcoBranch in connection with OpenScape 4000 SoftGate.

Starting with the release of the HiPath 4000 V6 the Novell provided Software Appliance Model (JeOS) will be used. With the ordering of a OpenScape 4000, or OpenScape 4000 SoftGate, the Royality SLES Appliance for the OpenScape 4000 family will be registered by SAP, such that the charging of the Royalties of these systems can follow at a fixed date.

Software Upgrade OpenScape 4000 V10

The checking of the JeOS license will be done by the system. The JeOs license key must be downloaded from CLS and installed at the OpenScape 4000 system. After that the system update from HiPath 4000 V6 R1 to OpenScape 4000 V10 can be done. The OpenScape 4000 Assistant will refuse the activation of OpenScape 4000 V10 software if the JeOS license is missing.

The remaining run down time of the JeOS license will be computed using the activation date of HiPath 4000 V6 R1. Hence the longer ago HiPath 4000 V6 R1 has been activated the earlier the renewing of JeOS licensing has to be done. The remaining run down time will be displayed at the OpenScape 4000 Assistant's dashboard.

New System OpenScape 4000 V10

Openscape 4000 orders will contain the JeOS licenses besides the regular licenses (e.g. Flex licenses). These licenses will be automatically provided at the CLS in the license file. The run down time of the JeOS license will be started through the activation of the license at the CLS and the checking of run down by the OpenScape 4000 Assistant.

Run down of JeOS License

The JeOS license is limited to 3 years. With the run down of the license the legal requirement to update the operating system will terminate.

Re-ordering the JeOS license (see Section 7.4.6.2, "Renewing of JeOS License by 3 Years") will cancel out the restrictions and therefore updates will be possible.

Simplification

In order to simplify run-down scenarios the OpenScape 4000 basic system is defined as Master.

That means that the expiration dates of all related controlled units such as OpenScape 4000 SoftGates, Duplex units, APEs will be geared to the date of expiration of the OpenScape 4000's basic unit.

The JeOS run down of the system triggers a warning or the locking for the updates of the operating system. All Switch related devices must follow the upgrade, although their date of expiration might not be reached.

The big advantage is that only at one point of time, namely every 3 years, an update of the JeOS Royalties will be necessary!

7.4.4 Central License Server (CLS)

All already installed systems with OpenScape 4000 software, as well as OpenScape 4000 SoftGates will be provided automatically with the JeOS license by the CLS, which will also determine the remaining run down time using the date of activation. This action will be done only once.

The JeOS license will be included within the order. Therefore all new orders of systems OpenScape 4000 and OpenScape 4000 SoftGates will have the JeOS license for run down checking. All orders later on for Duplex or OpenScape 4000 SoftGate are depending on the run down maturity of the host system.

Diagram

- JeOS license within new order of hardware (example)

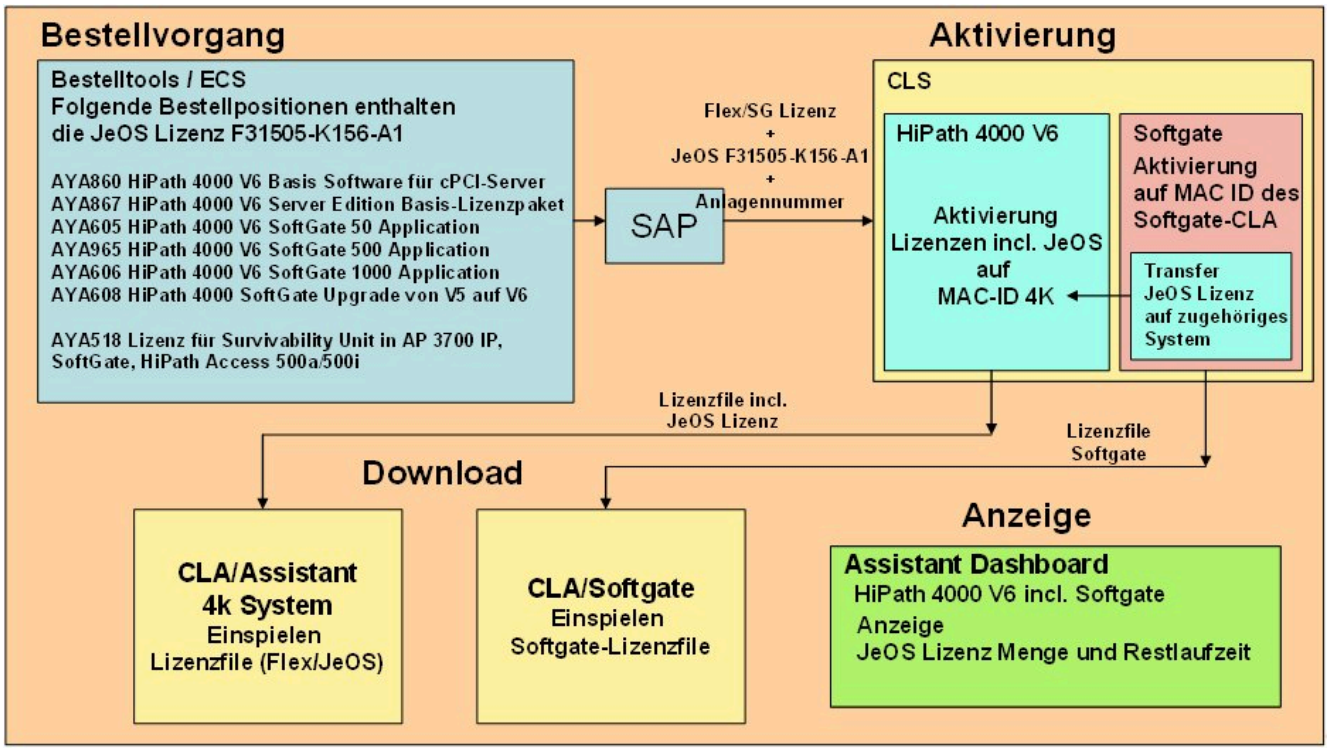


Figure 163: JeOS license within the new order of hardware

- Re-order JeOS License (example)

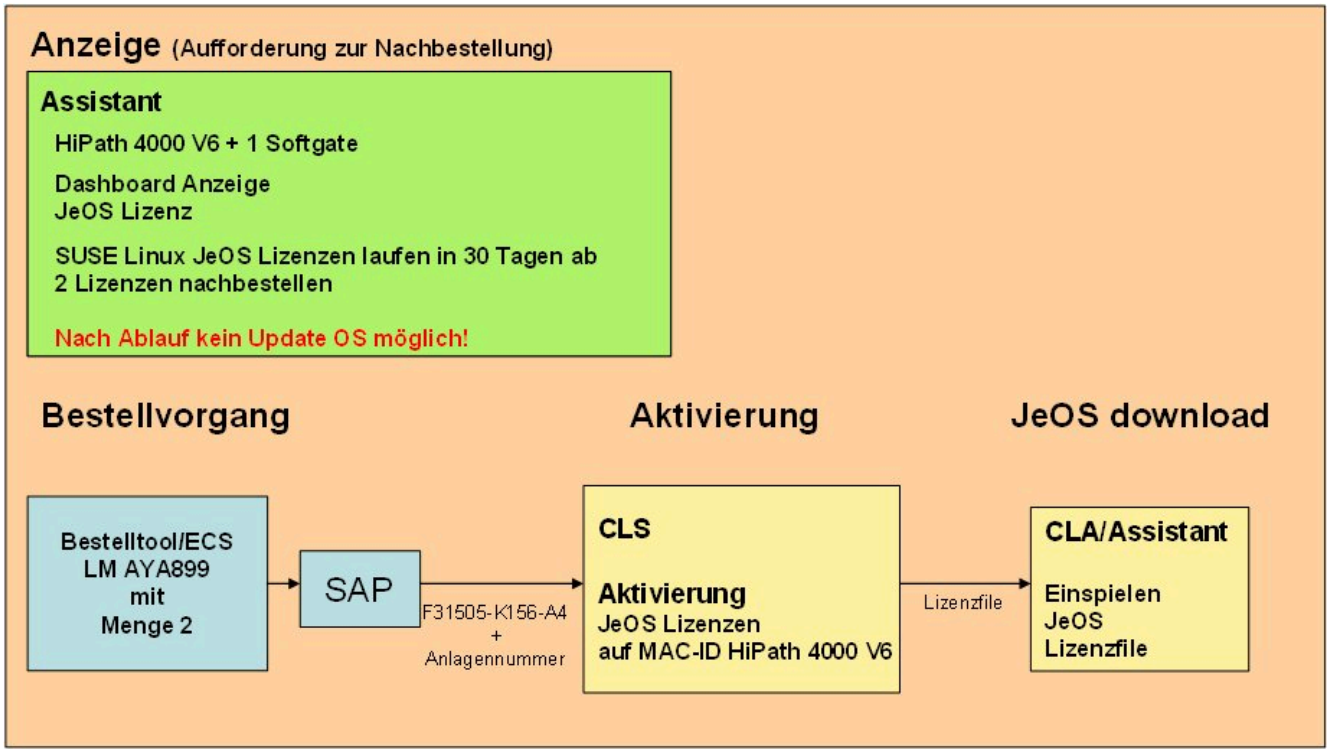


Figure 164: Re-order JeOS license

7.4.5 System Status depending on JeOS License

7.4.5.1 System Status and Information

The OpenScape 4000 Assistant's dashboard reads the current JeOS licenses and the amount of JeOS licenses in use for each system ID (L31...). The OpenScape 4000 Assistant provides a report of this information in the dashboard. The OpenScape 4000 Assistant provides a warning LAP2 message at the dashboard 6 months before the appliance license will end. Furthermore the user will get a pop-up message when logging in 3 month before maturity.

>>OpenScape 4000 V10 SLES Upgrade Protection for 3 years will discontinue in x days. After that no Update of Operating System SuSE Linux is allowed. Only Updates of RMX, CSTA and Assistant hotfixes can be performed.<<

The LICM_SLES_UPDATE_PROTECTION will send a minor alarm to the logging management 30 days before maturity stating the up-coming event. Finally a SNMP trap will be generated.

After run down of the master JeOS license (refer to Section 7.4.3, "Simplification") no update of the Operating System Software can be done. The OpenScape 4000 Assistant urges to renew the JeOS license. The user will get the information from the dashboard how many appliance licenses (JeOS) need to be ordered.

The dashboard is partitioned in following products:

- OpenScape 4000 Host System
- CC-AP for AP Emergency (only IPDA)
- OpenScape 4000 SoftGate incl. OpenScape Access and OpenScape 4000 EcoBranch.

7.4.5.2 JeOS Extension

The renewal of JeOS licenses by the order process will initiate a license file by CLS with an ordered quantity and a max. run time of 3 years. The license file can be downloaded by the CLS interface and installed on the CLA of the OpenScape 4000 Assistant.

7.4.6 Order process

7.4.6.1 Initial order by Hardware

The JeOS license is part of the initial order of a OpenScape 4000 V10 system or a OpenScape 4000 SoftGate including OpenScape Access/ EcoBranch and will be registered by the particular LM (feature number). This license will expire in 3 years.

More details are described in Section 7.4.3, "OpenScape 4000 - JeOS".

7.4.6.2 Renewing of JeOS License by 3 Years

After the demand from the OpenScape 4000 Assistant to renew the JeOS licenses the order can be initiated by the Sales Tools. The Dashboard will report the sum of JeOS licenses that need to be renewed.

NOTICE: The quantity of JeOS licenses includes the OpenScape 4000 SoftGate.

By activation of JeOS licenses at the OpenScape 4000 Assistant the blocking of operating system will be eliminated respectively avoided.

7.4.7 Summary of JeOS Activities

7.4.7.1 Renewal of JeOS License

The need of renewal of the JeOS license will be displayed at the OpenScape 4000 Assistant's dashboard. Already 6 months prior to maturity the OpenScape 4000 Assistant notifies about the run down of JeOS license.

