A MITEL
PRODUCT
GUIDE

Unify OpenScape Enterprise Express

Migration from THIG to a non-THIG environment

Installation Guide

Installation Guide
07/2024

A31003-S5100-J100-02-7631

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

History of Changes

Issue	Date	Summary
1	04/2021	First issue of the guide.
2	02/2023	Added section: 4.5 Set new IP address for the SIP Server of Media Server

1 Introduction

This manual addresses system administrators who understand the described functions and processes and are familiar with OpenScape applications.

Based on the OSEE V9 (THIG) architecture and resource allocation, the same restrictions apply in terms of hardware and VM resources, even after the removal of the SBC-THIG.

The scope of this document is to provide steps to remove the SBC-THIG from the OSEE solution based on the basic automated provisioning of the solution that was performed during the initial deployment of the solution. Any updates or custom configuration must be modified accordingly.

The following instructions describe the steps that need to be executed to successfully remove the SBC-THIG from the OSEE solution. This manual applies for OSEE v9 and OSEE v10 (upgraded from OSEE v9) systems that include the SBC-THIG VM in the solution.

Once the migration procedure is completed, it is not possible to revert the solution back to the THIG environment.

In accordance to the installed OSEE solution (simplex or cluster), please follow the mandatory order, corresponding with the chapters below.

IMPORTANT : Please note this migration procedure will lead to system downtime

2 New IP schema design

Before proceeding with any action, the new IP schema of the solution must be defined, based on the Internal OSEE network (Design Guide v9 - App. A IP Schema)

IMPORTANT : Please note, that the migration process, described throughout this document, is based on the tables below that define the new IP schema. The OSEELAN fixed network (10.82.53.0/24) IP addresses will be replaced by a new set of IP addresses

2.1 OSEE with Simplex OSV

Note : It is highly recommended to re-use the SBC-THIG WAN IP address.

<table>
<tr><td colspan="4">OSEE with Simplex OSV</td></tr>
<tr><td>Component</td><td>Old IP address</td><td>New IP address</td><td>Comment</td></tr>
<tr><td>SBC-THIG</td><td>OLD_THIG_WAN_IP

Access SBC network</td><td>NEW_TMP_THIG_IP</td><td>Temporary new WAN IP address.
VM will be removed

SBC-THIG internal IPs are not affected</td></tr>
<tr><td rowspan="2">OSV</td><td>10.82.53.229

Management</td><td rowspan="2">NEW_OSV_IP

(Management & Signaling)</td><td rowspan="2">Set THIG WAN IP address as the new OSV IP address

NEW_OSV_IP = OLD_THIG_WAN_IP</td></tr>
<tr><td>10.82.53.231

Signaling</td></tr>
<tr><td>UC
OpenFire
CMP
Composer</td><td>10.82.53.233</td><td>NEW_UC_IP</td><td>New IP for the UC server</td></tr>
<tr><td>OSCC
OSCC-E
XPR</td><td>10.82.53.241</td><td>NEW_WIN_1_IP</td><td>New IP for the Windows 1 server</td></tr>
<tr><td>OSTM
DLS</td><td>10.82.53.249</td><td>NEW_WIN_2_IP</td><td>New IP for the Windows 2 server</td></tr>
</table>

2.2 OSEE with Cluster OSV

Note : It is highly recommended to re-use the SBC-THIG WAN IP addresses.

For OSEE with Cluster OSV, the three SBC-THIG WAN IP addresses will be re-used for OSV. An additional IP address is required in the same network with the SBC-THIG WAN IP addresses.

<table>
<tr><td colspan="4">OSEE with Cluster OSV</td></tr>
<tr><td>Component</td><td>Old IP address</td><td>New IP address</td><td>Comment</td></tr>
<tr><td rowspan="3">SBC-THIG 1

SBC-THIG 2</td><td>OLD_THIG_WAN_IP
(Virtual IP)

Access SBC network</td><td>-</td><td rowspan="3">Redundancy will be disabled.

Temporary new WAN IP address for SBC-THIG 1

SBC-THIG 2 will be powered off

VMs will be removed after migration is completed

SBC-THIG internal IPs are not affected</td></tr>
<tr><td>OLD_THIG_WAN_N1_IP

Access SBC network</td><td>NEW_TMP_THIG_IP</td></tr>
<tr><td>OLD_THIG_WAN_N2_IP

Access SBC network</td><td>-</td></tr>
<tr><td rowspan="2">OSV Node 1</td><td>10.82.53.229

Management</td><td>NEW_OSVN1_MGMT_IP

Management</td><td>Set THIG Node 1 WAN ip address as the new OSV node 1 management ip address

NEW_OSVN1_MGMT_IP
= OLD_THIG_WAN_N1_IP</td></tr>
<tr><td>10.82.53.231

10.82.53.236

Signaling</td><td>NEW_OSVN1_SIG_IP

Signaling</td><td>Set THIG Virtual WAN ip address as the new OSV node 1 signaling ip address

NEW_OSVN1_SIG_IP
= OLD_THIG_WAN_IP</td></tr>
<tr><td rowspan="2">OSV Node 2</td><td>10.82.53.230

Management</td><td>NEW_OSVN2_MGMT_IP

Management</td><td>Set THIG Node 2 WAN ip address as the new OSV node 2 management ip address

NEW_OSVN2_MGMT_IP
= OLD_THIG_WAN_N2_IP</td></tr>
<tr><td>10.82.53.232

10.82.53.237

Signaling</td><td>NEW_OSVN2_SIG_IP

Signaling</td><td>Set a new IP address
for NEW_OSVN2_SIG_IP.</td></tr>
<tr><td>UC</td><td rowspan="4">10.82.53.233</td><td rowspan="4">NEW_UC_IP</td><td rowspan="4">New IP for the UC server</td></tr>
<tr><td>OpenFire</td></tr>
<tr><td>CMP</td></tr>
<tr><td>Composer</td></tr>
<tr><td>OSCC</td><td rowspan="2">10.82.53.241</td><td rowspan="2">NEW_WIN_1_IP</td><td rowspan="2">New IP for the Windows 1 server</td></tr>
<tr><td>OSCC-E</td></tr>
</table>

XPR			
OSTM DLS	10.82.53.249	NEW_WIN_2_IP	New IP for the Windows 2 server

2.3 Media Server IP addresses

The default media server of the solution is running on the UC server (10.82.52.233)

Pending your solution setup, additional media servers might exist. To verify the internal IP address that corresponds to the external IP address, please follow the steps below :

1. Login to THIG → https://OLD_THIG_WAN_IP → Features → Remote Endpoints : Configure → Remote Endpoint Configuration table → Locate entries with "Type : MediaServer". If these Media Servers were configured on the webCDC project, remote endpoint "Name" contains site name set on webCDC. Each entry must be matched to an internal OSEELAN IP address (10.82.53.xxx)
2. **Navigate to Network/Net Services → Core realm Configuration → Note down all "*Non-VLAN IP*" IP addresses**. Number of "*Non-VLAN IP*" entries must be at least as many as "Media Server" type entries in Remote Endpoint Configuration table. If these Media Servers were configured on the webCDC project, the Network ID contains site name set on webCDC.

Note: In case, of manual addition and names set by administrator → identify the "Core realm profile" string set for the Media Server entry in "Remote Endpoint Configuration" table → locate the string from previous step in the "Realm Profile" table under "Network/Net Services" and identify the "Signaling Network ID" string and "Media Network ID" string → locate the string from previous step in the "Core realm Configuration" table in the "Network ID" column → identify IP address (type : "*Non-VLAN IP*")

Following the steps above, you have the following matches

Media server	Old IP address	New IP address
Default	10.82.53.233	NEW_UC_IP
Additional 1	OLD_MS1 10.82.53.1-220, 10.82.53.234, 10.82.53.235	NEW_MS1
Additional 2	OLD_MS2 10.82.53.1-220, 10.82.53.234, 10.82.53.235	NEW_MS2
.....	.....	.....

2.4 Optional IP addresses

Optional, depending on the webCDC project settings.

Component	Old IP address	New IP address
SESAP	10.82.53.251	NEW_SESAP_IP
Zenos GW	10.82.53.252	NEW_ZENOS_IP
External Survival Authority (SA)	10.82.53.238	NEW_SA_IP

Based on the OSEE Staging Guide (appendixes : Optional Direct Access to OSEE VMs, OpenScape Accounting V2 Configuration, Optional installation of an external OSCC-E server), it is possible that additional external IP addresses have been assigned to the SBC-THIG .

These IP addresses can be re-used in the new IP Schema table.

