Unify OpenScape Business

myPortal @work
Scenarios & Configuration

Tutorial

V2.4 – April 15th, 2021

Trusted Partner for your **Digital Journey**

Atos

Content

Disclaimer

This tutorial is intended for trained OpenScape Business technicians.

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of the contract.

Availability and technical specifications are subject to change without notice.

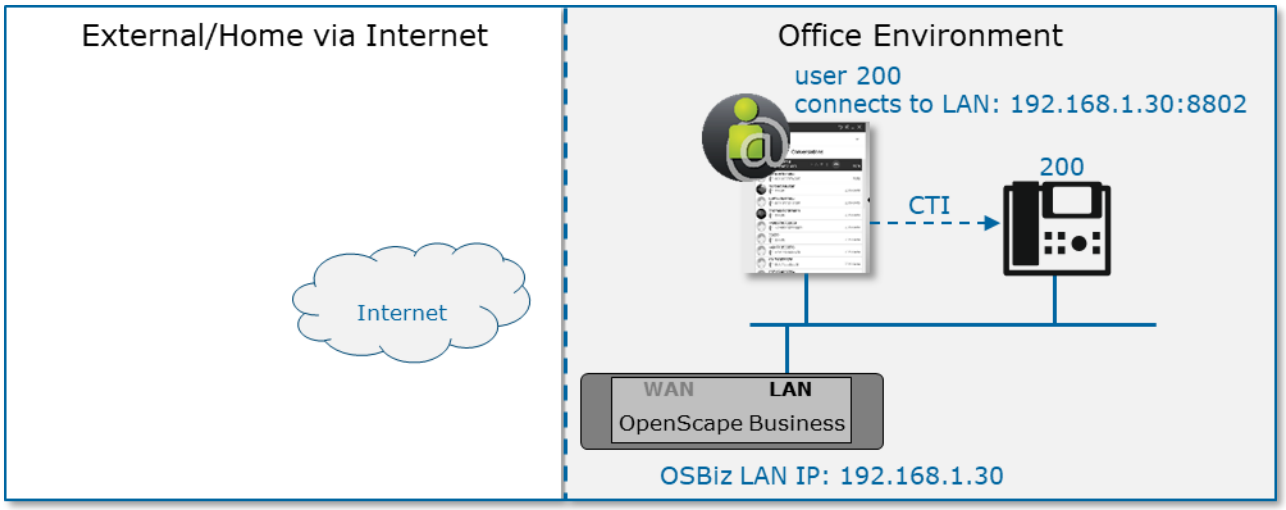
The following description refers to myPortal @work within OpenScape Business V3R0 / V3R1.

1 myPortal @work user configuration

myPortal @work is a combination of a UC client and a VoIP client and those two functionalities require the following configurations/licenses based on different UC modes (Smart/UC Suite) and use cases.

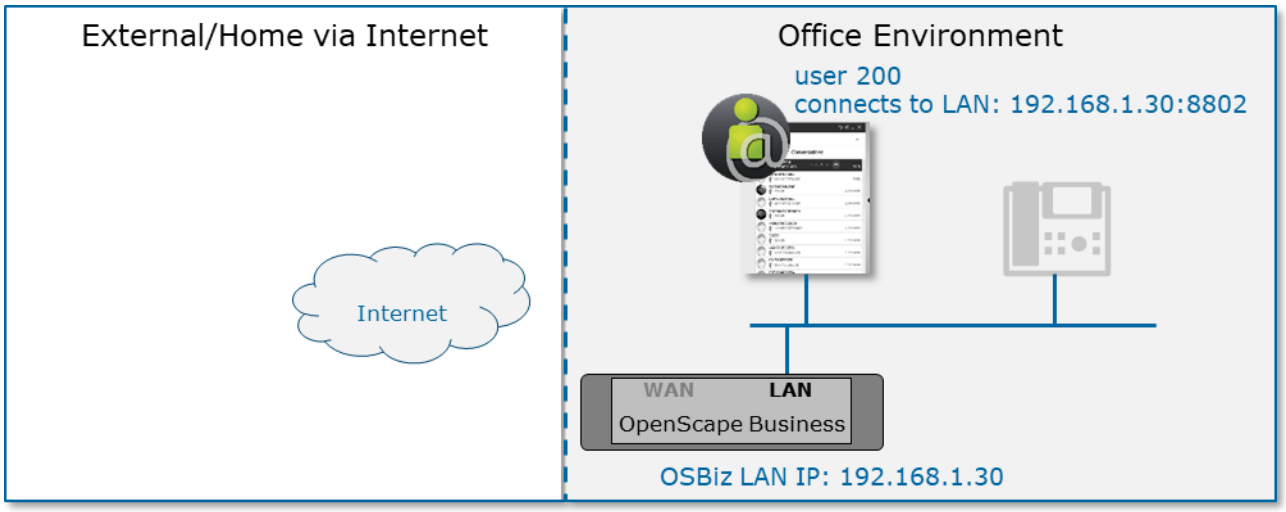
1.1 Local LAN configuration - UC and CTI client only

myPortal @work is used as UC and CTI client for an associated desk phone without VoIP.