Furthermore 1 month prior to maturity theOpenScape 4000 Assistant dumps a message how many JeOS licenses need to be ordered, including the OpenScape 4000 SoftGates.

If there is no reaction the OpenScape 4000 Assistant will lock the upgrade of operating system software at maturity date.

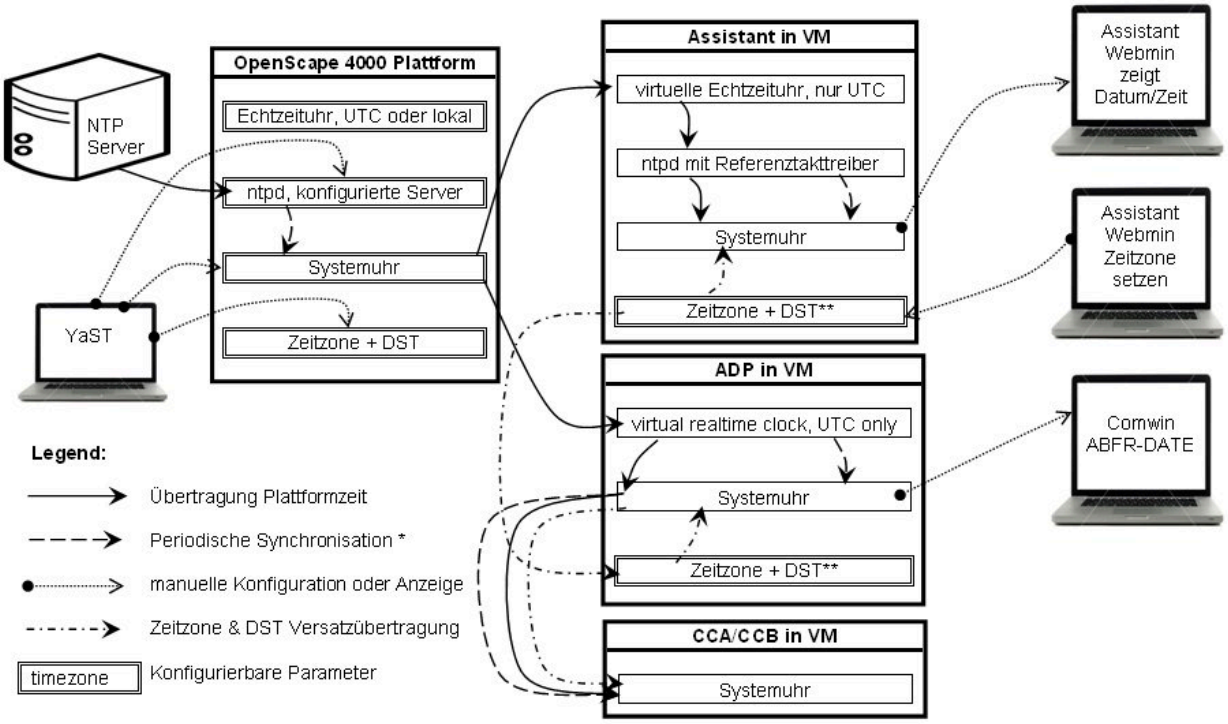
The locking can be avoided by ordering the right amount of JeOS licenses and downloading it to the OpenScape 4000 CLA via CLS. There is no need of assignment of all existing OpenScape 4000 SoftGates because they are already assigned to the host. Service will activate the JeOS licenses and install it on the host CLA using his MAC-Id. Thereby a potential lock will disappear. However if the amount of JeOS licenses does not match to the requested number, OpenScape 4000 Assistant refuses the license file. OpenScape 4000 Assistant notifies this situation by an error message and refers to the amount of JeOS licenses that are missing. While the license lack occurs no update of operating system software can be done until the requested licenses are installed. That means an additional order of JeOS licenses is necessary in that case.

7.4.7.2 Expansion by OpenScape 4000 SoftGates

Additional OpenScape 4000 SoftGates that have not assigned yet to the system require 2 license keys. The JeOS license must be assigned and activated to the MAC-ID of the adjacent OpenScape 4000 V10 system and must be imported at the particular CLA. However the OpenScape 4000 SoftGate itself needs a license key that must be activated to the MAC-ID of the OpenScape 4000 SoftGate's CLA and downloaded to this CLA.

8 Time Synchronization

The OpenScape 4000 platform is the time source for all servers in the network (e.g. OpenScape 4000 Assistant, OpenScape 4000 CSTA, ADP, CCs, Access Points, OpenScape 4000 SoftGates, CC-APs, OpenScape Access modules, Survivable OpenScape 4000 SoftGates).



* Das Synchronisierungsintervall für ADP und CCs beträgt 2 Minuten. Für den Assistant the nimmt ntpd ständig fein abgestimmte Synchronisierungsintervalle vor. Wird an der OpenScape 4000 Plattform die Zeit vorgestellt, so erfolgt darauf die Synchronisation am Assistant innerhalb von 3 Minuten.
** Wert für Sommerzeitumstellung.

Figure 165: Time synchronization - overview

8.1 Network Time Protocol Server

- An NTP server must be used as an accurate time source for time synchronization of all OpenScape 4000 network components. A reliable clock source ensures cluster components remain synchronised and that software watchdogs of other components are not triggered due to clock drift of poor time sources. Acceptable NTP sources are direct connection to public NTP, or a local NTP server which is slaved from either public NTP or GPS/Atomic clock (when a connection to public NTP infrastructure is not available).
- NTP synchronization issues and failures have been noticed when customers try to simulate an NTP server (e.g. using shareware) with a poor clock source. Although some shareware programs allow you to spoof the stratum information, stratum by itself is not an indicator of a stable clock. An accurate time source is imperative for the stability of the OpenScape 4000.
- OpenScape 4000 nodes do not have a suitable clock and should not be used as NTP server.

- Systems running SNTP are not considered acceptable as servers unless they are connected to a hardware reference clock, such as a GPS Timing Receiver.
- Hardware clock in BIOS has to be set to UTC time and not local time. This has to be done during the initial setup of the system. A later change during operations can lead to service outage due to the time jumps.
- UTC-Time has to be set up once during startup of Linux and then synchronized via a reliable NTP-source to avoid any large forward or backward time jumps. The NTP server(s) should be configured in the XML file used during the first installation.
- For further information please also see Chapter 13, "Time change / synchronization".

8.1.1 Large Jumps Forward in System Time

Large jumps in system time can be rejected by the NTP daemon. To avoid such large jumps in system time that might be rejected, you can manually force the system to synchronize with the time of the NTP server using the following Linux commands:

```
sntp -4 -x.x.x.x
```

(x.x.x.x is your NTP server IP address)

hwclock --systohc --noadjfile --utc

After configuring the NTP server, you can verify that the system is synchronized with the NTP server using the following Linux command:

```
chronyc sources
```

8.1.2 Important Information for Setting or Changing the Time

- Following the NTP server configuration when the system has been synchronized with the remote time server, the time might step back by a large time frame.
- Please make sure that all virtual machines are restarted (e.g. via Linux reboot), otherwise the virtual real time clock on the OpenScape 4000 Assistant/OpenScape 4000 CSTA and ADP gets stuck and the result is unpredictable.
- If the time on the NTP server is only reset by a small time frame (up to 60 seconds) by the ntpd, synchronization is performed automatically. The virtual machines do not have to be shut down and a restart also does not have to be performed.
- All time steps forward (manually or via ntpd) of any amount are resolved automatically on all virtual machines.
- When the host time jumps back, the RMX-OS assumes the hardware clock is defective and stops synchronizing.

- The RMX needs 0-2 minutes to identify that the host time has jumped backwards.

  This can be seen in the HISTA:

  F8102 E8 N4856 OUT SERV A1 TIMEDATE NOT READY 10-06-25 13:05:31

  ALARM CLASS:CENTRAL:028

  FORMAT:0

  A9001 M5 N4857 NO ACT A1 NMCALARM MAJOR ALARM ON 10-06-25 13:05:40

  ALARM CLASS:CENTRAL:028

  ALARM NAME:SYSTEM TIME FAILURE

  FORMAT:2C

  There are two possibilities for resolving this situation:

  Manually re-synced (call AMO "change-date")

  REG-DATE;

  Use the output of `REG-DATE;`

  e.g `CHANGE-DATE:GMTDIR=EAST,TIMEOFFS=60,MODE=NT,DSTOFFS=0;`

  and feed it back to the system.

  OpenScape 4000 Assistant detects the failure in hista via AFR3 and re-syncs RMX (by calling "change-date").

  The following commands have to be active for the time changes to take effect.

  ACTIVATE-AFR:LDU=AFR3,TYPE=LDU&PROT;

  ACTIVATE-SIGNL:SWITCCH=ALLMSG,DEV=AFR3;

  When the error is corrected via 1or 2, HISTA will show "TIMEDATE READY" and "MAJOR ALARM OFF".

  IMPORTANT: CHANGE-DATE should not be used during high traffic because (beside other things) it immediately forces a time update of all phone devices. Several individual messages will be generated for each device in the BP and transferred down to the devices. In the case of large PBXs, this will produce a lot of traffic and heavy load in the BP and in the LTUs. It will take several minutes to process all devices and this may interfere with other CP activities (calls may be delayed, ...).

8.2 Configuring the Time on all Servers

The system time of the OpenScape 4000 platform is transferred to all servers when all virtual machines are started.

Synchronization of the OpenScape 4000 Assistant is performed via ntpd within approximately three minutes. Synchronization of the ADP is performed within approximately two minutes.

Check in the OpenScape 4000 Assistant whether the date and time have been synchronized correctly:

Base Administration > Webmin > System Administration > Date/Time

---

IMPORTANT: The date and time cannot be configured in the OpenScape 4000 Assistant!

8.3 Configuring the Time Zones with OpenScape 4000 Assistant

The OpenScape 4000 Assistant is the central point for time zone management for the entire OpenScape 4000 including ADP, OpenScape 4000 CSTA and the host platform.

Displayed time zones should match on all these subsystems. If any time zone differs it can be modified with OpenScape 4000 Assistant (see Section 8.3.1, "Setting the Time Zone and Summer Time for OpenScape 4000 Assistant and RMX").

8.3.1 Setting the Time Zone and Summer Time for OpenScape 4000 Assistant and RMX

During installation of the OpenScape 4000 Assistant, its time zone is taken from the OpenScape 4000 platform. This means it is then independent of the OpenScape 4000 platform.

The time zone and summer time are set via the OpenScape 4000 Assistant.

Base Administration > Webmin > System Administration > Timezone

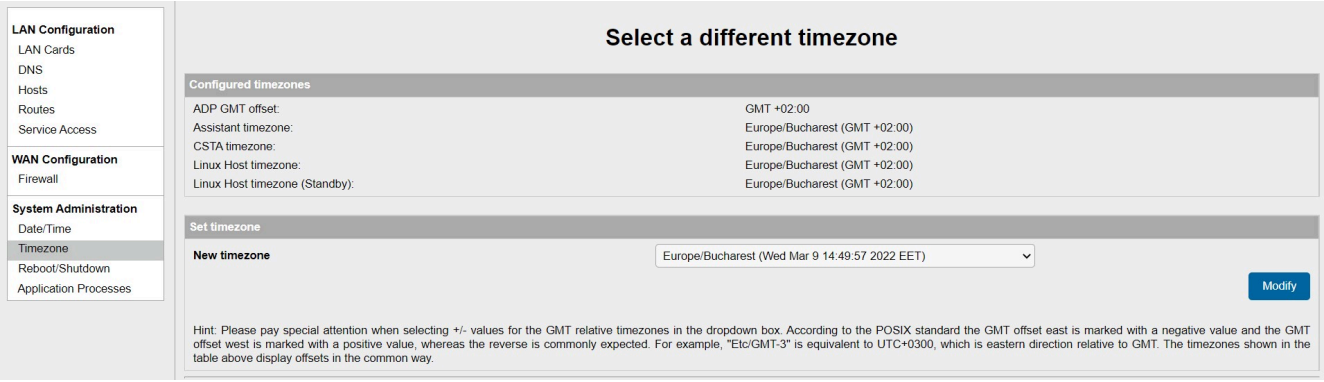


Figure 166: Time zone configuration with OpenScape 4000 Assistant

You can set the time zone and summer time by selecting the desired time zone from the **New Time Zone** list and then clicking the **Modify** button. The time zone change is effective immediately.