3 Migration overview

The migration procedure is divided in two sequential logical steps ;

1. Apply new IP address schema : set new IP addresses for all OpenScape VMs
2. Update application provisioning : update each application's provisioning to correspond the new IP schema

3.1 Prerequisites

- License files
  - New ALI for OSEE Windows 1 server
  - New ALI for UC server
  - New ALI for OSV server(s)
- Certificates (if current custom solution certificates are based on IP addresses)
- Snapshots of the all the VMs before continuing to the migration procedure
- Latest NCPE (based on your OSV version)
- (OSV Cluster only) Mandatory OSV software level if OSV node 1 hostname is a substring of OSV node 2 hostname and vice versa. Due to an OSV Cluster limitation, if OSV hostname of one node is a substring of the hostname of the other node, then the corresponding hotfix must be installed prior to the migration procedure:
  - for V9 systems: V9R4.48.11 hotfix
  - for V10 systems: V10R1.8.2 hotfix
    OSV hostnames : e.g. (n1) oseeosv & (n2) oseeosvn2 → n1 hostname is a substring of n2 hostname
    Login to your OSV as root and execute the command → ohnn1=$(hostname); ohnn2=$(ssh cluster_partner_alias 'hostname'); echo $ohnn1 | grep $ohnn2; STATUS=$?; echo -n "Migration check : ";[[$STATUS == 0]] && echo "WARNING" || echo "OK"
    - Command output : "Migration check : OK" → Proceed with the migration
    - Command output : "Migration check : WARNING" → Proceed to install the corresponding hotfix based on your system version and then procced with the migration procedure.

4 Apply new IP address schema

Take a snapshot of each OSEE VM before continuing.

4.1 Set new DNS & DLS IP for devices

4.1.1 Set DNS IP for devices

- Login to DLS → IP Devices → IP Phone Configuration → IP routing
  - For OSEE with Simplex OSV
    - Select DNS Server tab → enter OLD_THIG_WAN_IP for DNS Server Address → Search
    - Select table View and update DNS Server Address to NEW_OSV_IP
  - For OSEE with Cluster OSV
    - Select DNS Server tab → enter OLD_THIG_WAN_IP for DNS Server Address → Search
    - Select table View and update DNS Server Address to NEW_OSVN1_SIG_IP

Note: If DNS server is set on the phones via DHCP, please update the new DNS server IP address, accordingly, on your DHCP server.

4.1.2 Set new DLS IP for devices

Based on the OSEE Staging Guide, section 9.3 Enable Plug & Play via DHCP, the DLS IP address can be configured via DHCP server or manually set in the device.

DLS IP address configured via DHCP

Follow instruction from the corresponding chapter and replace the IP address of SBC-THIG with the new DLS IP address : *NEW_WIN_2_IP*

Once the DHCP server settings have been updated, login to DLS and restart phones.

- Login to DLS → IP Devices → IP Device Interaction → Reset IP Devices → Reset IP Device
  Note: Do not select Restore Factory Setting

DLS IP address configured manually

No action needed at this point. Once DLS is reconfigured to the new IP address, we will use the *Scan IP devices* functionality to update DLS IP in the devices.

4.2 Set temporary IP address for SBC-THIG

Based on your solution, please follow the corresponding sub chapter below

OSEE with Simplex OSV

Login to SBC-THIG management portal : https://<*OLD_THIG_WAN_IP*>

Select Network/Net Services → Settings

Scroll down to Access and Admin Realm Configuration and edit the Main IPv4 entry: Set a new IP address and Subnet mask (*NEW_TMP_THIG_IP*)

Scroll down to **Routing** and edit **Default gateway address** to match the temporary SBC-THIG IP address (*NEW_TMP_THIG_IP*)

Select **OK** and then **Apply Changes**

Select **OK** for pop up messages to restart the SBC-THIG.

Note: Depending on the network of the *NEW_TMP_THIG_IP*, you might need to set the corresponding option for the SBC-THIG (OSEEWAN) network adapter

You can monitor the VM console and wait for the SBC-THIG to come up. Then login using the new IP address : https://<*NEW_TMP_THIG_IP*>

Optional : You can export SBC-THIG configuration files on your local client by selecting **Maintenance** → **Import/Export** (tab)→ **Export** → **Export all** (button)

OSEE with Cluster OSV

Power off SBC-THIG 2 VM : **osee_v9_sbc_thig_n2** (default VM name)

Disconnect network adapters for SBC-THIG 2 VM : **osee_v9_sbc_thig_n2** (default VM name)

Login to SBC-THIG management portal : https://<*OLD_THIG_WAN_IP*>

SBC-THIG 1 VM is the Master node at this point

Select Network/Net Services → Settings

Scroll down to **Core Realm Configuration** and edit the **Main IPv4** entry: Set **IP address** 10.82.53.1
Note: If for any reason 10.82.53.1 is already in use, set any IP address from the Internal OSEE network 10.82.53.0/24 that is not used

Scroll down to Access and Admin Realm Configuration and edit the Main IPv4 entry: Set a new IP address and Subnet mask (*NEW_TMP_THIG_IP*)

Scroll down to **Routing** and edit **Default gateway address** to match the temporary SBC-THIG IP address (*NEW_TMP_THIG_IP*)

Scroll down to **Redundancy** and uncheck **Enable redundancy** checkbox. Select **OK** for pop up message.

Select **OK** and then **Apply Changes**

Select **OK** for pop up messages to restart the SBC-THIG.

Note: Depending on the network of the *NEW_TMP_THIG_IP*, you might need to set the corresponding option for the SBC-THIG (OSEEWAN) network adapter

You can monitor the VM console and wait for the SBC-THIG to come up. Then login using the new IP address : https://<*NEW_TMP_THIG_IP*>

Select Network/Net Services → Settings

Scroll down to **Core Realm Configuration** and edit the **Main IPv4** entry: Set **IP address** 10.82.53.227

Select **OK** and then **Apply Changes**

Select **OK** for pop up messages to restart the SBC-THIG.

You can monitor the VM console and wait for the SBC-THIG to come up. Then login using the new IP address : https://<*NEW_TMP_THIG_IP*>

Optional : You can export SBC-THIG configuration files on your local client by selecting **Maintenance** → **Import/Export** (tab)→ **Export** → **Export all** (button)

4.3 Set new IP address for OSV

For the update of the OSV, please refer to the corresponding version of the OpenScape Voice Vx Service Manual: Installation and Upgrades, → chapter C Updating the Node.cfg File (Also Known as EZIP)

The EZIP method that will be used is the NCPE Tool in Update mode. It is mandatory to use the NCPE tool following the OSV guidelines from the document above.

For the purpose of this manual, use OSEE Windows 2 server as the PC mentioned in the OSV manual

Connect to Windows 2 server VM using RDP based on the new SBC-THIG IP address *NEW_TMP_THIG_IP*

Copy latest NCPE software (based on your OSV version) to Windows 2 server VM via RDP

Based on your solution, please follow the corresponding sub chapter below

OSEE with Simplex OSV

Reminder : Simplex OSV in OSEE V9 is not considered an OSV integrated system.

Based on the OSV guidelines, verify System Health before EZIP Configuration Change → OSV Rapidstat → execute as *root* user : *~srx/bin/RapidStat*

Check service manual to evaluate warnings or errors before proceeding.

OSEE specific workaround is needed : edit node.cfg and set new DNS IP *NEW_OSV_IP* = *OLD_THIG_WAN_IP*

Connect to OSV, as root user, and update the value of the *name_server_ip_1* entry with the *NEW_OSV_IP*, in the file /etc/hiq8000/node.cfg

On the Windows 2 RDP Session and start NCPE in update mode : ifgui.cmd → Update → Next

Follow the instructions from chapter *C.2.2.2 Update the node.cfg file for the OpenScape Voice system* with the following supplementary OSEE specific information

In section 1 : **System Menu** enter the requested data, based on the OSV service manual

- OSEE specific : **Node 1 IP** set 10.82.53.229
- OSEE specific : **Port** set 22

Note: Since NCPE is running on OSEE Windows 2 server it will connect directly on the OSV nodes (not via the SBC-THIG)

After setting necessary entries, select *Next* and *OK* for any informational messages

In section 2 : System Configuration window → Edit System Configuration → Click OK to any messages

- Under IP Configuration 1/4
  - Set the **Subnet** to match the *NEW_OSV_IP*
  - Set the **Default Router IPv4** to match the *NEW_OSV_IP*
  - Set ALL the IP addresses in the NCPE tool under **Node1** and **Node2** to *NEW_OSV_IP*
    - Select **OK** for any informational message (e.g. License, TLS & MTLS addresses)
  - You can ignore SIS IP setting : *SIS IP 10.82.53.227*
- Under IP Configuration 2/4
  - → **Name Server IP 1** : NCPE tool will report "Invalid data". You can ignore this display (TOOLS-3646). The IP address displayed MUST be the *NEW_OSV_IP*
  - → **Super User** : Set NEW_UC_IP
- Under IP Security 1/2 → SNMP servers table
  - Replace "10.82.53.233" with NEW_UC_IP
- Select **Check** → Only 1 entry is expected : NameServerIP 1 from IP Configuration 2/4 : Duplicate Value
  - Only acceptable and expected entry is the one described above
- Select **Save** → Question pop-up : *Node.cfg is not valid* → Select **YES** → Click **OK** to popup message
- Select **Exit** → Select **YES**
- Select **Apply New Configuration** → Select **YES** and follow on screen instructions and messages

Once the update is completed, a message is shown certifying that all of the changes were made.