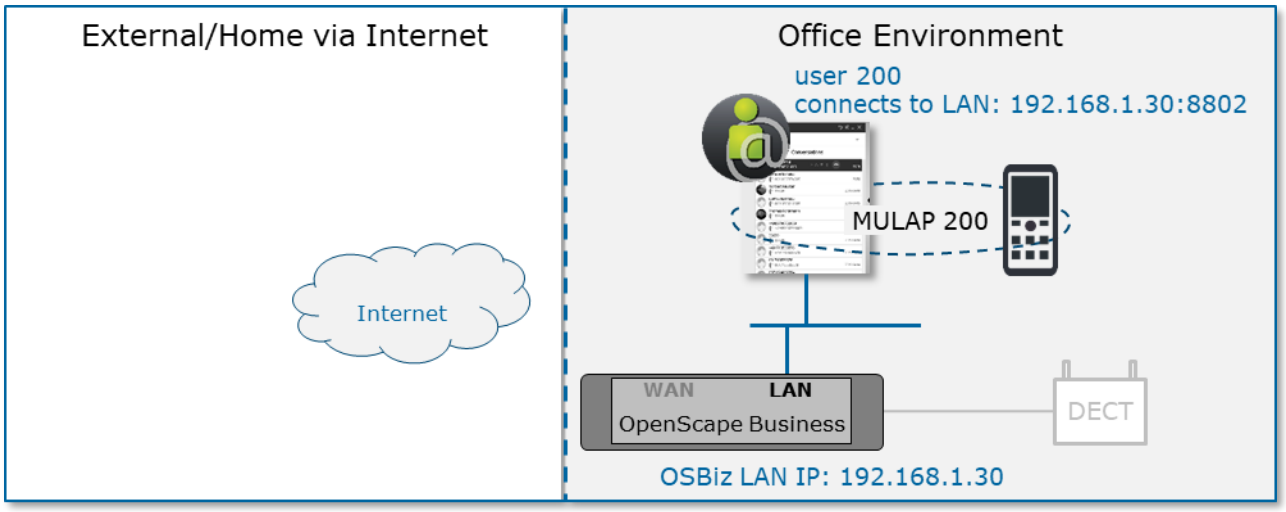
- **Licenses**: UC user or Groupware User
- **myPortal @work login:** in the login screen set your login username/password / **LAN IP address**:8802

1.2 Local LAN configuration - UC and VoIP client



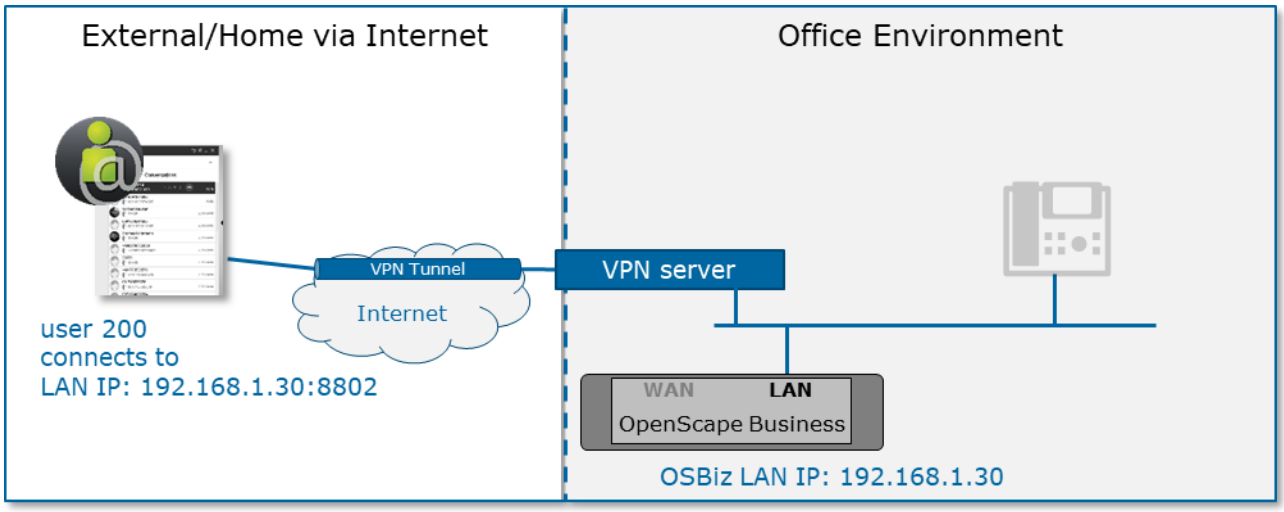
- **Licenses*:*** *IP* User **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set your login username/password / **LAN IP address**:8802
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- STUN connectivity in the client is not needed for pure inhouse connections. Nevertheless, this is required in some hybrid scenarios with other users using myPortal @work VoIP via pubic internet.
  In order to check STUN connectivity, go to Settings > VoIP > Advanced ICE settings > Check ICE status.