When the time zone is modified, the changes are automatically propagated to the host platform, OpenScape 4000 CSTA and ADP.

Also the daylight savings time offset, which is controlled by the OpenScape 400 Assistant is automatically forwarded to the ADP.

IMPORTANT: The time zone on the ADP should not be changed manually with AMO DATE!

8.3.2 Setting the Time Zone and Summer Time on the Access Point/ OpenScape 4000 SoftGate

Because the Access Points/OpenScape 4000 SoftGates may also be located in a different time zone than the host system, their time zone/summer time can be configured with the assistance of AMO SIPCO and AMO UCSU.

Specify the timeshift of the access point with respect to the host in AMO SIPCO (parameters **OFFSET** and **DIRECT**). In addition, you can also specify the parameters for the daylight-saving time adjustment.

```
CHANGE-SIPCO:TYPE=TCLASS,TCLASS=1,OFFSET=120,DIRECT=WEST,DSTSW=AUTO,MONTHDST=1,
WKDAYDST=SO,DAYNODST=FIRST,
 HOURDST=2,MINDST=30,MONTHNT=1,WKDAYNT=SA,DAYNONT=FIRST,HOURNT=2,MINNT=20;
```

You then assign the access points to the relevant time classes in AMO UCSU with the **TCLASS** parameter).

CHANGE-UCSU:UNIT=AP,LTG=<nummer>,**TCLASS=1**;

Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
SIPCO	TCLASS	d	Zeitklassen-Index
		e	Time Class Index
	OFFSET	d	Der Parameter OFFSET gibt die Zeitverschiebung in dieser Zeitklasse in Minuten an.
	OFFSET	e	The parameter OFFSET defines the time shift of this time class in minutes.
	RICHT	d	Der Parameter RICHT gibt die Richtung der Zeitverschiebung an. Eine Verschiebung nach OST ergibt immer eine spatere Zeit, d.h., der Zeit-Offset wird zur aktuellen Systemzeit addiert. Hingegen wird bei einer Verschiebung nach WEST der Zeit-Offset von der aktuellen Systemzeit subtrahiert, d.h., es wird fruher.

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
	DIRECT	e	The parameter DIRECT specifies the direction of the time shift. A shift to EAST results in a later time, which means that the time offset will be added to the actual system time. A shift to WEST results in an earlier time because the time offset will be subtracted from the actual system time.
UCSU	TCLASS	d	Zeitklassen-Index
	TCLASS	e	Time Class Index

9 Appendix A: Tables for Infrastructure Planning

Customer LAN and IPDA LAN are located in one Subnet

Table 35: Empty tables for infrastructure planning (Customer and IPDA LAN in one subnet)

Customer & IPDA LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)				
phys. IP Node 2 (YaST)				
phys. IP Quorum (YaST)				
OpenScape 4000 Platform Administration (Portal)				
OpenScape 4000 Assistant				
OpenScape 4000 CSTA				
CCA				
CCB				
NGS				
Default Gateway/Router				
Corosync LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)				
phys. IP Node 2 (YaST)				
phys. IP Quorum (YaST)				
Atlantic LAN				
				Interface
Interface				
Interface				
Interface				
Interface				

Customer LAN and IPDA LAN are located in separate Subnets

Table 36: Empty tables for infrastructure planning (Customer and IPDA LAN in separate subnets)

Customer LAN				
	IP Address	Netmask	Hostname	Interface

phys. IP Node 1 (YaST)				
phys. IP Node 2 (YaST)				
phys. IP Quorum (YaST)				
OpenScape 4000 Platform Administration (Portal)				
OpenScape 4000 Assistant				
OpenScape 4000 CSTA				
Default Gateway/Router				
IPDA LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)				
phys. IP Node 2 (YaST)				
CCA				
CCB				
NGS				
Default Router				
Corosync LAN				
	IP Address	Netmask	Hostname	Interface
phys. IP Node 1 (YaST)				
phys. IP Node 2 (YaST)				
phys. IP Quorum (YaST)[6]				
Atlantic LAN				
				Interface
Interface				
Interface				
Interface				
Interface				

[6] For Quorum a suitable interface can be chosen

10 Appendix B: First Installation Script & XML Configuration file

10.1 Introduction

The first installation of a OpenScape 4000 system is done with the script **firstinst-netw.sh**.

To call the script type the following: **./firstinst-netw.sh [options]**

It is highly recommended, to call the script for the first time with **-c** option, in order to check it for network plausibility, syntax errors and also for OpenScape 4000 specified dependencies. For all possible options please refer to Section 10.2, "First Installation Script - Command Line Options".

The first installation script should be used on a fresh installed OpenScape 4000 system and will not start on a system with an already configured network.

However, if it is really necessary to start it for a second time, e.g. after a faulty installation, all configured IP addresses must be removed from the system (e.g. call the first installation script with **-d** option).

The script writes relevant information, errors or warnings to the file **firstinst-netw.log**, which is created in the directory **/var/log**. Also the results by calling with **-c** option will be written to this file.

The first installation script will stop working by an error message, while the warning messages don't cause a stop.

The installation is done using a XML file which contains all relevant configuration data. For more information on the XML file please refer to Section 10.3, "XML Configuration File".

10.2 First Installation Script - Command Line Options

1) Called without any options

The script looks into the directory **/var/opt/firstinstall** for the XML files beginning with firstinst-netw in the file name. All these XML files must contain a line with a MAC address from a network device. The script searches for this MAC address line in all XML files in this directory and compares them with the MAC addresses from the running server. The XML file with the corresponding MAC address of the server will be taken for the installation.

Every time in a Duplex or Separated Duplex environment, when the script is called without any options, the following question must be answered:

Is this a First Installation (i) or Recovery (r)?

The script waits for 10 seconds for an answer. The countdown is displayed.

If nothing entered within in the countdown, the script works as usual. That means, a first installation or node recovery will be applied according to the

configuration in the XML file (see Section 10.3.2.2, "Node Section" > node-replacement).

Answered with **i** (first installation): An existing **<entry key="node-replacement">** tag will be removed from the corresponding node section.

Answered with **r** (recovery): The parameter value of the **<entry key="node-replacement">** tag will be changed from **0** to **1** or added if the tag does not exist in the corresponding node section (**<entry key="node-replacement">1</entry>**).

The original XML file stays unchanged. This Information will be passed to OpenScape 4000 Platform Administration (Portal) via another XML file.

2) Called with **-h** option

Help to all possible options is shown.

3) Called with **-i** or **-r** option.

- **-i**: installs system, indicates primary server in duplex or separated duplex deployment
- **-r**: installs system, indicates replacement server in duplex or separated duplex deployment

For more information see Called without any options.

4) Called with **-c xml file node name** option

The script does not make any configuration, but checks the given XML file for network plausibility, syntax errors and also for OpenScape 4000 dependency, e.g. Corosync configuration etc.. With this option, the file name must be given as second argument and the node name as a third argument. It is up to you if you give fully file name here including path name or only the file name. The script can also work with a file name only and looks for that in the directory /var/opt/firstinstall.

The best usage for this option is of course on the system, where the network will be installed later. Used like this, the script delivers also the hardware associated errors, e.g. if a network card is really installed in the machine, etc..

With the third argument (node name) all errors, except hardware associated errors, can be also found and corrected by starting the script on another Linux system.

Example: **firstinst-netw.sh -c firstinst-netw-node1.xml node1**

This option checks the XML file only in data part, so the errors in header or in end part will be ignored. But you should let all these parts in the file, because the line numbers are calculated by supposition of existence of these parts. An error dedicated to the headers is written into the log file, however it is ignored by the script.

IMPORTANT: In this check mode, the script won't stop working by an error message.

---

5) Clean the network from any network configuration

Be aware that after calling the script with the following options, every configured IP address except the loop address with 127.0.0 will be removed from the system.

Be aware that you will not have a network connection to the server after calling this option, so it is recommended not to call this option from remote.

It is not recommended to use this option in an already configured and running system, because you will lose every manual made configuration.

Afterwards, you should start the script in normal way again for configuring the network.

A single IP address can be removed also via XML file, given as parameter system-delete.ip. For more information please refer to Section 10.3.2, "Possible Parameters and their Values" > system-delete.ip.

a) Called with **-d** option

With this option, the script asks you **Do you really want to remove all configured IPs from the System?**. It will stop working, when you answer with **n** or **N** and will delete all IP addresses when you answer with **y** or **Y**.

Called with **-d -y** option

With these options the script deletes all configured IP addresses in silent mode.

6) Called with **-w**

This option creates a XML file from a running system. The created XML file is automatically checked against plausibility errors and warnings. This file can be used as a first installation XML file.

NOTICE: Templates and examples of different XML configuration files for all deployment types are included in

XML Config File Generator (under File > Load Examples), available with the latest ComWin release.

The output file is saved with the name **firstinst-netw-<first 36 characters of hostname>-<macaddress>.xml** and is written into the directory **/var/opt/firstinstall**.

In the <comment> block of the ouput file the hardware type is displayed, like in the following example:

<comment>Wed Oct 16 16:12:27 CEST 2013 Firstinstall Script Version : V2.59 **Hardware=ECOSRV**</comment>

Instead of the host name the user can define an own name (e.g. customer name). Therefore, he must use the **-w** option with a second parameter.

Example : firstinst-netw.sh **-w simplex**

The output file is then saved with the name **firstinst-netw-simplex-<macaddress>.xml** and is written into the directory **/var/opt/firstinstall**.

XML-File: /var/opt/firstinstall/firstinst-netw-simplex-00-19-99-5f-df-51.xml

NOTICE: -w option can also be used for OpenScape 4000 SoftGate deployments.

Only the configuration parameters will be restored, which are also represented in the first installation XML file. The user must/should restore manually all other network parameters, such as routing entries or host name entries etc..

7) Called with **-e** option

Script called with the option **-e**, collects every necessary data from the Server, and then archives, compresses them and saves the file to the **/tmp** directory. When finished, you will get the name of the compressed file in **/tmp** directory. The file has a size of approximately 50kB.

This file can be attached to the problem tickets for diagnosys issues.

The message is similar to the following:

Compressed Diagnosys File : /tmp/fnetw-28022013-10-36-53-537.bz2

8) Called with **-s** option

Script called with the option **-s** and a second parameter makes only the following configurations from the XML file, without removing/reinstalling the network configuration.

IMPORTANT: XML file must be copied into the directory **/var/opt/firstinstall**.

Usage:

firstinst-netw.sh, option -s

./firstinst-netw.sh **-s keyboard**	--> Configures only the keyboard layout

./firstinst-netw.sh **-s timezone**	--> Configures only the timezone
./firstinst-netw.sh **-s dns**	--> Configures only the DNS server(s) Hint: If DNS entries are changed directly via YAST, all IP interfaces will be restarted causing an outage to the system!
./firstinst-netw.sh **-s ntp**	--> Configures only the NTP server(s)
./firstinst-netw .sh**-s all**	--> Configures only the 4 parameters above

Any existing configuration will be replaced with the values from the XML file, which corresponds to the server.

9) Called with **-v** option

Script called with **-v** option prints the script version.