Note: After OSV has rebooted successfully (check console for status), you can proceed to set the new network adapter for the OSV VM (OSEELAN → New network)

Exit NCPE tool : select Back → Section 1: System Menu screen → Finish

At this point you can connect to the OSV node using the IP address : ssh *NEW_OSV_IP* port 22

OSEE specific : At this point, the applications server, has not been migrated yet so it is not possible to use the CMP.

Before proceeding, wait until the system comes up to state 4 (mandatory step)

- srxqry → expected result "Online at state 4" & "UCE and all signaling managers are up and running on mgmt""

Execute the following command in OSV: /unisphere/srx3000/callp/bin/buildDNSconfig

Based on the OSV guidelines , verify System Health after EZIP Configuration Change → OSV Rapidstat → execute as *root* user : *~srx/bin/RapidStat*

Check service manual to evaluate warnings or errors before proceeding.

OSEE with Cluster OSV

Based on the OSV guidelines, verify System Health before EZIP Configuration Change → OSV Rapidstat : execute as root user : *~srx/bin/RapidStat -b*

Check service manual to evaluate warnings or errors before proceeding.

OSEE specific workaround is needed : edit node.cfg on both OSV nodes and set new DNS IP *NEW_OSVN1_SIG_IP*

Connect to OSV node 1, as root user, and update the value of the *name_server_ip_1* entry with the *NEW_OSVN1_SIG_IP*, in the file /etc/hiq8000/node.cfg

Connect to OSV node 2, as root user, and update the value of the *name_server_ip_1* entry with the *NEW_OSVN2_SIG_IP*, in the file /etc/hiq8000/node.cfg

On the Windows 2 RDP Session and start NCPE in update mode : ifgui.cmd → Update → Next

Follow the instructions from chapter *C.2.2.2 Update the node.cfg file for the OpenScape Voice system* with the following supplementary OSEE specific information

In section 1 : **System Menu** enter the requested data, based on the OSV service manual

- OSEE specific : **Node 1 IP** set 10.82.53.229
- OSEE specific : **Port** set 22

Note: Since NCPE is running on OSEE Windows 2 server it will connect directly on the OSV nodes (not via the SBC-THIG)

After setting necessary entries, select *Next* and *OK* for any informational messages

In section 2 : System Configuration window → Edit System Configuration → Click OK to any messages

- Under **Configuration 1/1** → **Survival Authority :** Replace "10.82.53.233" with NEW_UC_IP
- Under IP Configuration 1/4
  - Set the **Subnet** to match the *NEW_OSVN1_MGMT_IP*
  - Set the **Default Router IPv4** to match the *NEW_OSVN1_MGMT_IP*
  - Under **Node1** (while setting values, select **OK** for any informational message : license, TLS-MTLS etc.)
    - set *NEW_OSVN1_MGMT_IP* for **Mgmt, Billing** and **Sig**
    - set *NEW_OSVN1_SIG_IP* for **Lsm, Sip, Sipmtls, MGCP** and **CSTA**
  - Under **Node2** (while setting values, select **OK** for any informational message : license, TLS-MTLS etc.)
    - set *NEW_OSVN2_MGMT_IP* for **Mgmt, Billing** and **Sig**
    - set *NEW_OSVN2_SIG_IP* for **Sip, Sipmtls, MGCP** and **CSTA**

    - You can ignore SIS IP setting : *SIS IP 10.82.53.227*
- Under IP Configuration 2/4
    - → **Name Server IP 1** : NCPE tool will report "Invalid data". You can ignore this display (TOOLS-3646). The IP address displayed MUST be the *NEW_OSVN1_SIG_IP*
    - → **Super User** : Set NEW_UC_IP
- Under **IP Security 1/2** → **SNMP servers** table : Replace "10.82.53.233" with NEW_UC_IP
- Select **Check** → Only 1 entry is expected : NameServerIP 1 from IP Configuration 2/4 : Duplicate Value
    - Only acceptable and expected entry is the one described above
- Select **Save** → Question pop-up : *Node.cfg is not valid* → Select **YES** → Click **OK** to popup message
- Select **Exit** → Select **YES**
- Select **Apply New Configuration** → Select **YES** and follow on screen instructions and messages

Once the update is completed, a message is shown certifying that all of the changes were made.

Note: After OSV both nodes have rebooted successfully (check console for status), you can proceed to set the new network adapter for both OSV VMs (OSEELAN → New network)

Exit NCPE tool : select Back → Section 1: System Menu screen → Finish

At this point you can connect to the OSV nodes using the new IP addresses

- ssh NEW_OSVN1_MGMT_IP port 22
- ssh NEW_OSVN2_MGMT_IP port 22

OSEE specific : At this point, the applications server, has not been migrated yet so it is not possible to use the CMP.

Before proceeding, wait until the system comes up to state 4 (mandatory step)

- srxqry → expected result "Online at state 4 4" & "UCE and all signaling managers are up and running on both nodes""

Execute the following command on both OSV nodes
: */unisphere/srx3000/callp/bin/buildDNSconfig*

Based on the OSV guidelines , verify System Health after EZIP Configuration Change → OSV Rapidstat → execute as root user : *~srx/bin/RapidStat -b*

Check service manual to evaluate warnings or errors before proceeding.

4.4 Set new IP address for UC

For the update of the UC server, please refer to the corresponding version of the OpenScape UC Application Vx Configuration and Administration → chapter 5.25.10.1 Changing the IP Address/FQDN for Small Deployment

- On the UC VM console, stop OpenScape UC Application and the rest of the applications on the UC OSEE server
    - /etc/init.d/symphoniad stop
    - /etc/init.d/openfire stop

    - systemctl stop cmpn.service
- On the UC VM console, change the IP address of the computer system using YAST → System → Network Settings
    - → Overview → IP Address : set new IP address & corresponding netmask *NEW_UC_IP* :
    - → Hostname → DNS server : set new DNS server :
        - for OSEE with Cluster OSV, new DNS server : *NEW_OSVN1_SIG_IP*
        - for OSEE with Simplex OSV, new DNS server : *NEW_OSV_IP*
    - → Routing → Default IPv4 Gateway : set new gateway to match NEW_UC_IP address :
- Once YAST is completed, you can proceed to set the appropriate new network adapter for the UC VM.
- Restart the application computer with the following command: *shutdown -r now*
- On the UC VM console, stop OpenScape UC Application and the rest of the applications on the UC OSEE server
    - /etc/init.d/symphoniad stop
    - /etc/init.d/openfire stop
    - systemctl stop cmpn.service

Note: In the default OSEE UC response file, the computer system is addressed via hostname "im". If any modification has taken place, please update the command in the next step according to the official UC documentation.

- On the UC VM console, execute the following commands
    - cd /opt/siemens/
    - servicetools/install/bin/changeSFWip.sh -c change -n none -a im -CF
- On the UC VM console, start OpenScape UC Application and the rest of the applications on the UC OSEE server
    - /etc/init.d/symphoniad start
    - /etc/init.d/openfire start
    - systemctl start cmpn.service
- Note: The CMP is accessible on the default port , port 446 is no longer needed.

4.5 Set new IP address for the SIP Server of Media Server

For the update of the Media server, please refer to the corresponding version of the OpenScape Media Server Vx, Administrator Documentation → chapter 8.2.2 How to Configure the SIP Provider. It is strongly suggested to set new IP address for the SIP Server of Media Server and to do that please follow the steps below:

- Login to CMP → https://*NEW_UC_IP*
- Select Configuration → Unified Communications → Configuration → Media Server
- Select the link of Media server that you want to set a new IP address for its SIP server, from the **Media Server Nodes** list
- On the pop-up window, under Providers tab, select the link **IP Telephony (SIP)**
    - A pop-up window with the SIP provider settings opens.
- Select **Add** under **SIP Servers** area.
    - A pop-up window for creating an SIP server line to a communications system opens.
- Enter a unique name for the new SIP server line in the **ID** field.
- In the **SIP Server Name (FQDN / IP Address)** field specify the IP address of the Master SIP server to be preferably used by the Media Server for the relevant SIP server line.
    - Note: If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.
- Select in the **Listening Point ID** field one of the configured listening points.