1.3 MULAP user configuration (Local LAN)



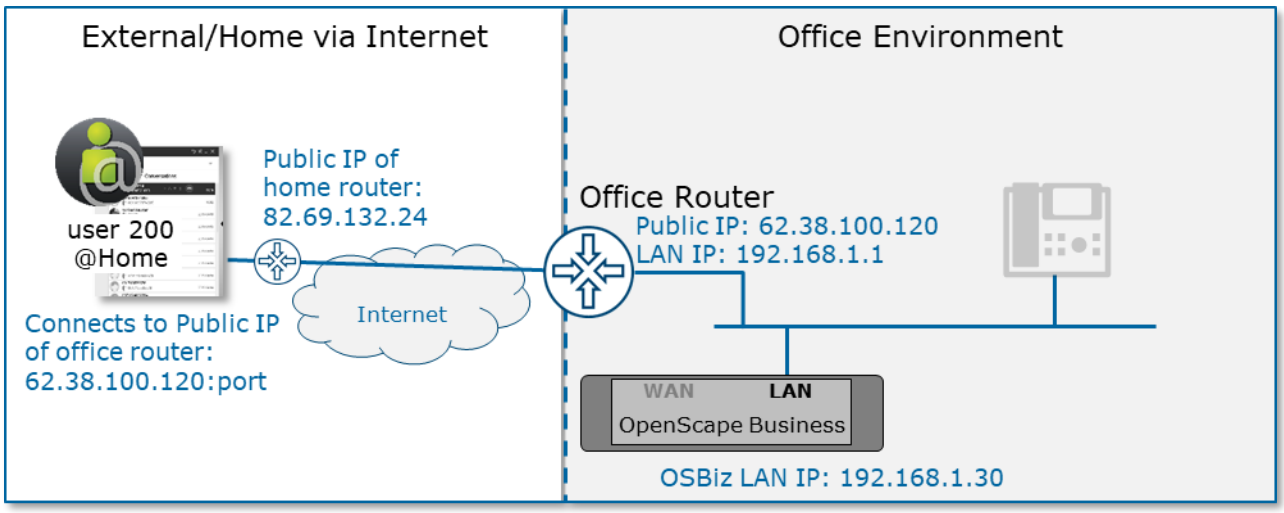
- **Licenses**
  - **myPortal @work**: *IP* User **and** *UC* User or *Groupware* license
  - other Mulap device - in this example DECT: TDM User license or IP User *(Mulap configuration is recommended for combination with TDM or DECT devices, but could also be used with an IP device. In case of an IP device see also chapter 1.8 "Deskshare user via local LAN" and 1.9 "Remote Deskshare user via VPN").*
- **myPortal @work login:** in the login screen set your login username/password of the *MULAP number* / **LAN IP address**:8802
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> choose the controlled device and then enable VoIP
- STUN connectivity in the client is not needed for pure inhouse connections. Nevertheless this is required in some hybrid scenarios with other users using myPortal @work VoIP via public internet.
  In order to check STUN connectivity, go to Settings > VoIP > Advanced ICE settings > Check ICE status.

1.4 Home user with VPN connection configuration



- **Licenses:** *IP* User **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set your login username/password / **LAN IP address**:8802
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- STUN connectivity is mandatorily needed. In order to check STUN connectivity go to Settings > VoIP > Advanced ICE settings > Check ICE status.

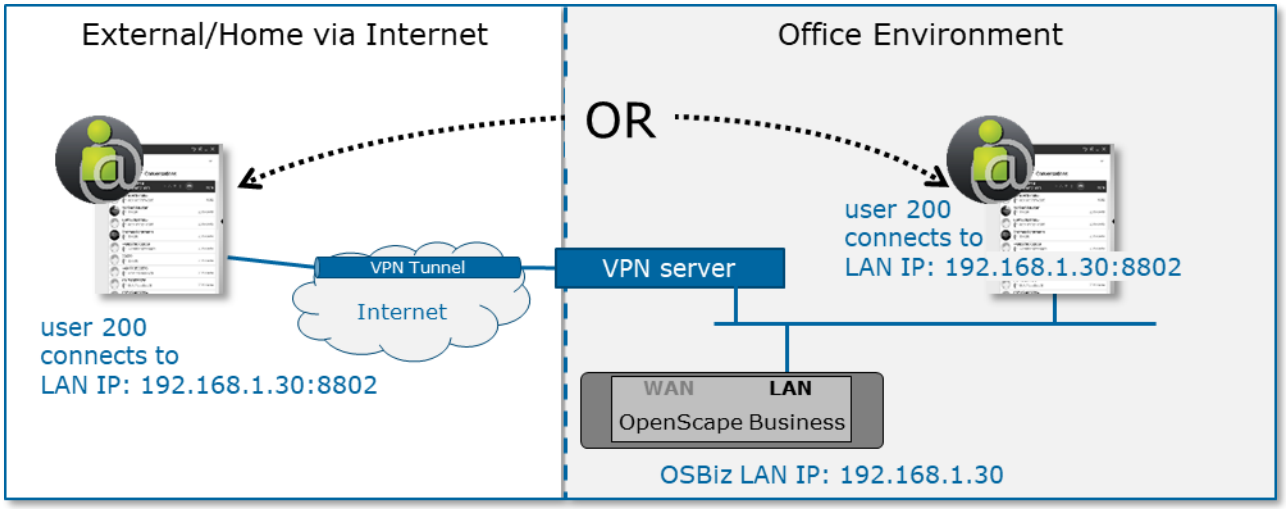
1.5 myPortal @work via public Internet



- **Licenses:** *IP* User **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set your login username/password / **Public IP address**:port configured from the administrator.