10) Called with **-p <XML file> <tag name> node1|node2|node3**

Script called with **-p** option and the above parameters parses tag value from a given xml file and node.

11) Called with **-m add <XML file> <tag name> <tag value> common|node1|node2|node3**

Script called with **-m** option and the above parameters inserts/overwrites the given xml tag into the given section in the given XML file.

12) Called with **-m del <XML file> <tag name> <tag value> common|node1|node2|node3**

Script called with **-m** option and the above parameters removes a given xml-tag from the given section in the given XML file.

13) Called with **-x** option

Script called with **-x** option only checks XML file status in the directory **/var/opt/firstinstall**.

Following outputs are possible

- Normal case : One corresponding XML file, exit code=0

Configuration XML file : /var/opt/firstinstall/firstinst-netw-node-a-00-20-ce-df-8a-70.xml

- Error case : no XML file, exit code=5

********** Configuration XML file not found **********

- Error case : more than one XML file, exit code=1

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

File 1 : /var/opt/firstinstall/firstinst-netw-ecosrv-simplex-00-20-ce-f0-bd-80.xml

File 2 : /var/opt/firstinstall/firstinst-netw-simplex-00-20-ce-f0-bd-80.xml

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

Following outputs are possible if the deployment is OpenScape 4000 Softgate environment

- Normal case : One corresponding XML file, exit code=0

Configuration XML file : /var/opt/firstinstall/firstinst-netw-ecosrv-simplex-00-20-ce-f0-bd-80.xml

initialcfg XML file : /var/opt/firstinstall/initialcfg-simplex-00-20-ce-f0-bd-80.xml

- Normal case : initialcfg file does not exist or no OpenScape 4000 installation section in the XML configuration file, exit code=0

Configuration XML file : /var/opt/firstinstall/firstinst-netw-ecosrv-simplex-00-20-ce-f0-bd-80.xml

Warning : Softgate Initial Config file is missing in directory /var/opt/firstinstall/

- Error case : more than one initialcfg XML file, exit code=1

Configuration XML file : /var/opt/firstinstall/firstinst-netw-ecosrv-simplex-00-20-ce-f0-bd-80.xml

There are several initialcfg.xml files, that corresponds with a MAC-Address from this Server.

File 1 : /var/opt/firstinstall/initialcfg-ecosrv-simplex-00-20-ce-f0-bd-80.xml

File 2 : /var/opt/firstinstall/initialcfg-simplex-00-20-ce-f0-bd-80.xml

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

NOTICE: The root pwd is automatically encrypted and added to the .xml file with the tag name system-root.password

---

10.3 XML Configuration File

NOTICE: Templates and examples of different XML configuration files for all deployment types are included in XML Config File Generator (under File > Load Examples), available with the latest ComWin release.

10.3.1 Format

10.3.1.1 Directory of the XML file

The XML file must be copied to the directoy **/var/opt/firstinstall**.

10.3.1.2 Name of the XML file

The XML file name must have the format firstinst-netw-XXXXX.xml, where the XXXXX can be given freely.

IMPORTANT:

XXXXX must only contains letters, numbers and/or "-" (dash), "." (dot), "_" (underline)!

First installation XML file names must not contain any spaces.

10.3.1.3 Structure of the XML file

IMPORTANT: The structure of the XML file should not be changed.

The XML file always has a "common" section and for each node an own section.

Every node section must contain a valid MAC address (see also Section 10.3.2, "Possible Parameters and their Values").

For Simplex deployments (such as Simplex, APE, RG 8350a, Standalone Softgate ...) only one node section is needed.

For a Duplex deployment two node sections (for node a and node b) are needed and for a Separated Duplex deployment three node sections (for node a, node b and quorum node) are needed.

<common>

....

</common>

<node1>

...

</node1>

<softGateInitialConfiguration>

<Property value=...>

...

</softGateInitialConfiguration>

<node2>

...

</node2>

<node3>

...

</node3>

NOTICE: For Enterprise GW the section <softGateInitialConfiguration> is renamed to <Enterprise GWInitialConfiguration>.

Data Line

Example:

<entry key="**system-deployment**">simplex</entry>

The middle part, in this example **system-deployment**, is the **parameter name**, which is also called "key". These parameter names are hard coded.

The second part, simplex in this example, the parameter value, which can be set free. But there are some restrictions for this values also, e.g. IP address conventions. For all the restrictions and rules please refer to Section 10.3.2, "Possible Parameters and their Values".

The words <entry key="..."> and </entry>, define begin and end of a data line and must be used strictly in this format.

Comment Tag

As in HTML XML has a comment tag that starts with these characters:

<!--

and ends with these characters:

-->

- A comment can be any number of lines long.
- It can start and end anywhere in a XML file.
- Multiple comments cannot be nested.
- Use comments to describe what various sections of your XML file are meant to do.

Examples:

<!-- Following three lines belong to own server Corosync -->

<entry key="eth1.ip.0">10.0.0.10/24</entry>

<entry key="eth1.hostname.0">node-a</entry>

<entry key="eth1.domainname.0">h4k.com</entry>

or

<entry key="eth1.ip.0">10.0.0.10/24</entry> <!-- This is the IP Address of Corosync -->

or

<!-- Following three Lines

belong to own

Server Corosync -->

<entry key="eth1.ip.0">10.0.0.10/24</entry>

<entry key="eth1.hostname.0">node-a</entry>

<entry key="eth1.domainname.0">h4k.com</entry>

or

<entry key="customer-timezone">Asia/Manila</entry> <!-- This is my Time zone -->

Rules

- All variables are case-sensitive!
- The script ignores every data, which is not necessary for a given deployment. This means, that you don't have to delete data lines which are not necessary for the deployment you entered.
- Example: It is not necessary to remove Corosync data from a XML file defined for a Simplex deployment. In this case, the script ignores the Corosync data lines.
- A none existent line or a line with an empty value field has the same effect.
- For example, the line **<entry key="eth0.hostname.0"></entry>** has the same effect as if this line is not existent.

10.3.2 Possible Parameters and their Values

The following entry keys are defined.

10.3.2.1 Common Section

system-deployment

In every XML file the deployment has to be defined with the following data line. If this data line is missing in the XML file, the installation won't be executed.

<entry key="**system-deployment**">[deployment name]</entry>

The following deployments are possible and must be entered as listed below:

- simplex
- duplex
- separated_duplex
- standalone_softgate

- survivable_softgate
- ape (V10R0 only)
- enterprise_gw
- survivable_enterprise_gw

> **IMPORTANT:** Every other naming causes an error and stops the script. Because of that be careful with typing mistakes!

The deployments **standalone_softgate**, **survivable_softgate**, **ape, enterprise_gw and survivable_enterprise_gw** are handled like a simplex server configuration.

For more information on a Duplex/Separated Duplex deployment please refer to Section 10.3.3.2, "Duplex/Separated Duplex Deployment Dependent Rules".

For more information on all deployments handled like a Simplex deployment (Simplex, Standalone SoftGate) please refer to Section 10.3.3.1, "Simplex Deployment Dependent Rules".

system-hpa.type

Type of OpenScape Access.

This tag must be entered if the system is a OpenScape Access.

Example:

<entry key="system-hpa.type">hpa500i</entry>

Possible values:

- hpa500i
- hpa500a

> **NOTICE:** The values are not case sensitive.

customer-portal.ip

IP address/Prefix length of the OpenScape 4000 Platform Administration (Portal).

Example:

<entry key="**customer-portal.ip**">218.1.17.8/26</entry>

Notes

- If the parameter **customer-portal.ip** is given, the following will be checked: The parameter **customer-interface** in the node section of the XML file represents the Customer LAN network interface, and the first IP address on this interface represents Customer LAN IP address. The script checks if the Customer LAN interface/IP address are defined. If yes, the script checks if both IP addresses are valid and configured in the same subnet.
- Only in a Simplex system the parameter **customer-portal.ip** can be configured permanently on an interface. This is not allowed within a Duplex system.
- The script checks if the default gateway is defined and if it is in the same subnet as the Customer LAN IP address.

Here is an example for this configuration.

<entry key="**customer-interface**">**eth5**</entry>

<entry key="**eth5.ip.0**">**192.168.0.72/24**</entry>

<entry key="**customer-portal.ip**">**192.168.0.75/24**</entry>

<entry key="**customer-def.gw**">**192.168.0.1**</entry>

ccap-number

For the deployments **ape** and **survivable_softgate** as access point number the **ccap-number** must be entered.

Example:

<entry key="**ccap-number**">**17**</entry>

Possible values: 17 - 99 , default value: 17

When the "ccap-number" is not set, the "ltu" value from the SoftGate configuration will be used instead. If both "ccap-number" and "ltu" are missing in the configuration, default value will be used.

corosync-name.node1

Host name of node 1 (e.g. node-a)

Example:

<entry key="**corosync-name.node1**">node-a</entry>

corosync-name.node2

Host name of node 2 (e.g. node-b)

Example:

<entry key="**corosync-name.node2**">node-b</entry>

corosync-name.quorum

Host name of quorum node (e.g. node-q)

Example:

<entry key="**corosync-name.quorum**">node-q</entry>

corosync-ip.node1

IP address/Prefix length of node 1 (e.g. 10.0.0.10/24)

Example:

<entry key="**corosync-ip.node1**">10.0.0.10/24</entry>

corosync-ip.node2

IP address/Prefix length of node 2 (e.g. 10.0.0.11/24)

Example:

<entry key="**corosync-ip.node2**">10.0.0.11/24</entry>

corosync-ip.quorum

IP address/Prefix length of quorum node (e.g. 10.0.0.12/24)

Example:

<entry key="**corosync-ip.quorum**">10.0.0.12/24</entry>

customer-lan.assistant-ip-address

IP address/Prefix length (e.g. 10.7.117.105)

Example:

<entry key="**customer-lan.assistant-ip-address**">10.7.117.105/19</entry>

customer-lan.csta-ip-address

IP address/Prefix length (e.g. 10.7.117.106/19)

Example:

<entry key="**customer-lan.csta-ip-address**">10.7.117.106/19</entry>

customer-dns.server.0

IP address of the Domain Name Service (DNS) server.

Example:

<entry key="**customer-dns.server.0**">**192.168.1.1**</entry>

<entry key="**customer-dns.server.1**">**211.22.33.04**</entry>

<entry key="**customer-dns.server.2**">**112.32.43.111**</entry>

- Index number 0 is mandatory, the following indexes can be given optionally (e.g. customer-dns.server.1, customer-dns.server.2).
- The first entry with the index number 0 is the preferred server.

ipda-interface

Network interface for IPDA LAN (e.g. eth2, bond1, vlan123).

Example:

<entry key="**ipda-interface**">eth2</entry>

Configuration without IPDA:

Delete the whole entry for the ipda-interface or leave the value emtpy (<entry key="**ipda-interface**"></entry>).

If IPDA is not configured an RTM must be configured:

<entry key="system.rtm-configured">1</entry>

For more information on RTM please refer to system.rtm-configured.

ipda-lan.cca-ip-address

IP address/Prefix length for IPDA LAN (e.g. 172.16.2.11/16)

Example:

<entry key="**ipda-lan.cca-ip-address**">172.16.2.11/16</entry>

ipda-lan.ccb-ip-address

IP address/Prefix length for IPDA LAN (e.g. 172.16.2.12/16)

Example:

<entry key="**ipda-lan.ccb-ip-address**">172.16.2.12/16</entry>

ipda-lan.ngs-ip-address

IP address/Prefix length (e.g. 172.16.2.41/16)

Example:

<entry key="**ipda-lan.ngs-ip-address**">172.16.2.41/16</entry>

ipda-lan.default-router-ipda

IP address of the default router for IPDA LAN (e.g. 172.16.3.1)

Example:

<entry key="**ipda-lan.default-router-ipda**">172.16.3.1</entry>

internal-lan.network

IP address of the Internal LAN subnet

Example:

<entry key="**internal-lan.network**">192.168.187.0</entry>

- It is a 24 bit network (Netmask: 255.255.255.0)
- No other IP address must be configured in this subnet.
- The last octet must always be 0. If it is not 0, it will be set to 0 during installation.
- If this Tag is missing, the network will be initialized with the default address 192.168.187.0.

atlantic-interface.0

Network interface for Atlantic LAN.