    - Note: Listening point defines the local network address of the Media Server via which the Media Server is to communicate with the Master SIP server.
- Specify in the **Port number** field the port number of the Master SIP server via which the Media Server is to communicate with the Master SIP server.
    - If you have selected a UDP- or TCP-based listening point in the Listening Point ID field, you will need to enter port 5060 here as a rule, because this is the UDP/TCP default port of SIP
    - If you have selected a TLS-based listening point, you will need to enter port 5061 here as a rule, because this is the TLS default port of SIP servers.
- You can configure optionally, alternative SIP server connections for the SIP server line:
    - Select **Add** under **Alternative SIP Servers** area.
        - A pop-up window for creating an alternative SIP connection to a communications system opens.
    - In the **SIP Server Name (FQDN / IP Address)** field specify the IP address of the alternative SIP server the Media Server is to use for the relevant SIP server line if required.
        - Note: If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.
    - Specify in the **Port number** field the port number of the alternative SIP server via which the Media Server is to communicate with the Master SIP server.
        - If you have selected a UDP- or TCP-based listening point in the Listening Point ID field, you will need to enter port 5060 here as a rule, because this is the UDP/TCP default port of SIP
        - If you have selected a TLS-based listening point, you will need to enter port 5061 here as a rule, because this is the TLS default port of SIP servers.
    - Select **Save** to copy the settings of the fail-over SIP connection.
    - If required, configure for the SIP server line further alternative SIP server connections in the same way.
- Select **Save**
- Select **Save**
- Select the radio button for the **IP Telephony (SIP)** provider.
- Select **Restart Provider**
    - Important: When you reboot the SIP provider (IP Telephony), all associated connections are interrupted that exist at the time of the reboot. Before the reboot you can switch to the Monitoring tab to see whether connections are currently active.
- Select **Close**

4.6 Set new IP address for OSEE Windows 1 Server

Login on the OSEE Windows 1 VM console

Before proceeding to any changes on the windows server,

- Run XPR renserv tool
    - Open command prompt and execute
        - cd C:\openscape\xpr\SDKTools
        - renservr 10.82.53.241 NEW_WIN_1_IP
          follow on screen instructions
- Open Services window : Select *Start* → type *Services*
    - Stop Connection APL (CONAPL)
        - Stop XPR Connection APL(conapl) service
    - If Contact Center is installed, stop OSCC services
        - Stop OpenScape Contact Center
        - Stop OpenScape Contact Center Agent Portal Server
        - Stop OpenScape Contact Center AutoPA
            - Wait until all OSCC servers are in status Not Started

    - Stop Concierge
        - Stop OSCC-E Service
        - Stop OSCC-E SI Router
- Select Start → Control Panel → Network and Internet → Network and Sharing Center → Change adapter settings
- Right-click on the ethernet adapter and select Properties → Internet Protocol Version 4 (TCP/IPv4) → Properties
    - Set new IP address NEW_WIN_1_IP and the corresponding netmask and default gateway
    - Set preferred DNS server
        - for OSEE with Cluster OSV, new DNS server : *NEW_OSVN1_SIG_IP*
        - for OSEE with Simplex OSV, new DNS server : *NEW_OSV_IP*
    - Select OK → Close
- Stop XPR server
    - Select *Start,* type and select *Services*
    - Stop XPR License Server (licsvc)
    - Stop XPR Administrator (mrs)
        - Wait until all XPR services have stopped
- Restart Windows server
    - You can proceed to set the appropriate new network adapter for the OSEE Windows 1 VM.

4.7 Set new IP address for OSEE Windows 2 Server

- Login on the OSEE Windows 2 VM console
    - Stop DLS service
        - Select *Start,* type and select *Services*
        - Stop DeploymentService
    - Select Start → Control Panel → Network and Internet → Network and Sharing Center → Change adapter settings
    - Right-click on the ethernet adapter and select Properties → Internet Protocol Version 4 (TCP/IPv4) → Properties
        - Set new ip address NEW_WIN_2_IP and the corresponding netmask and default gateway
        - Set preferred DNS server
            - for OSEE with Cluster OSV, new DNS server : *NEW_OSVN1_SIG_IP*
            - for OSEE with Simplex OSV, new DNS server : *NEW_OSV_IP*
        - Select OK → Close
    - Restart Windows server
    - You can proceed to set the appropriate new network adapter for the OSEE Windows 2 VM.

5 Update application provisioning

5.1 CMP

Login to CMP → https://*NEW_UC_IP*

Select Configuration → OpenScape Voice → General → Switches

Expected error time out since OSV has changed IP addresses → Select **Close** on the pop up window

Click on the Switch **Name** or select checkbox and press **Edit** button

On the pop-up window, under General tab. press **Change IP Address**

Enter srx password and IP address based on your solution

- Simplex OSV : *NEW_OSV_IP*
- Cluster OSV : NEW_OSVN1_MGMT_IP

Select **OK** → **Save**

Expected Result → Switch Connectivity : Reachable

Select Maintenance → Licenses → Information

Set items/page to 200. Install all the updated license files for your applications using the button **Offline Activation** → **Choose File** → **Activate**

Note: XPR, Concierge and DLS license files will be uploaded to Windows license server

Select Maintenance → Inventory → Applications

Set items/page to 200. Any application with IP address from the OSEELAN internal network (10.82.53.xxx) must be updated based on the tables from the New IP schema design section

- Select the right arrow and select "Configure Connection
- Based on the tables from the New IP schema design section, update each IP address e.g. 10.82.53.241 → NEW_WIN_1_IP
- Save
- Repeat for any application with 10.82.53.xxx IP address

Select Maintenance → Monitoring

Under Logs → Remote Logging for OSV-TM

- If SFTP server is set with IP address, please update IP address : 10.82.53.249 → NEW_WIN_2_IP

Under SNMP Notifications → Sender → Destinations

- If any IP address is set from the OSEELAN internal network (10.82.53.xxx), then this entry must be updated based on the tables from the New IP schema design section

Select Maintenance → Recovery

Under General → Archives

- If FTP/SFTP server is set with IP address from the OSEELAN internal network (10.82.53.xxx), please update the IP address accordingly

5.2 OSV

5.2.1 Install OSV license files

- Upload lic to OSV
- Login to OSV, as root, via SSH or console
- Copy the licenses key file to directory /opt/unisphere/srx3000/cla/import → # cp <license_file> /opt/unisphere/srx3000/cla/import/

For OSEE Cluster, install licenses on both nodes.

5.2.2 Update OSV integrated DNS server

IMPORTANT: execute steps below in the exact order that are stated

Connect to OSV (ssh OR console), as root user, to update fqdn.cfg file (for Cluster OSV on both nodes)

- Execute → vi /etc/hiq8000/fqdn.cfg → First line replace 10.82.53.0/24 with 0.0.0.0/0 → save and exit
- Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

IMPORTANT : Based on your solution, it is possible that the DNS server configuration file has been updated manually with additional entries, after the initial provisioning. The steps below are required to update entries related to core components, based on the initial provisioning. Please

update the manual entries, by deleting both IP addresses and setting the correct public IP, for each entry.

Note: In the examples below, the "stathens.net" is the domain name set in the webCDC project

UC server related entries
1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.233" 2. Note down all entries from the output and for each entry : ○ delete both IP addresses and set IP address NEW_UC_IP → *vi /etc/hiq8000/fqdn.cfg* e.g. *cat /etc/hiq8000/fqdn.cfg* | *grep "10.82.53.233"* → output one entry "A conf.uc.stathens.net 10.5.33.70 10.82.53.233" → modified "A conf.uc.stathens.net 10.5.33.73" 3. Once modification is completed ○ execute → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.233" → expected output : 0 entries ○ execute → cat /etc/hiq8000/fqdn.cfg | grep "NEW_UC_IP" → expected output : entries from step 2, pointing to *NEW_UC_IP* 4. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep -i "openfire" ○ expected output, one entry : e.g. "A openfire.stathens.net *NEW_UC_IP*" ○ update this entry and set same IP address twice → expected output, one entry : e.g. "A openfire.stathens.net *NEW_UC_IP NEW_UC_IP*"
• Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

Win 1 server related entries
1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.241" 2. Note down all entries from the output and for each entry : ○ delete both IP addresses and set IP address NEW_WIN_1_IP → vi /etc/hiq8000/fqdn.cfg e.g. cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.241" → output one entry "A vm.xpr.stathens.net 10.5.33.70 10.82.53.241" → modified ""A vm.xpr.stathens.net 10.5.33.74" 3. Once modification is completed ○ execute → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.241" → expected output : 0 entries ○ execute → cat /etc/hiq8000/fqdn.cfg | grep "NEW_WIN_1_IP " → expected output : entries from step 2, pointing to NEW_WIN_1_IP
• Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

Win 2 server related entries
1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.249" 2. Note down all entries from the output and for each entry : ○ delete both IP addresses and set IP address NEW_WIN_2_IP → vi /etc/hiq8000/fqdn.cfg e.g. cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.249" → output one entry "A

dls.stathens.net 10.5.33.70 10.82.53.249" → modified ""A dls.stathens.net 10.5.33.75"

3. Once modification is completed
    - execute → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.249" → expected output : 0 entries
    - execute → cat /etc/hiq8000/fqdn.cfg | grep "NEW_WIN_2_IP " → expected output : entries from step 2, pointing to NEW_WIN_2_IP

- Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

External Media Server (MS) related entries

Pending your solution setup, additional media servers might exist.