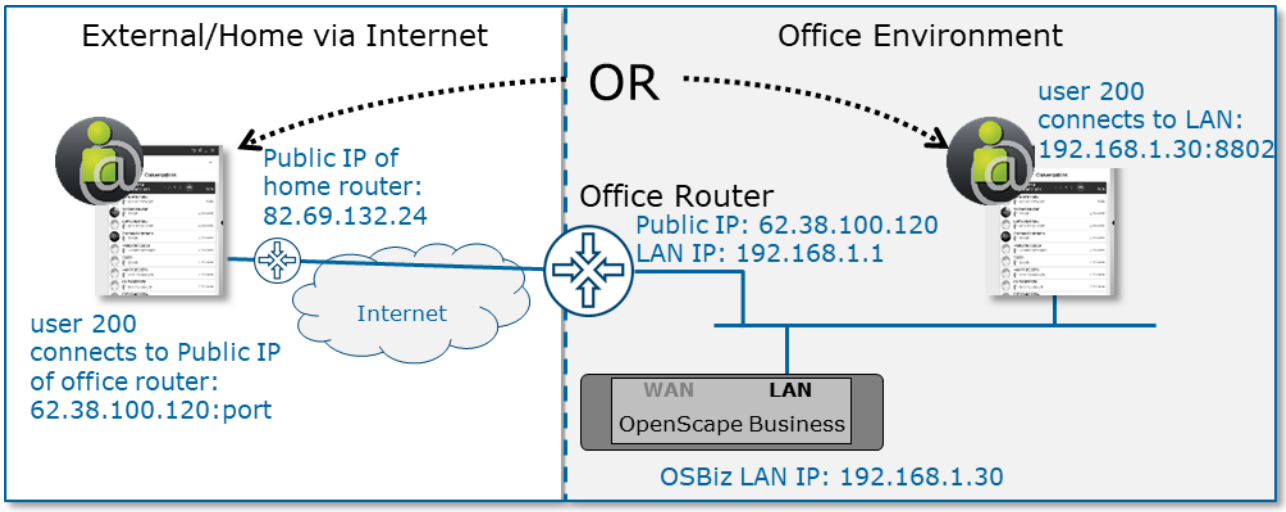
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- Prepare the network environment as described in chapter 2 “Configuration steps to use myPortal @work via the internet”
- SBC flag is not required for myPortal @work. It is only needed if you use a Hardware device.
- Please do not use the OSBiz WAN interface for connecting to the internet when using myPortal @work via Public IP. If this is done internal SBC will detect the Public IP address of the WAN interface and will use this in the communication between the client and the OSBiz which will lead to payload issues. Proposed configuration: Connect the ITSP via the LAN interface. This can be done via the normal ISP router or via a second router and static routes.
- STUN connectivity is needed. In order to check STUN connectivity go to Settings > VoIP > Advanced ICE settings > Check ICE status.

1.6 Home user with VPN and local LAN configuration (e.g. Moving from office to home and back)



- **Licenses:** *IP* User **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set your login username/password/ **LAN IP address**:8802
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- myPortal @work can be used in both environments without changing the settings.
- STUN connectivity is mandatorily needed. In order to check STUN connectivity, go to Settings > VoIP > Advanced ICE settings > Check ICE status.

1.7 myPortal @work via public Internet and local LAN configuration (e.g. moving from office to home and back)



- **Licenses:** *IP* User **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set your login username/password/ **LAN IP address**:8802 and **Public IP address**:port configured from the administrator.
  By configuring both addresses there is no need to use a second profile when moving from office to home and back.
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- Prepare the network environment as described in chapter 2 "Configuration steps to use myPortal @work via the internet"
- SBC flag is not required for myPortal@work. It is only needed if you use a Hardware device.

Please note for VoIP registration:

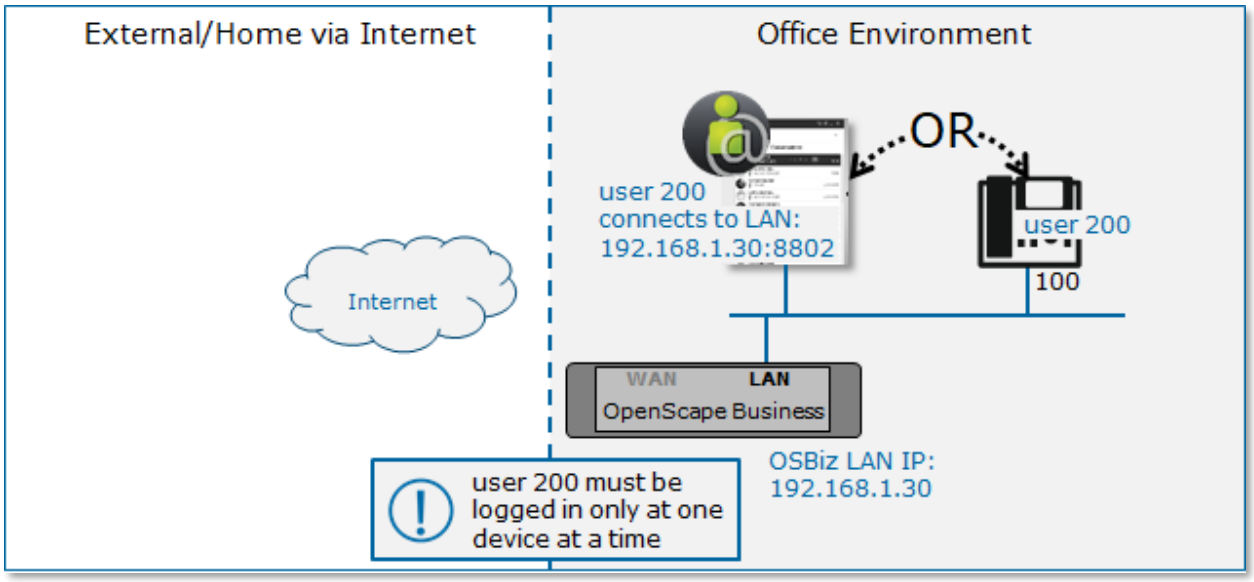
In case both local and home user are used, the user should have only one VoIP connection either in home or in office.