Increment the index when more than one Atlantic LAN interface is used.

Example:

<entry key="**atlantic-interface.0**">**eth5**</entry>

<entry key="**atlantic-interface.1**">**eth6**</entry>

customer-def.gw.dev

Network interface of the default gateway (e.g. eth5)

The script takes the default gateway interface from the **customer-interface**. However, it can be defined also via the following line, if no **customer-interface** is configured.

Example:

<entry key="**customer-def.gw.dev**">**eth5**</entry>

A default gateway can be configured without interface also, therefore this line is not mandatory for default gateway configuration.

integrated-softgate

If on a Simplex server or on a Separated Duplex deployment an additional OpenScape 4000 SoftGate should be configured on the same server the **integrated-softgate** tag must be set to **1**.

<entry key="**integrated-softgate**">**1**</entry>

In case of Separated Duplex with integrated SoftGate, the SoftGate can run on the Quorum Node or on the Active/Standby node. In this case the parameters are:

- <entry key="integrated-softgate">1</entry>
- <entry key="integrated_softgate_node1">1</entry>
- <entry key="integrated_softgate_node2">1</entry>

Possible values: **0** or **1**

system.rtm-configured

In case of a Simplex or Duplex deployment, the tag

<entry key="**system.rtm-configured**">[0 or 1]</entry>

must be set to **0** or **1** to indicate, if a Rear Transition Module (RTM) is configured or not.

Possible values: **0** or **1**

0	RTM is not configured
1	RTM is configured

node-replacement

If a node should be replaced during other nodes are active at a Duplex or Separated Duplex system, an additional tag in the respective node section is necessary and must be set to **1**.

This parameter must be given in the depending node section and indicates if it is a new installation or a replacement of this node.

<entry key="**node-replacement**">**1**</entry>

Possible values: **0** or **1**

0	new installation
1	node replacement

Example:

<common>

<entry key="**system-deployment**">**separated_duplex**</entry>

.

.

</common>

<node1>

<entry key="**mac-address**">**00:20:ce:df:88:e0**</entry>

.

</node1>

<node2>

<entry key="**mac-address**">**00-4c-ce-df-5e-e2**</entry>

<entry key="**node-replacement**">**1**</entry>

.

</node2>

<node3>

<entry key="**mac-address**">**00-4c-ce-df-5e-e2**</entry>

</node3>

10.3.2.2 Node Section

system-root.password

Encrypted password

<entry key="**system-root.password**">[encrypted password]</entry>

mac-address

MAC address of the server.

Example:

<entry key="**mac-address**">14-fe-b5-db-b2-82</entry>

customer-interface

Network interface for Customer LAN (e.g. eth0).

Example:

<entry key="**customer-interface**">eth0</entry>

corosync-interface

Network interface for Corosync LAN (e.g. eth4).

Example:

<entry key="**corosync-interface**">eth4</entry>

system-route.destination.0

IP address or IP address/Prefix length

Increment the index when more routes are configured (e.g. system-route.destination.1).

For more information please refer to Section 10.3.3.4, "Route Configuration Rules".

system-route.via.0

IP address

Increment the index when more routes are needed (e.g. system-route.via.1).

For more information please refer to Section 10.3.3.4, "Route Configuration Rules".

system-route.dev.0

Network interface (e.g. eth0)

Increment the index when more routes are needed (e.g. system-route.dev.1).

For more information please refer to Section 10.3.3.4, "Route Configuration Rules".

eth0.ip.0

dhcp or IP address/Prefix length

Increment the index when more IP addresses are configured (e.g. eth0.ip.1).

Interface name: eth[0-9]

Example:

<entry key="**eth0.ip.0**">218.1.17.41/26</entry>

<entry key="**eth0.ip.1**">145.23.23.12/24</entry>

<entry key="**eth0.ip.2**">172.17.3.39/16</entry>

For more information please refer to Section 10.3.3.3, "Interface Configuration Rules".

eth0.hostname.0

Host name

Increment the index when more IP addresses are configured (e.g. eth0.hostname.1).

Interface name: eth[0-9]

Example:

<entry key="**eth0.hostname.0**">SIMPLEX-PCI44</entry>

<entry key="**eth0.hostname.1**">SIMPLEX-PCI44-IPDA</entry>

For more information please refer to Section 10.3.3.3, "Interface Configuration Rules".

eth0.domainname.0

Domain name

Increment index when more IP addresses are configured (e.g. eth0.domainname.1).

Interface name: eth[0-9]

Example:

<entry key="**eth0.domainname.0**">eth0.com</entry>

<entry key="**eth0.domainname.1**">SIMPLEX-PCI44-IPDA</entry>

For more information please refer to Section 10.3.3.3, "Interface Configuration Rules".

eth0.speed-duplex

Bit rate of ethx interface

This tag is used for hardware configuration of the network devices and can be configured for every interface with different values.

Example:

<entry key="**eth0.speed-duplex**">100-full</entry>

Possible values:

- The first value configures the speed of interface in Mbit/s
  - 10
  - 100
  - 1000 (for a GB Interface)

- The second value defines the duplex transmission:
  - full
  - half

NOTICE: If this tag is not existing, the interface will be started in autonegotiation mode.

---

bond0.dev.0

Interface 1

Increment the index when more IP addresses are configured (e.g. bond0.dev.1).

Example:

<entry key="**bond0.dev.0**">eth0</entry>

<entry key="**bond0.dev.1**">eth1</entry>

For more information please refer to Bond Interface Rules.

bond0.ip.0

dhcp or IP address/Prefix length

Increment the index when more IP addresses are configured (e.g. bond0.ip.1).

Example:

<entry key="**bond0.ip.0**">0.0.0.0/0</entry>

For more information please refer to IP 0.0.0.0/0 Rules and Bond Interface Rules.

bond0.hostname.0

Host name

Increment the index when more IP addresses are configured (e.g. bond0.hostname.1).

Example:

<entry key="**bond0.hostname.0**">bond0</entry>

For more information please refer to Bond Interface Rules.

bond0.domainname.0

Domain name

Increment the index when more IP addresses are configured (e.g. bond0.domainname.1).

Example:

<entry key="**bond0.domainname.0**">bond0.com</entry>

For more information please refer to Bond Interface Rules.

bond0.speed-duplex

Bit rate of bond

All Bonding slave devices are used with the same configuration. It is not necessary to add XML tags for bonding slaves additionally.

Example:

<entry key="**eth0.speed-duplex**">100-full</entry>

Possible values:

- The first value configures the speed of interface in Mbit/s
  - 10
  - 100
  - 1000 (for a GB Interface)

- The second value defines the duplex transmission:
  - full
  - half

> **NOTICE:** If this tag is not existing, the interface will be started in autonegotiation mode.

vlan<vlanid>.dev

Interface

Example:

<entry key="**vlan1031.dev**">bond1</entry>

<entry key="**vlan1127.dev**">bond0</entry>

For more information please refer to VLAN Interface Rules.

vlan<vlanid>.id

VLAN ID number

For each VLAN ID an entry must be configured.

Example:

<entry key="**vlan1031.id**">1031</entry>

<entry key="**vlan1127.id**">1127</entry>

For more information please refer to VLAN Interface Rules.

vlan<vlanid>.ip.0

dhcp or IP address/Prefix length

For each VLAN ID an entry must be configured.

Example:

<entry key="**vlan1031.ip.0**">10.7.17.108/19</entry>

<entry key="**vlan1127.ip.0**">10.7.117.108/19</entry>

For more information please refer to VLAN Interface Rules.

vlan<vlanid>.hostname.0

Host name

For each VLAN ID an entry must be configured.

Example:

<entry key="**vlan1031.hostname.0**">PCI07-APE17-IPDA</entry>

<entry key="**vlan1127.hostname.0**">PCI07-APE17</entry>

For more information please refer to VLAN Interface Rules.

vlan<vlanid>.domainname.0

Domain name

For each VLAN ID an entry must be configured.

Example:

<entry key="**vlan1031.domainname.0**">vlan1031.com</entry>

<entry key="**vlan1127.domainname.0**">vlan1127.com</entry>

For more information please refer to VLAN Interface Rules.

system-delete.ip

IP address/Prefix length of the IP address you want to delete from the system.

Example:

<entry key="**system-delete.ip**">192.168.0.2/24</entry>

customer-ntp.server.0

IP address or name of the Network Time Protocol (NTP) sevrer.

Example:

<entry key="**customer-ntp.server.0**">**ntp1.ptb.de**</entry>

<entry key="**customer-ntp.server.1**">**ntps1-0.uni-erlangen.de**</entry>

<entry key="**customer-ntp.server.2**">**187.168.2.22**</entry>

- Index number 0 is mandatory, the following indexes can be given optionally (e.g. customer-ntp.server.1, customer-ntp.server.2).
- The first entry with the index number 0 is the preferred server.

customer-timezone

Time zone configuration

Examples:

<entry key="**customer-timezone**">**Europe/Berlin**</entry>

<entry key="**customer-timezone**">**America/Los_Angeles**</entry>

<entry key="**customer-timezone**">**Asia/Kuala_Lumpur**</entry>

The time zone variables are all given through the directory structure /usr/share/zoneinfo

Possible values: see Section 10.3.5, "Time Zone Values".

customer-keyboard-layout

Keyboard layout configuration

Example:

<entry key="**customer-keyboard-layout**">**german**</entry>

Possible values:

arabic belgian canadian chinese croatian czech czech-qwerty danish dutch dvorak english-uk english-us estonian finnish french french-ca french-ch german german-ch german-deadkey greek hungarian icelandic italian japanese khmer korean lithuanian norwegian polish portugese portugese-br portugese-br-usa russian serbian slovak slovak-qwerty slovene spanish spanish-lat swedish taiwanese turkish ukrainian

customer-def.gw

IP address of the default gateway (e.g. 218.1.17.1)

Example:

<entry key="**customer-def.gw**">218.1.17.1</entry>

10.3.3 Rules

10.3.3.1 Simplex Deployment Dependent Rules

The script determines the Customer IP address through the parameter **customer-interface** index number 0.

The index number is the number at the end of parameter name **eth0.ip.0**.

The host name from the Customer LAN will be set as server host name.

10.3.3.2 Duplex/Separated Duplex Deployment Dependent Rules

The script compares the two/three given IP addresses with the one IP address, that is determined through the parameter **corosync-interface**. The IP address from the Corosync server must have the index number **0** on this interface. The index number is the number at the end of the parameter name **eth1.ip.0**.

By this way, also the own server is determined and its host name will be set as server host name.

The script checks also the following conditions in this deployment:

- Checks if all two/three host names and IP addresses are different.
- Checks if the IP addresses are valid.
- Checks if the netmask entries are valid. The netmask is given through the prefix length at the end of each IP address, which is in this case **24**. **24** corresponds to the netmask 255.255.255.0. A list for all 32 prefix lengths and corresponding netmasks is given at the end of this document (Section 10.3.4, "Netmask and Prefix Length").
- Checks if all Corosync IP addresses are configured in the same subnet.

10.3.3.3 Interface Configuration Rules

An interface configuration section includes the following lines.

<entry key="**eth0.ip.0**">**192.168.0.72/24**</entry>

<entry key="**eth0.hostname.0**">**first-host**</entry>

<entry key="**eth0.domainname.0**">**site.com**</entry>

Every interface configuration must have at least an IP address for **eth0.ip.0**. If there is no valid value entered for **eth0.hostname.0** and **eth0.domainname.0** or the lines itself are not existent the respective lines will be ignored (see example above).