1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep -E 'A ms[0-9]'
2. Expected output, a list of entries based on webCDC project : e.g. "A ms2.<domain name from WebCDC> 10.5.33.70 10.82.53.220" etc.
3. For each entry
    - Delete both IP addresses from fqdn.cfg for the specific entry and set IP address based on the *Media Server IP addresses* table from the *New IP schema design* chapter
    - Repeat for each Media Server related entry
4. Once modification is completed, execute → cat /etc/hiq8000/fqdn.cfg | grep -E 'A ms[0-9]' → expected output : single IP address per line, no 10.82.53.xxx IP address

- Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

SBC-THIG related entries

1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.227" | grep "OLD_THIG_WAN_IP"
2. Expected output are SBC-THIG entries : "A <domain name from WebCDC> 10.5.33.70 10.82.53.227", "A Thig1.<domain name from WebCDC> 10.5.33.70 10.82.53.227"
    - For entry "<domain name from WebCDC>" of the fqdn.cfg file
        - delete both IP addresses from fqdn.cfg and set IP address
            - for OSV Simplex → NEW_OSV_IP
            - for OSV Cluster → NEW_OSVN1_SIG_IP
            Note: If recommendation was followed to re-use the OLD_THIG_WAN_IP address, you will only have to delete only the 10.82.53.227 entry
    - Delete entry "Thig1.<domain name from WebCDC>"

3. Once modification is completed, execute → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.227" | grep "OLD_THIG_WAN_IP" → expected output : 0 entries

- Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.227"
2. Expected output is a list of entries of the solution endpoints, with their public IP addresses
   followed by OLD_THIG_WAN_IP
   - For each entry of the fqdn.cfg file → delete only the "10.82.53.227" IP address
3. Once modification is completed, execute → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.227" → expected output : 0 entries

- Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

Based on your solution, please follow the corresponding table below

OSV Simplex related entries

1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.2"
2. Note down all entries from the output and for each entry :
   - delete both IP addresses and set IP address NEW_OSV_IP → vi /etc/hiq8000/fqdn.cfg
     e.g. cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.2" → output one entry "A mgmt.osv.stathens.net 10.5.33.70 10.82.53.229" → modified "A mgmt.osv.stathens.net NEW_OSV_IP"
     Note: If recommendation was followed to re-use the OLD_THIG_WAN_IP address, you will only have to delete only the 10.82.53.xxx entries
3. Once modification is completed, execute → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.2" → expected output : 0 entries

- Execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

OSV Cluster related entries

1. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.229"
   - Expected output, one entry : e.g. "A mgmt.osv.stathens.net 10.5.33.40 10.82.53.229"
   - Delete both IP addresses and set IP address NEW_OSVN1_MGMT_IP → vi /etc/hiq8000/fqdn.cfg
2. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.230"
   - Expected output, one entry : e.g. "A mgmt2.osv.stathens.net 10.5.33.40 10.82.53.230"

- Delete both IP addresses and set IP address NEW_OSVN2_MGMT_IP → vi /etc/hiq8000/fqdn.cfg

3. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.231"
   - Expected output, multiple entries : e.g. "A sip.osv.stathens.net 10.5.33.40 10.82.53.231"
   - Delete both IP addresses and set IP address NEW_OSVN1_SIG_IP → vi /etc/hiq8000/fqdn.cfg
     Note: If recommendation was followed to re-use the OLD_THIG_WAN_IP address, you will only have to delete only the 10.82.53.xxx entries
4. Execute the following command → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.232"
   - Expected output, multiple entries : e.g. "A sip2.osv.stathens.net 10.5.33.40 10.82.53.232"
   - Delete both IP addresses and set IP address NEW_OSVN2_SIG_IP → vi /etc/hiq8000/fqdn.cfg
5. Once modification is completed, execute → cat /etc/hiq8000/fqdn.cfg | grep "10.82.53.2" → expected output : 0 entries
6. Repeat steps on OSV node 2

- On both OSV nodes : execute → */unisphere/srx3000/callp/bin/buildDNSconfig* → No error is expected, modification successful

Note: At this point, no 10.82.53.xxx entry should be found in /etc/hiq8000/fqdn.cfg

5.2.3 Update hosts file

Connect to OSV (ssh OR console), as root user, to check /etc/hosts (for Cluster OSV on both nodes)

- Execute the following command → cat /etc/hosts | grep "10.82.53"

Based on the previous step (Update OSV integrated DNS server), expected output is 0 entries. In case, manual entries have been added, please update them accordingly by setting the correct public IP

5.2.4 Update OSV provisioning

IMPORTANT : The OSEE solution has been configured based on webCDC project settings. Many items are configured using FQDNs so there is no need to set new IP addresses, since DNS has been updated. However, these settings may have been modified manually, so the administrator must modify, when necessary, the IP addresses to correspond to the new IP Schema.

Login to CMP → https://NEW_UC_IP

Configuration → OpenScape Voice → Administration

General Settings → **CDR** : In case, Billing Servers are using IP addresses from the OSEELAN fixed network (10.82.53.0/24), please update them accordingly

General Settings → Packet Filter Rules :

Note: Modification of packet filter rules must be made with extreme caution and verify that no other attribute is modified except from the ones documented below.

PFRs can also be updated via CLI : Connect to OSV (ssh OR console) as srx → startCli → Login: sysad → 6 for Application-level Management → 8 for Network Element Security Management → 3 for Packet Filter Rules Security Management

- PFR *Names* containing IP addresses from the OSEELAN fixed network (10.82.53.0/24), can be updated optionally by the administrator.
- PFR *Remote FQDN or IP Address* that correspond to IP addresses from the OSEELAN fixed network (10.82.53.0/24) must be updated accordingly based on the tables from the *New IP schema design* section
    - 10.82.53.233 → NEW_UC_IP
      Note: When updating the new IP addresses manually, via CMP, you may get an error message "*Packet Filter Rule specified is invalid*". New PFRs have been added by NCPE update mode and when OSV was added to CMP, so modifying existing PFRs may lead to error since PFRs with exact same values but different names are not allowed. When encountering, this specific error "*Packet filter rule with same exact values already exists in database*" for a PFR with remote IP address 10.82.53.xxx, you can delete this PFR.
    - 10.82.53.241 → NEW_WIN_1_IP
      Note: System defined PFRs cannot be deleted or modified via CMP, so for these PFRs, CLI must be used for any modification → Connect to OSV (ssh OR console) as **srx** → **startCli** → Login: **sysad** → 6 for **Application-level Management** → 8 for **Network Element Security Management** → 3 for **Packet Filter Rules Security Management** → 2 to **Modify** → copy paste exact name from CMP and follow on screen instructions to modify "**Remote IP Address**"
    - 10.82.53.249 → NEW_WIN_2_IP

Media Server → List :

- Select all → **Block**
- For each entry the internal OSEELAN IP address must be replaced : select Media Server → General tab
    - *Fully Qualified Domain Name* → set the new IP address inside the brackets based on the *Media Server IP addresses* table from the *New IP schema design* chapter : e.g. [10.82.53.233] → [NEW_UC_IP]
    - MG Signaling → set the new IP address based on the *Media Server IP addresses* table from the *New IP schema design* chapter : 10.82.53.233 → NEW_UC_IP
    - Repeat for all MS entries
- Select all → **Unblock**

Signaling Management → **CSTA** → tab **Applications** → Check entries with OSEELAN IP address and update accordingly based on the *New IP schema design* section

- Select entry → *Edit* → Update IP address under *Application IP Address* → *Save*
- Repeat for all entries
- *Save* on CSTA settings window

Signaling Management → Authentication → tab Realms

- Delete realm entry with IP address 10.82.53.227 : Select → Delete
    - For OSV Cluster : delete also realm entries with IP address 10.82.53.226 & 10.82.53.225 : Select → Delete
- Check all realms and replace any 10.82.53.xxx IP address based on the tables from the *New IP schema design* section → Select realm and *Edit* → e.g. 10.82.53.233 is replaced by NEW_UC_IP

Tools → **Continuous Tracing** → By default, IP address is set with FQDN. If it has been modified manually, update accordingly by setting the correct public IP.