Please note for UC:

When the user wants to be connected in UC at the same time in more than one place:

- **UC Smart** mode: UC client can be connected at the same time from home and from office, but only one VoIP client is supported in this scenario and the VoIP functionality from the other client should be unregistered.
- **UC Suite** mode: Please check *paragraph* **"**Combination of myPortal @work with other UC Suite clients and license configuration**" Only one** myPortal @work client **is allowed.**

1.8 Deskshare user via local LAN

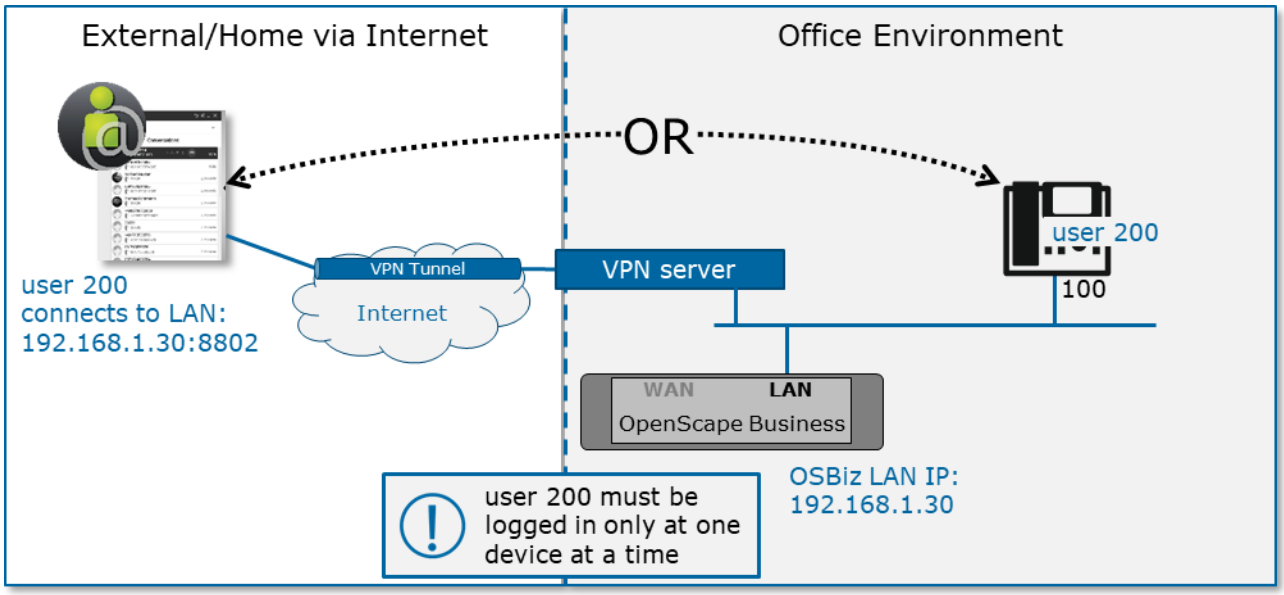


- **Licenses:** *Deskshare* license **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set the login of the deskshare extension username/password/ **LAN IP address**:8802
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP

  Example: Device uses dummy number = "100"
  *Connect to "100" with your DeskPhone as deskshare e.g. 200 using service code *9419.*
  Now, in order to use myPortal @work with user 200, the deskphone is automatically logged out and returns to the dummy number "100". When switching back to deskphone again please ensure that myPortal @work is unregistered (→ user must exit the application or log out).

1.9 Remote Deskshare user via VPN

The same configuration as described in the previous chapter is also supported for home user via VPN.