It is possible to enter **dhcp** instead of an IP address, when you want to get your IP address through a DHCP server.

<entry key="**eth0.ip.0**">**dhcp**</entry>

eth0.hostname.0 and **eth0.domainname.0** will be ignored in this case.

IMPORTANT: DHCP can be configured only on the IP index 0.

IMPORTANT: DHCP is only supported for Standalone SoftGates and Survivable SoftGates.

IMPORTANT: DHCP must not be used on Host System (nodeA, nodeB, quorum) nodes.

On the same device additional IP addresses can be configured:

<entry key="**eth0.ip.0**">**dhcp**</entry>

<entry key="**eth0.ip.1**">**192.168.1.45/24**</entry>

<entry key="e**th0.hostname.1**">**host1**</entry>

<entry key="**eth0.domainname.1**">**site.com**</entry>

<entry key="**eth0.ip.2**">**10.35.44.45/24**</entry>

<entry key="**eth0.hostname.2**">**host2**</entry>

<entry key="**eth0.domainname.2**">**site2.com**</entry>

The domain name part will be determined from the host name and the domain name. In this example here, the following lines will be added to the /etc/hosts file.

192.168.1.45	host1.site.com	host1
10.35.44.45	host2.site2.com	host2

The first part of this parameter defines the interface itself and can have the following values:

eth0 ---- eth[numerical]

vlan0 ---- vlan[numerical]

bond0 ---- bond[numerical]

IMPORTANT: The identifier **eth**, **vlan** and **bond** are mandatory. The numerical part can be every number if it is a **vlan** or **bond**. In case of **eth** device, the given interface number must be really existent in the system.

The number at the end of the parameter name, in this example **0** (zero), identifies the IP index number. The number **0** is used for the main IP address of this Interface, other addresses are secondary IP addresses.

Following an example for this.

<entry key="**eth0.ip.0**">**192.168.0.72/24**</entry>

<entry key="**eth0.hostname.0**">**host0**</entry>

<entry key="**eth0.domainname.0**">**site0.com**</entry>

<entry key="**eth0.ip.1**">**192.168.0.74/24**</entry>

<entry key="**eth0.hostname.1**">**host1**</entry>

<entry key="**eth0.domainname.1**">**site1.com**</entry>

<entry key="**eth0.ip.2**">**192.168.0.76/24**</entry>

<entry key="**eth0.hostname.2**">**host2**</entry>

<entry key="**eth0.domainname.2**">**site2.com**</entry>

In this configuration the following IP addresses will be configured on the eth0 interface.

eth0	192.168.0.72	Netmask: 255.255.255.0	Broadcast: 192.168.1.255
eth0:1	192.168.0.74	Netmask: 255.255.255.0	Broadcast: 192.168.1.255
eth0:2	192.168.0.76	Netmask: 255.255.255.0	Broadcast: 192.168.1.255

Netmask and broadcast will be calculated from the given IP address and prefix length.

Every Interface must have a main IP address, which is determined from the number **0** (zero) at the end of the parameter name. if the ip index 0 line is not existent, the next IP address will be used as the main IP address. In the example below, the IP Address 192.168.0.74 will be set as main IP address.

<entry key="**eth0.ip.1**">**192.168.0.74/24**</entry>

<entry key="**eth0.ip.2**">**192.168.0.76/24**</entry>

- IP addresses and netmasks will be checked for validity, the broadcast will be calculated from these two values.
- IP addresses will be checked against double input, the script stops in this case unless one of them is configured as **ip to delete**.
- You can configure one or more IP addresses fro removing from the system (see Section 10.3.2, "Possible Parameters and their Values" > system-delete.ip).

IP 0.0.0.0/0 Rules

If the first IP address is configured as **0.0.0.0/0**, all the following configurations on this device will be ignored.

In the following configuration the IP addresses number 1 and 2 (second anf third line) will be ignored.

<entry key="**eth0.ip.0**">**0.0.0.0/0**</entry>

<entry key="**eth0.ip.1**">**192.168.0.74/24**</entry>

<entry key="**eth0.ip.2**">**192.168.0.76/24**</entry>

IP address **0.0.0.0/0** must be configured as the main address with suffix **0** (zero). Otherwise it will be ignored.

In the following configuration example the IP address number 1 (second line) will be ignored:

<entry key="**eth0.ip.0**">**192.168.0.72/24**</entry>

<entry key="**eth0.ip.1**">**0.0.0.0/0**</entry>

Bond Interface Rules

A bond interface can be configured on any not configured eth device. That means, the corresponding eth device must be free from any IP configuration. It is also not possible to configure a bond interface on an eth device, which is allocated as vlan device.

Here is a possible bond configuration.

<entry key="**bond0.dev.0**">**eth2**</entry>

<entry key="**bond0.dev.1**">**eth4**</entry>

<entry key="**bond0.ip.0**">**192.168.1.51/24**</entry>

<entry key="**bond0.hostname.0**">**bond0**</entry>

<entry key="**bond0.domainname.0**">**bond0.com**</entry>

<entry key="**bond0.ip.1**">**192.168.1.53/24**</entry>

<entry key="**bond0.hostname.1**">**bond0-1**</entry>

<entry key="**bond0.domainname.1**">**bond0.com**</entry>

<entry key="**bond1.dev.0**">**eth5**</entry>

<entry key="**bond1.dev.1**">**eth3**</entry>

<entry key="**bond1.ip.0**">**0.0.0.0/0**</entry>

If the bond interface has no IP address configured, so this bond interface will be initialized with IP address **0.0.0.0/0** and started.

The following is an example for this.

<entry key="**bond0.dev.0**">**eth2**</entry>

<entry key="**bond0.dev.1**">**eth4**</entry>

In this example, bond interface **bond0** with the slave devices **eth2** and **eth4**, will be initialized with IP address **0.0.0.0/0** and started afterwards. The given host name and domain name will be ignored in this case.

VLAN Interface Rules

A virtual LAN can be configured on any device including bond interfaces, but not on an eth interface, which is allocated already from a bond interface.

The VLAN ID must not be the same as the VLAN interface name, but it should be same for YaST compatibility.

Here is a possible VLAN configuration.

<entry key="**vlan4.dev**">**eth7**</entry>

<entry key="**vlan4.id**">**4**</entry>

<entry key="**vlan4.ip.0**">**192.168.1.68/24**</entry>

<entry key="**vlan4.hostname.0**">**vlan4-0**</entry>

<entry key="**vlan4.domainname.0**">**vlan4.com**</entry>

<entry key="**vlan4.ip.1**">**192.168.1.64/24**</entry>

<entry key="**vlan4.hostname.1**">**vlan4-1**</entry>

<entry key="**vlan4.domainname.1**">**vlan4.com**</entry>

<entry key="**vlan7.dev**">**bond0**</entry>

<entry key="**vlan7.id**">**7**</entry>

<entry key="**vlan7.ip.0**">**192.168.1.88/24**</entry>

<entry key="**vlan7.hostname.0**">**vlan7-0**</entry>

<entry key="**vlan7.domainname.0**">**vlan7.com**</entry>

<entry key="**vlan7.ip.1**">**192.168.1.86/24**</entry>

<entry key="**vlan7.hostname.1**">**vlan7-1**</entry>

If the VLAN interface has no IP address configured, so this VLAN interface will be initialized with the IP address **0.0.0.0/0** and started.

The following is an example for this.

<entry key="**vlan4.dev**">**eth2**</entry>

<entry key="**vlan4.id**">**4**</entry>

In this example, the VLAN interface **vlan4** with the slave device **eth2** and the VLAN ID **4**, will be initialized with the IP address **0.0.0.0/0** and started afterwards. The given host name and domain name will be ignored in this case.

10.3.3.4 Route Configuration Rules

Routes can be configured with the following tags.

- Route destination is a single host:

<entry key="**system-route.destination.0**">**192.56.76.0**</entry>

- Route destination is a network:

<entry key="**system-route.destination.0**">**192.56.76.0/24**</entry>

The following tags can be configured additionally:

<entry key="**system-route.via.0**">**192.168.0.1**</entry>

<entry key="**system-route.dev.0**">**eth0**</entry>

All routes that are configured on the Customer LAN interface will be added also into the OpenScape 4000 special route tables.

10.3.4 Netmask and Prefix Length

Table 37: Netmask and prefix length dependency on an IPv4 system

1	128.0.0.0	192.0.0.0	224.0.0.0	240.0.0.0	4
5	248.0.0.0	252.0.0.0	254.0.0.0	255.0.0.0	8
9	255.128.0.0	255.192.0.0	255.224.0.0	255.240.0.0	12
13	255.248.0.0	255.252.0.0	255.254.0.0	255.255.0.0	16
17	255.255.128.0	255.255.192.0	255.255.224.0	255.255.240.0	20
21	255.255.248.0	255.255.252.0	255.255.254.0	255.255.255.0	24
25	255.255.255.128	255.255.255.192	255.255.255.224	255.255.255.240	28

29	255.255.255.248	255.255.255.252	255.255.255.254	255.255.255.255	32

10.3.5 Time Zone Values

Africa/

Abidjan Asmara Banjul Bujumbura Conakry Douala Harare Kigali

Lome Malabo Mogadishu Niamey Sao_Tome Windhoek Accra Asmera

Bissau Cairo Dakar El_Aaiun Johannesburg Kinshasa Luanda Maputo

Monrovia Nouakchott Timbuktu Addis_Ababa Bamako Blantyre Casablanca Dar_es_Salaam

Freetown Kampala Lagos Lubumbashi Maseru Nairobi Ouagadougou Tripoli

Algiers Bangui Brazzaville Ceuta Djibouti Gaborone Khartoum Libreville

Lusaka Mbabane Ndjamena Porto-Novo Tunis

America/

Adak Barbados Catamarca Dawson_Creek Goose_Bay Inuvik Managua Monterrey

Pangnirtung Resolute St_Kitts Virgin Anchorage Belem Cayenne Denver

Grand_Turk Iqaluit Manaus Montevideo Paramaribo Rio_Branco St_Lucia Whitehorse

Anguilla Belize Cayman Detroit Grenada Jamaica Marigot Montreal

Phoenix Rosario St_Thomas Winnipeg Antigua Blanc-Sablon Chicago Dominica

Guadeloupe Jujuy Martinique Montserrat Port-au-Prince Santa_Isabel St_Vincent Yakutat

Araguaina Boa_Vista Chihuahua Edmonton Guatemala Juneau Matamoros Nassau

Port_of_Spain Santarem Swift_Current Yellowknife Argentina Bogota Coral_Harbour Eirunepe

Guayaquil Kentucky Mazatlan New_York Porto_Acre Santiago Tegucigalpa

Aruba Boise Cordoba El_Salvador Guyana Knox_IN Mendoza Nipigon

Porto_Velho Santo_Domingo Thule Asuncion Buenos_Aires Costa_Rica Ensenada Halifax

La_Paz Menominee Nome Puerto_Rico Sao_Paulo Thunder_Bay Atikokan Cambridge_Bay

Cuiaba Fort_Wayne Havana Lima Merida Noronha Rainy_River Scoresbysund

Tijuana Atka Campo_Grande Curacao Fortaleza Hermosillo Los_Angeles Mexico_City

North_Dakota Rankin_Inlet Shiprock Toronto Bahia Cancun Danmarkshavn Glace_Bay

Indiana Louisville Miquelon Ojinaga Recife St_Barthelemy Tortola

Bahia_Banderas Caracas Dawson Godthab Indianapolis Maceio Moncton Panama

Regina St_Johns Vancouver

America/Argentina/

Buenos_Aires Catamarca ComodRivadavia Cordoba Jujuy La_Rioja Mendoza Rio_Gallegos Salta