Configuration → OpenScape Voice → Business Group

Members → Subscribers

- Uncheck "*Registration via Central SBC Allowed*" setting for all SIP subscribers (not *Profile* Only, crosscheck *Connection Information* under tab *Connection*) that are not actual remote users, registering through an SBC. Removing the THIG, all subscribers located in the corporate network are no longer considered remote subscribers
    - To bulk edit the subscribers, for each Branch Office, repeat the steps below (Verify that remote users are not modified by the bulk edit action, must be excluded from the selection below)
        - Select *Subscribers* → Set *Items/Page* to 200 → Select All → Select button *More* → *Bulk Edit ...* → on the pop up window, select tab *Connection* → For "*Registration via Central SBC Allowed*" select the checkbox before and unselect the checkbox after → Save
        - Repeat for all Branch Offices

Members → Endpoints

Based on the THIG architecture, many OSV SIP endpoints are configured using SBC-THIG internal IP address or an FQDN resolving to the SBC-THIG internal IP address along with a unique port number. For all these OSV SIP endpoints, the corresponding public IP address and port must be identified via SBC THIG configuration, based on the steps below. At this point, it is mandatory to identify for all these OSV SIP endpoints the public IP address and port. *SIP endpoint address* for an OSV endpoint may be configured with FQDN or IP address.

For the purpose of this guide, we will use the following name format : 10.82.53.227:EP1_THIG_PORT→ EP_1_PUBLIC_IP:EP_1_PUBLIC_PORT and EP_1_FQDN

For every OSV SIP endpoint, check the steps below and create the corresponding table :

- **SIP Endpoint Address** *: SIP tab → Endpoint Address* (if FQDN is set, note it also under FQDN column)
- **SIP PORT :** SIP tab → Port number
- **Public IP & Public Port :** Applicable only if 10.82.53.227 is set under S*IP Endpoint Address* or under *Aliases* → EP_1_PUBLIC_IP & EP_1_PUBLIC_PORT : Login to SBC-THIG → https://OLD_THIG_WAN_IP → Features → Remote Endpoints : Configure → Remote Endpoint Configuration table → identify the row where the EP1_THIG_PORT matches to the "*Core realm port*" of the SBC-THIG EP table → In this row, value under "*Remote IP address*" is EP_1_PUBLIC_IP and value under "Remote Port" is EP_1_PUBLIC_PORT
- **FQDN** : Applicable only if FQDN is set under S*IP Endpoint Address* or under *Aliases.* It is possible that OSV endpoint EP_1 is configured only with IP address. When OSV endpoint EP_1 is set with FQDN, then string EP_1_FQDN can be identified under SIP tab in the *Endpoint Address* field and/or under *Alias* tab.

OSV Endpoint	SIP Endpoint Address (before migration)	SIP PORT (before migration)	Public IP (if applicable)	Public Port (if applicable)	FQDN (if configured under SIP or Aliases)
EP_1	10.82.53.227	EP1_THIG_PORT	EP_1_PUBLIC_IP	EP_1_PUBLIC_PORT	EP_1_FQDN
EP_2	10.82.53.227	50002	10.2.10.19	5060	gateway.stathens.net
EP_3	10.82.53.241	5060	N/A	N/A	N/A

EP_4	proxy.stathens.net	50004	10.3.21.33	5060	proxy.stathens.net

It is highly recommended to create the OSV endpoint table for reference

Back on the CMP configuration (OSV → BG → Endpoints), update all endpoints in all branch offices based on the steps below.

- Delete the SBC-THIG related endpoint from "*Main Office"*
  - for OSV Simplex : SBC-THIG EP : Default EP Name = *SbcThig1* - SIP EP Address = 10.82.53.227 - SIP Port = 5060 → Select EP and press "Delete"
  - for OSV Cluster : Three SBC-THIG EP :
    1. Default EP Name = *SbcThig1* - SIP EP Address = 10.82.53.225 - SIP Port = 5060 → Select EP and press "Delete"
    2. Default EP Name = *SbcThig2* - SIP EP Address = 10.82.53.226 - SIP Port = 5060 → Select EP and press "Delete"
    3. Default EP Name = *SbcThigVirt* - SIP EP Address = 10.82.53.227 - SIP Port = 5060 → Select EP and press "Delete"
- For every endpoint that is set with *Type Static* (under *SIP* tab) perform the two step modifications below :
  - Step 1 – EP IP & Port
    1. Select Endpoint → tab SIP
       - Endpoint Address :
         - if IP matches 10.82.53.227 → replace with EP_1_PUBLIC_IP for this endpoint from the OSV endpoint table above
         - if IP matches 10.82.53.xxx (except 10.82.53.227) → replace the IP address based on the tables from the *New IP schema design* section : e.g. 10.82.53.233 is replaced by NEW_UC_IP
         - if set with FQDN e.g EP_1_FQDN → no modification is needed
       - Port
         - if IP set in *Endpoint Address* matches *10.82.53.227* → replace with EP_1_PUBLIC_PORT for this endpoint from the OSV endpoint table above
         - if IP set in *Endpoint Address* matches 10.82.53.xxx (except 10.82.53.227) → no port modification is needed
         - if set with FQDN (e.g. EP_1_FQDN) → check *Aliases* tab :
           - if no 10.82.53.227 entry is found → do not modify port
           - if 10.82.53.227 entry is found → replace with EP_1_PUBLIC_PORT for this endpoint from the OSV endpoint table above
    2. tab Aliases
       - Alias with IP Address
         - if entry matches 10.82.53.227:EP1_THIG_PORT → replace with EP_1_PUBLIC_IP:EP_1_PUBLIC_PORT based on the OSV endpoint table above
         - if entry matches 10.82.53.xxx (except 10.82.53.227) → replace the IP address based on the tables from the *New IP schema design* section and (if configured) keep the same port number : e.g. 10.82.53.233;1234 → NEW_UC_IP:1234, 10.82.53.241 → NEW_WIN_1_IP
       - Alias with FQDN
         - if entry is set with FQDN and no port → no modification is needed
         - if entry is set with FQDN and port then :
           - If *Port* value from previous step (tab *SIP*) was updated, then update also this alias entry → replace EP_1_FQDN:port_number with EP_1_FQDN:EP_1_PUBLIC_PORT

- If *Port* value from previous step (tab *SIP*) was not updated → no modification is needed

3. Save

- Step 2 – Security
  1. Select *Endpoint* → tab *SIP*
     - Scroll down to *Security* → *Verify* that the corresponding "*Trusted Ports*" are *OK* (green checkmark), otherwise select *Edit* → new pop up window *Authentication*
       Note: For any custom endpoint configuration, please update the endpoint realm accordingly to match the new IP schema and your custom configuration. Rules below apply to the default (webCDC) and the basic endpoint provisioning configurations.
       - If endpoint realm is custom configured with *Trusted entity* disabled and realm attributes (passwords, usernames, etc.) used for authentication
         - modify IP (*Signaling Primary)* and port (*Signaling Port)* according to the OSV endpoint table
         - select *Save* to close *Authentication* pop up window (no other modification needed for this endpoint realm)
         - select *Save* to close the endpoint pop up window and procced to the next endpoint
       - If EP_1_FQDN exists in the list, update realm : select EP_1_FQDN → Edit → If *Port* value from previous step was updated, update also the Port Range : e.g. if applicable, set range EP_1_PUBLIC_PORT-EP_1_PUBLIC_PORT
       - If *Endpoint Address* was replaced with *EP_1_PUBLIC_IP* from previous step add a new realm entry : *Add :*
         - Signaling Primary : EP_1_PUBLIC_IP
         - *Trusted Entity :* Checked (enabled)
         - Port Range selected
         - *Port Range :* EP_1_PUBLIC_PORT-EP_1_PUBLIC_PORT
         - OK
       - If *Endpoint Address* of the selected endpoint is missing from the list, add the corresponding entry : Add
         - Signaling Primary : Value from Endpoint Address on SIP tab (IP or FQDN)
         - *Trusted Entity :* Checked (enabled)
         - Port Range selected
         - *Port Range :* Port-Port (Port value from *SIP tab)*
         - OK
       - If *Endpoint Address* of the selected endpoint is on the list (IP or FQDN), but port is not included in the *Trusted Ports* column → select entry → Edit :
         - Update Port Range, by adding comma Port-Port (Value from *Port* on *SIP tab*) : e.g.
           - Port Range (Before): 5060-5060
           - Port Range (After): 5060-5060 , 50002-50002
       - *Save* to close *Authentication* pop up window
     - Save to close the endpoint pop up window
  2. Save

Reminder : Repeat steps above for all static endpoints under all branch offices

Configuration → OpenScape Voice → Global translation and Routing

Endpoints Management → Endpoints

Based on the default provisioning from webCDC that was imported during the initial deployment of the solution, there should be no endpoints under *Global translation and Routing.* However , it is possible that endpoints have been added manually.