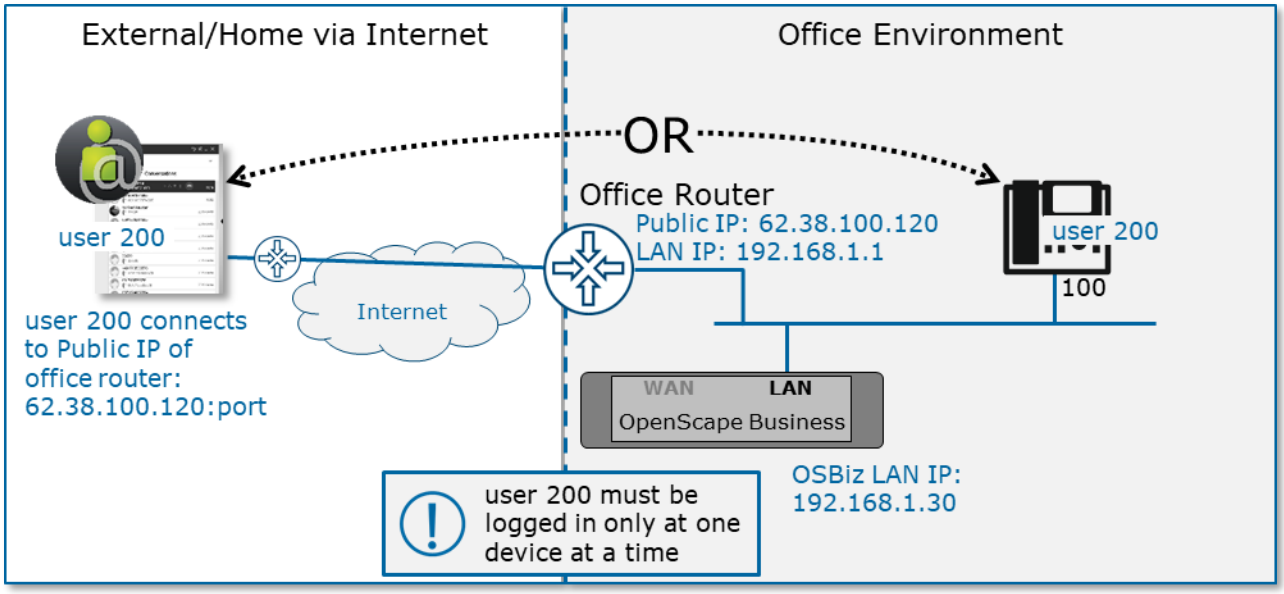


- **Licenses:** *Deskshare* license **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set the login of the deskshare extension username/password/ **LAN IP address**:8802
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- STUN connectivity is mandatorily needed. In order to check STUN connectivity, go to Settings > VoIP > Advanced ICE settings > Check ICE status.

  Example: Device uses dummy number = "100"
  *Connect to "100" with your DeskPhone as deskshare e.g. 200 using service code *9419.*
  Now, in order to use myPortal @work with user 200, the deskphone is automatically logged out and returns to the dummy number "100". When switching back to deskphone again please ensure that myPortal @work is unregistered (→ user must exit the application or log out).

1.10 Remote Deskshare user via public Internet

The same configuration as described in the previous chapter is technically also possible with home users via public Internet. Nevertheless, this is not yet completely tested and therefore described preliminary in this document version.



- **Licenses:** *Deskshare* license **and** *UC* User or *Groupware* license
- **myPortal @work login:** in the login screen set the login of the deskshare extension username/password/ **Public IP address**:8802
- **myPortal @work VoIP registration:** After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- STUN connectivity is mandatorily needed. In order to check STUN connectivity, go to Settings > VoIP > Advanced ICE settings > Check ICE status.

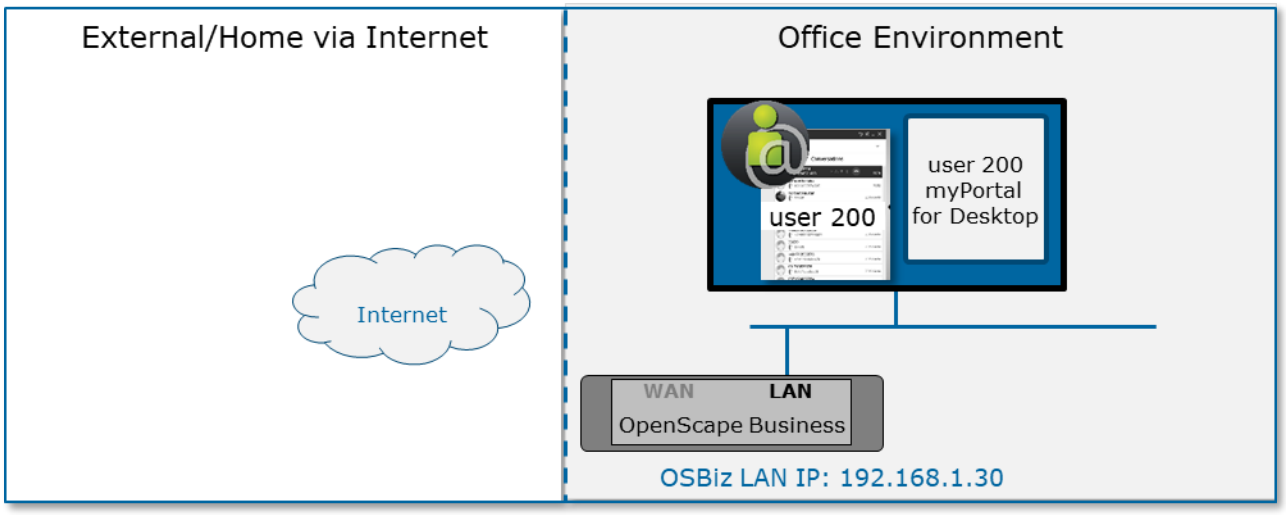
  Example: Device uses dummy number = "100"
  *Connect to "100" with your DeskPhone as deskshare e.g. 200 using service code *9419.*
  Now, in order to use myPortal @work with user 200, the deskphone is automatically logged out and returns to the dummy number "100". When switching back to deskphone again please ensure that myPortal @work is unregistered (→ user must exit the application or log out).