San_Juan San_Luis Tucuman Ushuaia

America/Indiana/

Indianapolis Knox Marengo Petersburg Tell_City Vevay Vincennes Winamac

America/Kentucky/

Louisville Monticello

America/North_Dakota/

Center New_Salem

Antarctica/

Casey Davis DumontDUrville Macquarie Mawson McMurdo Palmer Rothera South_Pole Syowa Vostok

Arctic/

Longyearbyen

Asia/

Aden Ashkhabad Bishkek Dacca Harbin Jayapura Katmandu Macau

Novosibirsk Qyzylorda Sakhalin Tbilisi Ulaanbaatar Yerevan Almaty Baghdad

Brunei Damascus Ho_Chi_Minh Jerusalem Kolkata Magadan Omsk Rangoon

Samarkand Tehran Ulan_Bator Amman Bahrain Calcutta Dhaka Hong_Kong

Kabul Krasnoyarsk Makassar Oral Riyadh Seoul Tel_Aviv Urumqi

Anadyr Baku Choibalsan Dili Hovd Kamchatka Kuala_Lumpur Manila

Phnom_Penh Riyadh87 Shanghai Thimbu Vientiane Aqtau Bangkok Chongqing

Dubai Irkutsk Karachi Kuching Muscat Pontianak Riyadh88 Singapore

Thimphu Vladivostok Aqtobe Beijing Chungking Dushanbe Istanbul Kashgar

Kuwait Nicosia Pyongyang Riyadh89 Taipei Tokyo Yakutsk Ashgabat

Beirut Colombo Gaza Jakarta Kathmandu Macao Novokuznetsk Qatar

Saigon Tashkent Ujung_Pandang Yekaterinburg

Atlantic/

Azores Bermuda Canary Cape_Verde Faeroe Faroe Jan_Mayen Madeira Reykjavik South_Georgia

St_Helena Stanley

Australia/

ACT Brisbane Canberra Darwin Hobart Lindeman Melbourne North Queensland Sydney

Victoria Yancowinna Adelaide Broken_Hill Currie Eucla LHI Lord_Howe NSW Perth

South Tasmania West

Brazil/

Acre DeNoronha East West

Canada/

Atlantic Central East-Saskatchewan Eastern Mountain Newfoundland Pacific Saskatchewan Yukon

Chile/

Continental EasterIsland

Etc/

GMT GMT+1 GMT+11 GMT+2 GMT+4 GMT+6 GMT+8 GMT-0 GMT-10 GMT-12 GMT-14 GMT-3 GMT-5 GMT-7

GMT-9 Greenwich UTC Zulu GMT+0 GMT+10 GMT+12 GMT+3 GMT+5 GMT +7 GMT+9 GMT-1 GMT-11 GMT-13

GMT-2 GMT-4 GMT-6 GMT-8 GMT0 UCT Universal

Europe/

Amsterdam Belgrade Bucharest Dublin Isle_of_Man Kiev Luxembourg Minsk Oslo

Riga Sarajevo Stockholm Uzhgorod Vilnius Zaporozhye Andorra Berlin Budapest Gibraltar Istanbul Lisbon Madrid Monaco Paris Rome Simferopol Tallinn Vaduz Volgograd Zurich Athens Bratislava Chisinau Guernsey Jersey Ljubljana Malta Moscow Podgorica Samara Skopje Tirane Vatican Warsaw Belfast Brussels Copenhagen Helsinki Kaliningrad London Mariehamn Nicosia Prague San_Marino Sofia Tiraspol Vienna Zagreb

Indian/

Antananarivo Chagos Christmas Cocos Comoro Kerguelen Mahe Maldives Mauritius Mayotte Reunion

Mexico/

BajaNorte BajaSur General

Mideast/

Riyadh87 Riyadh88 Riyadh89

Pacific/

Apia Chuuk Enderbury Funafuti Guadalcanal Johnston Kwajalein Midway Norfolk Palau

Ponape Saipan Tarawa Wake Auckland Easter Fakaofo Galapagos Guam Kiritimati Majuro Nauru Noumea Pitcairn Port_Moresby Samoa Tongatapu Wallis Chatham Efate Fiji Gambier Honolulu Kosrae Marquesas Niue Pago_Pago Pohnpei Rarotonga Tahiti Truk Yap

US/

Alaska Aleutian Arizona Central East-Indiana Eastern Hawaii Indiana-Starke Michigan Mountain Pacific Pacific-New Samoa

11 Appendix C: Bonds and VLAN Configuration

Bond and VLAN system configuration must be performed via firstinst-netw.sh and reconfiguration via the Recovery/Reconfiguration tool **recover-H4K.sh** (in the directory `/opt/soco-common`). No other method e.g. YAST is supported. For more information on the Recovery/Reconfiguration Tool please refer toSection 6.3, "Recovery/Reconfiguration Tool".

IMPORTANT: YAST does not display Bond complete configuration due to YAST internal design, however there is no problem with Bond functionality. Bond configuration/status should therefore be checked via typical Linux commands like: "cat /proc/net/bonding/bond0" or "ip addr show bond0". Furthermore, please note when setting Duplex or Interface Speeds for a Bond (e.g. via First Installation XML), they must be configured for each of the Bond eth port slaves and not for the Bond itself.

11.1 Bond Configuration

IMPORTANT: Do not erase eth0 LAN interface at this moment or else after reboot you will not be able to access the default address of the OpenScape 4000 Platform Administration (Portal) (https://192.168.0.3). eth0 can be erased and added to the Customer bond after LAN Wizard configuration from OpenScape 4000 Platform Administration (Portal) has been completed.

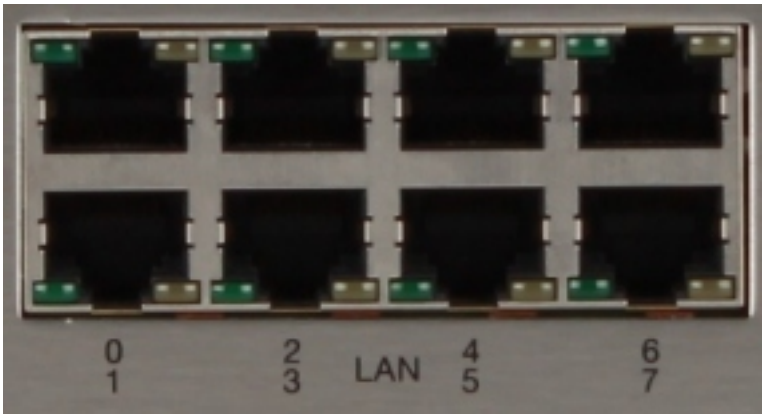


Figure 167: Ethernet interfaces of EcoServer

There are no recommendations for eth assignement for EcoServer hardware.

Notes:

- For **Duplex and Separated Duplex deployments bond names** (e.g. bond0) **have to be consistent on node1 and node2** (e.g. If bond0 was created for Customer LAN on node1 then bond0 must be assigned to Customer LAN in node2 as well).
- The type of Bond used is active-backup (Mode 1)

- This mode places one of the interfaces into a backup state and will only make it active if the link is lost by the active interface. Only one slave in the bond is active at an instance of time. A different slave becomes active only when the active slave fails. This mode provides fault tolerance.

11.2 Atlantic configuration

There are two options for configuring the two Atlantic (ATLT) LAN interfaces:

- Leave the interfaces bridged if you need ATLT access from an external TAP/PC or some other application, which is the default.

  IMPORTANT: In this case one and only one interface can be used for CCA/CCB connection.

  NOTICE: If both interfaces are connected to the corresponding two interfaces on the second EcoServer or all interfaces are connected to LAN switch, then you will have network loops.

- Make a bond out of the two ATLT interfaces if you prefer redundancy, but here no port is available as a standard to connect to the ATLT.

12 Appendix D: How to Create a XML File Automatically

It is possibe to create the XML file with the configuration data that is needed for the first installation script automatically.

Execute the script using the option -w:

#./var/opt/firstinstall/firstinst-netw.sh -w

or

#cd /var/opt/firstinstall/

#./firstinst-netw.sh -w

Depending on the deployment the following XML files will be generated in the directory **/var/opt/firstinstall**:

- firstinst-netw-<hostname>-<mac_address_of_eth0>.xml - used for First Installation (e.g.firstinst-netw-PCI06A-00-20-ce-f1-36-c8.xml)
- haipsetup.xml - used only for debugging in case of errors

For more information on the command line options of the first installation script see First Installation Script - Command Line Options.

13 Appendix E: Frequently asked Questions (FAQs)

13.1 Connectivity and Installation

13.1.1 Connectivity

1) Question: USB 1 looks like slave USB-controller. Is it supported at the moment? How can I use it?

Answer: Please see the `DriversAndTools\USB_Driver \USB_INSTALL_README.txt` on installation .iso file for connection details.

2) Question: Is it mandatory USB-docking station to have power adapter or does EcoServer provide enough power for external hard disk via USB?

Answer: Docking stations with their own power adapters have been preferred. This way we can be more generic and flexible. For more details please refer to the hardware section in the System Components' documentation.

3) Question: Is a USB-hub supported?

Answer: Yes if the power consumption is not exceed the USB port specification, but it is preferred to have externally powered USB devices to avoid power issues. Two USB host ports (USB 2.0 high speed) are available on the front panel. The USB controller device is part of the chipset. The +5V of the two USB host ports are protected with one electronic 1A fuse (Texas Instruments TPS2032) and because of UL with a second 2.5A melting fuse (size 0603) in series. So a 2,5" USB hard disk may be fully bus powered, even if it needs slightly more current as allowed by USB specifications, on the other port less power should be used.

4) Question: I am trying to connect with FTP in OpenScape 4000, but it is not working. What did you break?

Answer: Both Telnet and FTP are removed for security reasons. As those protocols transmit passwords in clear text they are a security issue. SSH and SFTP replace those forms of connection and are secure.

5) Question: The customer wants a Separated Duplex system. Can all systems be in different networks?

Answer: Corosync addresses on all 3 nodes should be in the same subnet. This is a L2 redundant cluster where all 3 nodes are connected over a gigabit switch or dark fiber switch.

6) Question: We want to force ADP/OpenScape 4000 Assistant/CSTA to run on the partner node and restarting the active node does not seem to work. Why?

Answer: To ensure only one node is running the relevant VMs a timer of 5 minutes is started before a switchover is initiated. The timer is there to prevent problems with both nodes being active together (so called split brain operation).

7) Question: I understand from the Feature Description two of the three nodes from a Separated Duplex deployment must always see each other to

ensure operation. Should two nodes fail is there anything I can do to ensure telephony is working.

Answer: Visibility of two nodes over the Corosync LAN are needed to ensure there is no "split brain" situation i.e. that both Node1 and Node2 try to take control of the same resources. Of course when any of the two nodes are available it is possible to automatically negotiate which Node is the master. When no Node can see each other an Administrator can decide to manually start one telephony Node using the command "standalone_operation enable" from the Platform SSH. The alternative command "standalone_operation disable" must be explicitly executed once operation node connectivity is restored.

13.1.2 Installation and Upgrades

1) Question: Is there any way to completely reinstall the already installed EcoServer-based system from the very beginning without using an USB stick.

   Answer: You can use RAR to reinstall some deployments. See RAR feature description for details.

2) Question: The parameter **BITRATE** in AMO SIPCO is no longer supported in HiPath 4000 V6 R2 and later versions. Where and how to set the needed LAN speed for the CCA/B LAN interface?