Please update the endpoints according to the guidelines from section **Members** → **Endpoints** under **Configuration → OpenScape Voice → Business Group**

5.3 UC

New URL for UC client → https://*NEW_UC_IP*:8443

Please update related entries in corporate DNS server (if applicable).

5.4 Openfire

- Login to CMP → https://*NEW_UC_IP*
- CMP > configuration > Unified Communications > Configuration > Presence & IM
- Under "**XMPP Server IP Address**" set "*NEW_UC_IP*" and select **Save**

5.5 CLA - CLM

Login to Win1 (via console or RDP using NEW_WIN_1_IP)

Install updated license files for :

- Xpressions
- Concierge
- DLS

For each license file , select "License Management" from the desktop → Activate license → Install local license key on license agent (offline activation) → Continue → License File → Browse → Select license file→ Activate

5.6 DLS

Login to DLS server → https://NEW_WIN_2_IP:10443

Register phones with DLS Phones with DLS IP address provided via DCHP have been updated in previous step. To register phones that the DLS IP address was manually set in the device, it is recommended to use the "*Scan IP Devices*" functionality : **DeploymentService → IP Devices → IP Device Interaction → Scan IP Devices**

Create an IP scanner for all your devices and send the new DLS IP address (tab *Configuration* → Select to *Send DLS Address* and set *DLS Address* to NEW_WIN_2_IP*).* Verify *Scan Results.*

Update HTTPS Server Configuration

DeploymentService → Administration → Server Configuration→ HTTPS Server Configuration → Search → CDC HTTPs Connection

Update only the IP address for "HTTPS Server URL" & "Internal URL"

- OLD_THIG_WAN_IP → NEW_UC_IP : updated URL
  → **https://**<*NEW_UC_IP*>**:444/repository/phoneloads**
- 10.82.533.233 → NEW_UC_IP : updated URL
  → **https://**<*NEW_UC_IP*>**:444/repository/phoneloads**

Save

Update Alarm Configuration

DeploymentService → Administration → Alarm Configuration → Tab SNMP

Update the entry of the *SNMP host* : 10.82.533.233 → NEW_UC_IP

Save

Update DCMP Configuration

DeploymentService → Administration → Workpoint Interface Configuration → Tab DCMP

In *Device-DCMP connection,* update the entry of the *Device-DCMP Host* : 10.82.53.249
→ NEW_WIN_2_IP

Save

Update OSVTM Configuration (if configured)

DeploymentService → Administration → Trace Configuration → Tab OSVTM Configuration

Update the entry of the *OSVTM IP address* : 10.82.53.249 → NEW_WIN_2_IP

Save

Update Server licenses

DeploymentService → Administration → Server Licenses

Update IP addresses
for **Licensagent** and **License Management**

- 10.82.53.241
  → NEW_WIN_1_IP

Save

Select **Read Licenses** button →
expected *Status : License file available*

Update IP Phone Configuration → DeploymentService → IP Devices → IP Phone Configuration

Note: Steps below are related to the initial OSEE provisioning and some core DLS functionalities. In case of manual additional provisioning on the DLS server, please proceed to update the IP addresses according to the *New IP schema design.*

Update DNS server IP address for phones

Note: If recommendation was followed to re-use
the OLD_THIG_WAN_IP address, you will not need to update the DNS server IP address for the phones

- Select IP Routing
- Under **Views** select radio button **Search** → tab **DNS Server** →
  type *OLD_THIG_WAN_IP* in **DNS Server Address:** → select **Search** (bottom right)
- Select radio button **Table**
- Under **DNS Server Address** column in the first entry (row),
  replace *OLD_THIG_WAN_IP* with
  - NEW_OSV_IP - for OSV Simplex
  - NEW_OSVN1_SIG_IP - for OSV Cluster
- Select **Edit** Menu→ **Select All**
- Select **Save**

Update DNS server IP address for templates

Note: If recommendation was followed to re-use
the OLD_THIG_WAN_IP address, you will not need to update the DNS server IP address for the phones

- Select IP Routing
- Under **Views** select radio button T**emplate** and then **Get** (bottom right)
- Select a template
- Under **DNS Server Address** field, if applicable,
  replace *OLD_THIG_WAN_IP* with
  - NEW_OSV_IP - for OSV Simplex

    - NEW_OSVN1_SIG_IP - for OSV Cluster
- Select **Save**
- Repeat for all templates

Update SIP server IP addresses for phones

Note: Default configuration from webCDC uses FQDN for SIP server IP addresses, so it is not expected that OLD_THIG_WAN_IP address is used. If it has been modified manually, please update accordingly. If recommendation was followed to re-use the OLD_THIG_WAN_IP address, no action is necessary.

- Select Gateway/Server
- Under **Views** select radio button **Search** → tab **SIP Registering 1** → type *OLD_THIG_WAN_IP* in **SIP Registrar Addr** → select **Search** (bottom right)
- Select radio button **Table**
- Check columns **Reg-Address (HFA)/SIP Server Address - SIP Gateway Addr - SIP Registrar Addr** and in the first entry (row), wherever *OLD_THIG_WAN_IP* is set, replace it with :
    - NEW_OSV_IP - for OSV Simplex
    - NEW_OSVN1_SIG_IP - for OSV Cluster
- Select **Edit** Menu→ **Select All**
- Select **Save**

Update SIP server IP addresses for templates

Note: Default configuration from webCDC uses FQDN for SIP server IP addresses, so it is not expected that OLD_THIG_WAN_IP address is used. If it has been modified manually, please update accordingly. If recommendation was followed to re-use the OLD_THIG_WAN_IP address, no action is necessary.

- Select Gateway/Server
- Under **Views** select radio button T**emplate** and then **Get** (bottom right)
- Select a template
- Check fields **Reg-Address (HFA)/SIP Server Address**, **SIP Gateway Addr** & **SIP Registrar Addr** across all tabs and, wherever *OLD_THIG_WAN_IP* is set, replace it with :
    - NEW_OSV_IP - for OSV Simplex
    - NEW_OSVN1_SIG_IP - for OSV Cluster
- Select **Save**
- Repeat for all templates

Update Mobile Users

Mobile user configuration is not part of the initial OSEE provisioning.

In case of manual provisioning , please proceed to update the IP addresses according to the *New IP schema design,* where applicable.

DeploymentService → Mobile Users

Update Element Manager

DeploymentService → Element Manager

- Select Element Manager Configuration
- Under **Views** select radio button **Search** and then **Search** (bottom right)
- Update Element Manager Address :
  - NEW_OSV_IP - for OSV Simplex
  - NEW_OSVN1_MGMT_IP - for OSV Cluster
- Save

5.7 Trace Manager

If *Allow Remote Access* is enabled for Trace Manager, it is possible to use the new URL for login → https://NEW_WIN_2_IP:28081

Otherwise login to Win2 (via console or RDP using NEW_WIN_2_IP) and select *FADE* from the desktop

No modification is needed.

5.8 Xpressions

Update the configuration files on the UC server

Login to UC server (ssh or console) and replace 10.82.53.241 with *NEW_WIN_1_IP*

- vi /opt/siemens/HiPathCA/config/common/voicemail.xml
  - <address>https://10.82.53.241> → <address>https://*NEW_WIN_1_IP*</address>
  - <remoteIpAddr>10.82.53.241</remoteIpAddr> → <remoteIpAddr>NEW_WIN_1_IP</remoteIpAddr>
- vi /opt/siemens/HiPathCA/config/common/xpressions.cfg
  - Xpressions.remoteIpAddr=10.82.53.241 → Xpressions.remoteIpAddr=NEW_WIN_1_IP
  - Xpressions.ServerAddress=https://10.5.33.40:28084 → Xpressions.ServerAddress=https://NEW_WIN_1_IP
- Stop and start symphonia
  - /etc/init.d/symphoniad stop
  - /etc/init.d/symphoniad start

Login to Win1, via console or RDP using *NEW_WIN_1_IP*

Verify that all XPR services are running after server restart → Open Services window : Select Start → type Services
If any XPR service is not in status *Running,* then :

- Stop XPR Administrator (mrs)

- Wait until all XPR services have stopped
- Start XPR Administrator (mrs)
- Wait until all XPR services are in status *Running*

Update UC IP address

- Go to directory "C:\openscape\xpr\res\WebApl\WebAdmin"
- Edit file "param.xml"
  - replace 10.82.53.233 with *NEW_UC_IP*
- Save file