1.11 Combination of myPortal @work with other UC Suite clients and license configuration

The configurations described in this chapter are also supported for home user via VPN.

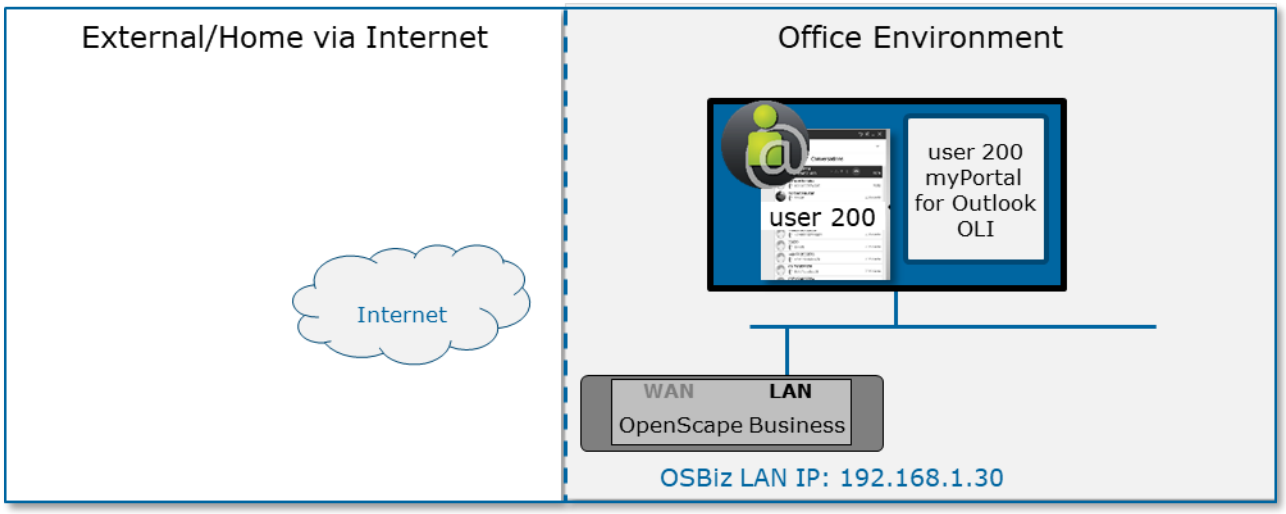
1.11.1 UC user license

The same user can be connected in parallel with myPortal @work and myPortal for Desktop