   Answer: The parameter was used in the past for HG3570 and CCA/B. Today it has effect only on HG3570. The bitrates for CCA/B are not configurable anymore as they don't connect physically to the LAN Network. The ports connect to a logical bridge in the Linux and therefore the admin has no need to configure them. This is all done in the background when the CCA/B VM is set up. From HiPath 4000 V6 R2 the only official way to configure/reconfigure LAN interfaces is using the firstinstall XML. The XML file is used during first installation or when calling *recovery.sh* (see Section 2.2.3, "Installation and OpenScape 4000 Configuration" or Section , "Changing Platform Configuration" for further details). **TOSSIGNL** however is still configurable in AMO only for CCA/B.

3) Question: What is the functionality of the parameter **VLAN** in AMO SIPCO in OpenScape 4000 and where and how to set the needed VLAN information for the CCA/B LAN interface?

   Answer: The parameter was used in the past for HG3570 and CCA/B, but today it has effect only on HG3570. To configure VLAN for CCA/CCB port please use the XML file with known first installation or recovery methods. **TOSSIGNL** is still configurable in AMO only for CCA/B.

4) Question: Keyboard type selection required at start of USB-Install.

   Answer: Keyboard configuration can be made in the XML file by adding the corresponding parameter (see Section 10.3.2, "Possible Parameters and their Values" > customer-keyboard-layout).

5) Question: Is there a soft procedure to swap the ADP from one processor to another?

   Answer: No, reboot the processor running the ADP.

   NOTICE: Only a shutdown of the node where ADP is running will lead to the ADP starting on the partner node after 5 minutes

6) Question: Can I clone one system and install another with this clone? Or should we install each system from the image individually?

   Answer: Each installation should be an individual installation.

7) Question: Is bonding supported in OpenScape 4000?

   Answer: Yes. The only official way to configure/reconfigure LAN interfaces is using the firstinstall XML. The XML file is used during first installation or when calling *recovery.sh* (see Chapter 11, "Appendix C: Bonds and VLAN Configuration" for further details).

8) Question: How is the RAID used in OpenScape 4000?

   Answer: Starting with V10R1, the RIGHT functionality is available on both Node 1 and Node 2, in case of Separated Duplex/ Duplex.

   Information which HD / SSD can be removed from the raid can be found on the LCD display of the system (and virtual LCD in portal). For information of the DSCL2+ display please refer to the hardware description of the DSCL2+ board in **OpenScape 4000, Volume 2: System Components (Hardware, Software)**.

   Data replication from Node 1 to Node 2 is done via DRBD.

9) Question: How can IP configuration be changed?

   Answer: From HiPath 4000 V6 R2 the only official way to configure/ reconfigure LAN interfaces is using the firstinstall XML. The XML file is used during first installation or when calling *recovery.sh* (see Section 2.2.3, "Installation and OpenScape 4000 Configuration" or Chapter 6, "Changing Platform Configuration" for further details).

10) Question: The customer wants to separate the Duplex Nodes via long cables, but is not interested in using the Quorum -can that be done?

    Answer: No. OpenScape 4000 Duplex active signals are signalled via the cross-connect cable, therefore if it is wanted to physically separate the duplex nodes, then a Separated Duplex deployment is needed.

11) Question: The customer wants to migrate a Seperated Duplex from one minor release R1 to R2 on Servers, can the standalone operation switch be used to minimise downtime the upgrade?

    Answer: The known switch "standalone_operation enable" can be used and it works instantly, so it should not be executed on a partner standby node. For minimal loss of telephone the following sequence is correct:

    a) Switch RMX SWU to be active on Node 2 (CCB).

    - Shutdown Node 1 (CCA) -OpenScape 4000 Assistant, CSTA, ADP will now start on Node 2 (CCB if not already running).
    - Active the mentioned standalone switch in Node 2 (CCB).
    - Shutdown Quorum (CCQ).
    - Perform new installation of Node 1 and Quorum ensuring they are not connected via the network to Node 2 (CCB).
    - After new Node 1 and Quorum are installed, shutdown Node 2 and disconnect relevant Node 2 network cables.
    - Connect IPDA cables to new Node 1 (CCA) -effectively RMX reload.
    - Now perform new installation of Node 2 (CCB) and then reconnect networks cables to finish synchronisation.

12) **Question**: I executed the XML script on an old OpenScape 4000 SoftGate and didn't get the OpenScape 4000 Platform Administration (Portal) IP address. Then I used the generated XML file to install the OpenScape 4000 SoftGate.

    Now I have no OpenScape 4000 Platform Administration (Portal) IP address, how can I access OpenScape 4000 Platform Administration (Portal) for OpenScape 4000 SoftGate configuration?

    Answer: You can access the OpenScape 4000 Platform Administration (Portal) on the physical address: `https://physical_IP_address/`

    Complete the installation of the OpenScape 4000 SoftGate and press **Submit**.

    From this point in time on, you can access the vNCUI WBM over:

    https://vNCUI/

    and you can access the OpenScape 4000 Platform Administration (Portal) over:

    https://vNCUI:8443/

    https://physical_ip_address:8443/

13) **Question**: I want to have an independent IP address for OpenScape 4000 Platform Administration (Portal) access on standalone OpenScape 4000 SoftGate. How can I do this?

    Answer: Add the following line in your XML file under the **<common>** section:

    <entry key="customer-portal.ip">10.13.68.36/21</entry>

    IMPORTANT: It is recommended that this address is the same as the Customer IP address you configure on Customer interface in the **<node1>** section. However if you prefer to have a separate IP address then it must be in the

same subnet as the Customer IP address you configure on Customer interface in the **<node1>** section.

14) Question: I am using a board from another customer and I am concerned about the BIOS settings. How can I ensure the correct settings?

Answer: OpenScape 4000 HW is delivered with the correct BIOS settings as their defaults. Just perform a "Reset to Default" on our proprietary HW.

13.2 Backup and Restore

1) Question: How do we know which hard drive of the two to replace if there is a physical hard drive failure? Is "sda" always on the bottom of the stack?

Answer: The one which LED is not flashing. There is no other method of knowing.

2) Question: What recovery steps should be taken if SLES 15 boots, but the OpenScape 4000 will **NOT** boot, and the OpenScape 4000 Platform Administration (Portal) is not accessible?

Answer: Take a look at the */var/log/messages* file. Do `crm_mon -1 -f -A` to see resources.

3) Question: Do we have any back-door troubleshooting tools if the OpenScape 4000 Platform Administration (Portal) is not available?

Answer: Take a look at the */var/log/messages* file. Do `crm_mon -1 -f -A` to see resources.

4) Question: Version compatibility requirements when older VHD1/VHD2 files are copied back onto a newer version? ex:Backup VHD1/VHD2 files were done with OpenScape 4000 V10R0.28.0 and copied onto a Backup-server but in the mean time there were some Hotfixes installed the system has OpenScape 4000 V10R0.28.4 installed.

Answer: No problem, but know that -The RMX Hotfixes of OpenScape 4000 V10R0.28.4 have to be re-installed. Have a look at the Release Notes for any possible interrelationships between the different Hotfixes.

13.3 Hotfix installation

1) Question: Hotfix order of installation?

Answer: Normally there is no order in which they have to be implemented, unless of course it is mentioned in the release notes. However Platform Hotfixes, in case of duplex, require that the 2 processors are on-line as otherwise the activation will fail. The transfer is accepted but in the SWA the PLT HF is grayed out.

2) Question: Hotfix will become available in SWA once the 2nd processor is on-line?

Answer: Yes.

3) Question: Is the syncronization process an automated process and can it be stopped or manually started?

Answer: It is automated and it doesn't make sense to stop/start it as split upgrade is not implemented.

13.4 Time change / synchronization

1) Question: All upgraded systems have a less precise clock than previous versions and few minutes per week are very noticeable! An NTP solution is OK, but many of our customers do not have any accessible NTP from their OpenScape 4000 Customer LAN. Do they have another solution?

   Answer: No the NTP is a requirement in the RN and is described in the how-to's. Workaround if you need precise clock and easy way to administer the time is to change it manually via YAST. For manual changes check the TIME synchronization documentation and read carefully the procedure and restrictions (seeChapter 8, "Time Synchronization").
2) Question: Previous versions allowed easy time change via OpenScape 4000 Assistant. Now this is not possible.

   Answer: Customer should configure an NTP server via xml. No changes via Yast are allowed.
3) Question: How are the phones synchronizing when time is changing?

   Answer: The phones display time is synchronized once a day overnight. If SPE is active NTP is absolutely necessary.
4) Question: What is the time source in OpenScape 4000?

   Answer: The time concept is NTP. This is the default and normal concept in the server world. You could have NTP server on Linux machines, Windows machines; even some routers have reliable clocks. You could have NTP relays to traverse several subnets.
5) Question: There is no summer/winter time change in Russia anymore. The time will be changed to summer in March, after that no more changes should apply. How to stop time change in OpenScape 4000?

   Answer: Just set the correct time zone (UTC+3:00 i.e. "ETC/GMT -3", which has no DST) on OpenScape 4000 host and OpenScape 4000 Assistant, and it will work, because OpenScape 4000 Assistant is controlling the DST switchover.
6) Question: Synchronization with Windows SNTP server is not working, why?

   Answer: Windows does not include NTP by default. It runs Microsoft's implementation of SNTP, a stripped down version which lacks many of the features and safeguards included in the full implementation. Microsoft's version, unless it is very recent, does not comply with RFC-2030, the standard for SNTP. Systems running SNTP are not considered acceptable as servers unless they are connected to a hardware reference clock, such as a GPS Timing Receiver.
7) Question: In the internet it states Microsoft Servers can be configured to use NTP, is that correct and is it supported? Answer: Any stable true NTP source is supported. Microsoft provide their own knowledge article on how to configure Windows Server as an authoritative time server https://support.microsoft.com/en-us/kb/816042. In addition it is important to change the LocalClockDispersion from 10 to 0 to allow successful NTP synchronisation as described under https://technet.microsoft.com/en-us/library/cc782681%28v=ws.10%29.aspx?f=255&MSPPError=-2147217396

13.5 Licensing

1) Question: CSTA License information?

Answer: Max of 4 adapters can be configured. Max of 4 applications per adapter can be configured. There are three options for CAP licenses:

a) No License

Up to 100 Monitor ports

Unlimited License

Unify applications do not require licenses, only 3rd party applications do. The license is based on the MAC of the OpenScape 4000 system i.e. not the MAC of the CSTA VM and is imported through OpenScape 4000 Assistant.

IMPORTANT: There is no further need for a CSTA license.

---

2) Question: Is there any possibility of checking whether and which license is installed/used from GUI (i.e. not involving checking logs)?

Answer: This information is planned to be included and released in OpenScape 4000 in a future HF/FR/MR.

IMPORTANT: There is no further need for a CSTA License.

---

3) Question: When exchanging a EcoServer/server, is necessary for a new license?

Answer: Since V8, the licenses (Manager, Assistant, Softgate) will not be locked into MAC address of system where Central License Agent (CLA) is running.

13.6 Hardware failure

1) Question: If I have a hard disk hardware failure?

Answer: Any hard disk hardware failure needs to be reported to GVS.

2) Question: How hardened is SUSE SLES against power failures?

Answer: As good as the ext3 file system mechanism. This is a Linux platform system based on ext3 journaling file system. The Linux Platform is using default level of journalling which is the "medium risk".

14 Glossary

A

active node

The active node/processor is the node where ADP, OpenScape 4000 Assistant and OpenScape 4000 CSTA are running.

I

IP address of the host system

IP addresses which have to be used for the backup configuration in OpenScape 4000 Assistant.

S

Single node deployment

The following single node deployments are available: Simplex, Simplex with integrated SoftGate, Standalone SoftGate, Survivable SoftGate, Enterprise GW, Enterprise Gateway with integrated SoftGate, Survivable Enterprise GW, Survivable Enterprise GW with integrated SoftGate, APE (only until V10R0).

Survivable unit

Survivable unit refers to: Survivable SoftGate, Survivable Enterprise GW or APE deployments.

Index