Open XPR Monitor - System Logging : Start > All Programs > Xpressions > Monitor – System Logging and login

Update ipApl configuration

- Under Modules of XPRESSIONS expand ipApl and double-click on Advanced Settings
- Select tab *Device*
- Select SIP Protocol Stack → Edit
  - New window : tab *SIP → SIP Options*
    - SIP proxy by default set with FQDN (*SIP Proxy DNS Name*), in case of custom configuration, please update accordingly
    - Update *Own IP Address* from 10.82.53.241 to *NEW_WIN_1_IP*
  - OK
- Apply → OK

Update WebAPL Configuration

- Under Modules of XPRESSIONS expand WebApl and double-click on Edit Settings
- Update *Bind Address* from 10.82.53.241 to *NEW_WIN_1_IP*
- Apply → OK

Update OSTM IP address

- Select Settings → Options → tab OSVTM
- Update *Server Address* from 10.82.53.249 to *NEW_WIN_2_IP*
- Apply → OK

Exit XPR Monitor – System Logging

Note: Please update any manual custom configuration on your XPR server to correspond to the new IP addresses according to the *New IP schema design, where applicable.*

5.9 Contact Center

Update OSV IP address for Contact Center

- Login to Win1, via console or RDP using *NEW_WIN_1_IP*
- Start > All Programs > OpenScape Contact Center Enterprise > *Manager* → Login
- Go to Tools > Options > Voice > tab Communications Platform
- Update CSTA Signaling Manager Settings from 10.82.53.231 to
    - NEW_OSV_IP - for OSV Simplex
    - NEW_OSVN1_SIG_IP - for OSV Cluster
- *Apply* → *OK* (restart if prompted)
- Exit the Contact Center Manager

Note: Windows 1 VM MAC address is assumed to remain the same, so OpenScape Contact Center license file is not affected.

Update IP address for Contact Center clients

The server(s) that are running Contact Center clients must be updated according to the *New IP schema design*

- In case, *hosts* file is used for name resolution, please update local *hosts* file
- In case, corporate DNS is being used, please update accordingly

5.10 Concierge (OSCC-E)

Login to Win1, via console or RDP using *NEW_WIN_1_IP*

Select System Management → Login

- Basics → Basic Services → Log transfer settings → OpenScape Trace Manager Settings → Host Name
    - If configured with IP address, please update IP address from 10.82.53.249 to *NEW_WIN_2_IP*
- *Resources* → *PABX Connections* → Select *Site ID* with PABX Host Name 10.82.53.231 → *Modify* button →
    - tab *General* → update *PABX Host Name* IP by replacing 10.82.53.231 with
        - NEW_OSV_IP - for OSV Simplex
        - NEW_OSVN1_SIG_IP - for OSV Cluster
    - tab Synchronization → OSV Export Settings → update OSV Management Server Host Name by replacing 10.82.53.229 with
        - NEW_OSV_IP - for OSV Simplex
        - NEW_OSVN1_MGMT_IP - for OSV Cluster
    - OK
- Applications → Concierge
    - Under Concierge Provider Service → update Default Registrar IP by replacing 10.82.53.231 with
        - NEW_OSV_IP - for OSV Simplex
        - NEW_OSVN1_SIG_IP - for OSV Cluster
    - Under Extended Concierge Provider Service Settings → update Local IP (primary) by replacing 10.82.53.241 with NEW_WIN_1_IP
- Select *Action* (top of the page) → *Publish Installation data* → Select Yes to restart

Note: At this point, configuration on all applications on OSEE Windows 1 server have been updated. It is highly recommended to restart the widows server

Update IP address for Concierge clients

The server(s) that are running Concierge clients must be updated according to the *New IP schema design*

- In case, *hosts* file is used for name resolution, please update local *hosts* file
- In case, corporate DNS is being used, please update accordingly

5.11 Composer

Update the IP addresses based on the *New IP schema design*

Login to Composer, using NEW_UC_IP :

- Under *operator,* select *Settings* and update, where applicable, any IP address, according to the *New IP schema design*.

Note : Please note that in the bullets below, default alias is used for each host added to Composer.

- OSV Host → ... → Edit → Update *FQDN or IP Address*
  - for OSV Simplex : 10.82.53.229 → NEW_OSV_IP
  - for OSV Cluster :
    - 10.82.53.229 → NEW_OSVN1_MGMT_IP
    - 10.82.53.230 → NEW_OSVN2_MGMT_IP
- UC Host → ... → Edit → Update *FQDN or IP Address* from 10.82.53.233 to *NEW_UC_IP*
- Windows Host 1 → ... → Edit → Update *FQDN or IP Address* from 10.82.53.241 to *NEW_UC_IP*
- Windows Host 2 → ... → Edit → Update *FQDN or IP Address* from 10.82.53.249 to *NEW_UC_IP*
- SBC THIG → ... → Delete → Delete

5.12 OSBs & SBCs

All OSB and SBC servers (except SBC-THIG) of the solution must be updated to reflect the *New IP schema design.*

For every OSB and SBC server, proceed with the following updates (when applicable):

- Login (either locally or via cmp) and navigate
- System → Licenses → Under General update License server IP address : OLD_THIG_WAN_IP → NEW_UC_IP → OK
- Network/Net Services → DNS → Client→ DNS server IP address : replace OLD_THIG_WAN_IP with
  - NEW_OSV_IP - for OSV Simplex
  - NEW_OSVN1_SIG_IP - for OSV Cluster
  - OK
- (only for OSBs) Network/Net Services → DNS → Server → DNS Configuration → IP masters/forwards : replace OLD_THIG_WAN_IP with
  - NEW_OSV_IP - for OSV Simplex
  - NEW_OSVN1_SIG_IP - for OSV Cluster
  - OK → OK

- VOIP → Sip Server settings
  - for OSV Simplex : under Node 1 update Primary server IP address : OLD_THIG_WAN_IP → NEW_OSV_IP
  - for OSV Cluster :
    - under General → set Comm System Type : Collocated
    - under Node 1 update Primary server IP address : OLD_THIG_WAN_IP → NEW_OSVN1_SIG_IP
    - under Node 2 update Primary server IP address : OLD_THIG_WAN_IP → NEW_OSVN2_SIG_IP
  - OK
- Diagnostics & logs → Continuous Tracing → Server : update IP address OLD_THIG_WAN_IP → NEW_WIN_2_IP → OK
- Alarms → tab SNMP Configuration → Under SNMP v2c Trap Destinations update IP Address : OLD_THIG_WAN_IP → NEW_UC_IP → OK
- Apply changes

Repeat steps for all OSB and SBC servers of the solution

5.13 Third party & other OpenScape Applications

Please note that all third party applications connected to the OSEE solution must be updated manually to reflect the *New IP schema design*

The same applies for OpenScape Applications that have been connected manually after the automated deployment of the solution.

5.14 Update Certificates

For any component, please update any custom certificate that is based on an IP address of the solution.

6 Post migration actions

Please note that older application backups, cannot be used to restore the OSEE solution anymore.

It is highly recommended to delete previous backup files prior to taking new backups (manually or via Composer).

In case, Composer was used to take backups, you will need to delete the corresponding folders manually. Folders are named based on the IP of the application.

The location of these folders depends on the repository option:

- default HD (builtin) repository: path is /opt/cmpnext/BACKUPS/ followed by a string corresponding to the solution id
    - execute : cd /opt/cmpnext/BACKUPS/<solution-ID-string>/solutions
    - delete any 10.82.53.xxx folder -> e.g *rm -rf 10.82.53.227*
    - execute : *ll | grep "10.82.53."* -> expected output : 0 entries
    - execute : cd /opt/cmpnext/BACKUPS/<solution-ID-string>/applications
    - delete any 10.82.53.xxx folder -> e.g *rm -rf 10.82.53.227*
    - execute : *ll | grep "10.82.53."* -> expected output : 0 entries
- FTP/SFTP repository : path based on repository settings followed by a string corresponding to the solution id
    - based on the OS, navigate to path + <solution-ID-string> + solutions -> delete any 10.82.53.xxx folder
    - based on the OS, navigate to path + <solution-ID-string> + applications -> delete any 10.82.53.xxx folder

Proceed to take new backups (manually or via Composer).

At this point, in order to revert the migration procedure, it is possible only by restoring the snapshots for all OSEE VMs that were taken before applying the new IP address schema. Changes related to clients (e.g. phones, application clients etc.), OSBs and SBCs must be reverted manually.

Based on "Best practices for using VMware snapshots in the vSphere environment (1025279)", do not use a single snapshot for more than 72 hours.

Once, the solution has been verified fully functional, please procced to :

- Power off and delete the SBC THIG VM(s)
- Delete snapshots that were taken before applying the new IP address schema