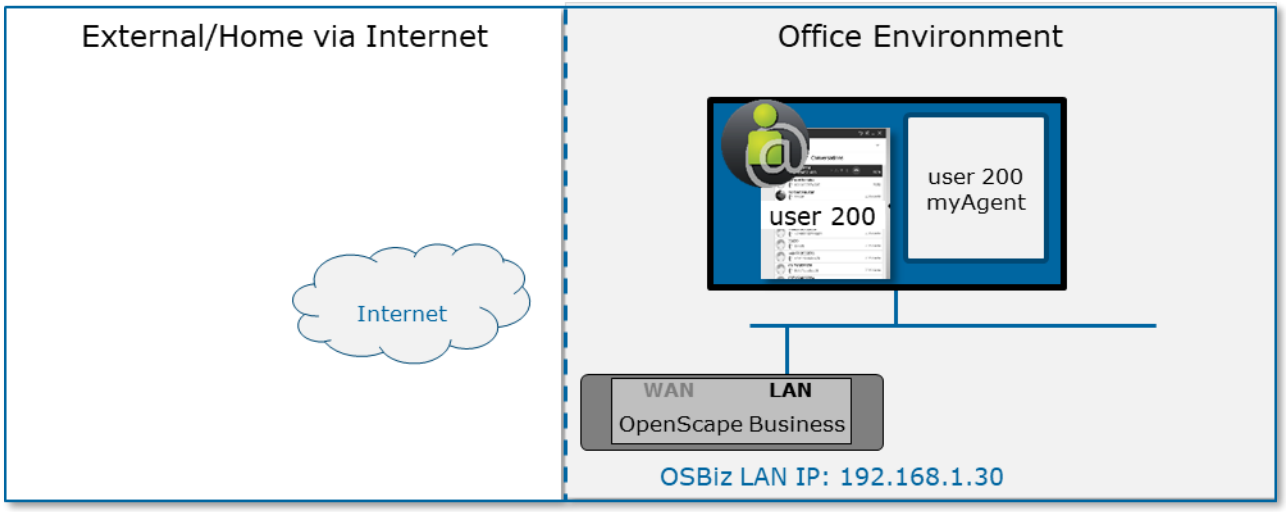
1.11.2 Groupware license

The same user can be connected in parallel with myPortal @work and OLI



1.11.3 Combination of IP, UC user and myAgent license

User can have myAgent and myPortal @work VoIP as a softphone in parallel

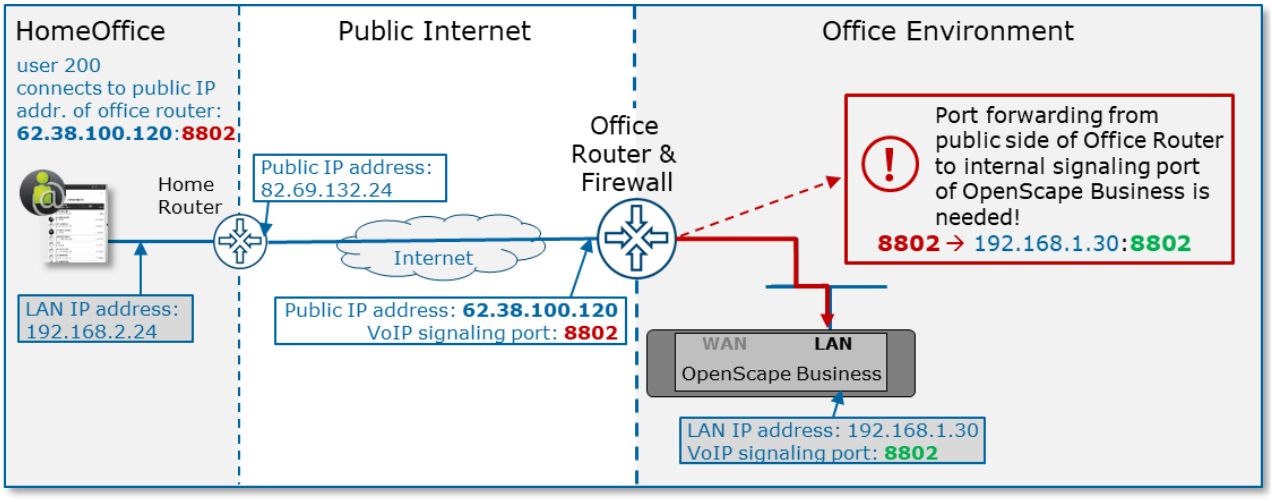


Please note that myAgent's "Free Seating" functionality (the agent can select the phone to be used via a drop-down menu during the logon process) i.e. free selection of a physical device by an agent is not supported in combination with myPortal @work.

2 Configuration steps to use myPortal @work via the internet

2.1 Configuration Overview

In order to use myPortal @work from the internet the OpenScape Business therefore needs to be accessible from the internet as well.
For all examples within this chapter, the following basic network scenario is assumed.



2.2 Network scenario description

The OpenScape Business is located within the office environment, which is connected to the internet via the office router. This router is accessible from the internet either via the public IP address of "62.38.100.120" or via a DNS name.

The myPortal @work client is connected to the LAN within a home or external network, which is connected to the internet via a separated router. The external router is accessible from the internet with the public IP address "82.69.132.24".

2.3 Configuration steps

To use the myPortal @work client on the OpenScape Business via the internet the following components need to be configured accordingly:

- OpenScape Business within the office
- Office router
- myPortal @work / external router

2.3.1 OpenScape Business configuration

- Active STUN support on the system if not already done for an ITSP
- Configure myPortal @work user (SBC flag is not needed for VoIP)

2.3.2 Office router configuration

Since the myPortal @work client must reach the OpenScape Business from the internet and vice versa, the following configuration must be done on the office router to accomplish this:

- HTTPS port forwarding from the external port (default is 8802) to the internal port 8802 of the system
    - External port (default is 8802) -> Office Router -> 192.168.1.30:8802
- Please also check chapter 3.4 Ports and Firewall Settings

2.3.3 myPortal @work and external router configuration

The myPortal @work client needs to connect to the public IP address or DNS of the office internet router on the external port, which is by default 8802 (due to the previously configured port forwarding this will point to the OpenScape Business within the office network).

In most cases nothing additional needs to be configured on the external router but in case of problems please check chapter 3.4 Ports and Firewall Settings and following.

3 Other Configuration Hints & Settings

3.1 STUN server settings

Check chapter "Configuring STUN" in guide "How to configure system device@home" and OpenScape Business V3, my Portal @work, User Guide section "How to add a STUN server"

3.2 Headsets

Every detected sound device / microphone found in the operating system can be used.

3.3 Jabra/Plantronics headset integration

In case of problems with Jabra headset integration, run the application with administrator rights.

In order to use Jabra headset integration, the Jabra device needs to be set as the main microphone device in myPortal @work.

For Plantronics integration, Plantronics hub should be installed.

3.4 Ports and Firewall Settings

Basically, the following ports must be configured for myPortal@work signaling:

- UC functionality & WebRTC / VoIP signaling: 8802

- Default STUN server port: 3478
  If a custom STUN server is configured, a different port may be required.

Configuration of ports for WebRTC / VoIP payload depends on the type of firewall used in the customer environment. In order to run myPortal @work in a customer network environment it is fundamental to understand and check the type of used firewall, either stateful or stateless, and configure the firewall settings together with the responsible IT admin.

To better understand the differences between both type of firewalls please read the following:

- Stateless firewalls are designed to protect networks based on static information such as source and destination.
- A stateful firewall is a firewall that monitors the full state of active network connections. This means that stateful firewalls are constantly analyzing the complete context of traffic and data packets

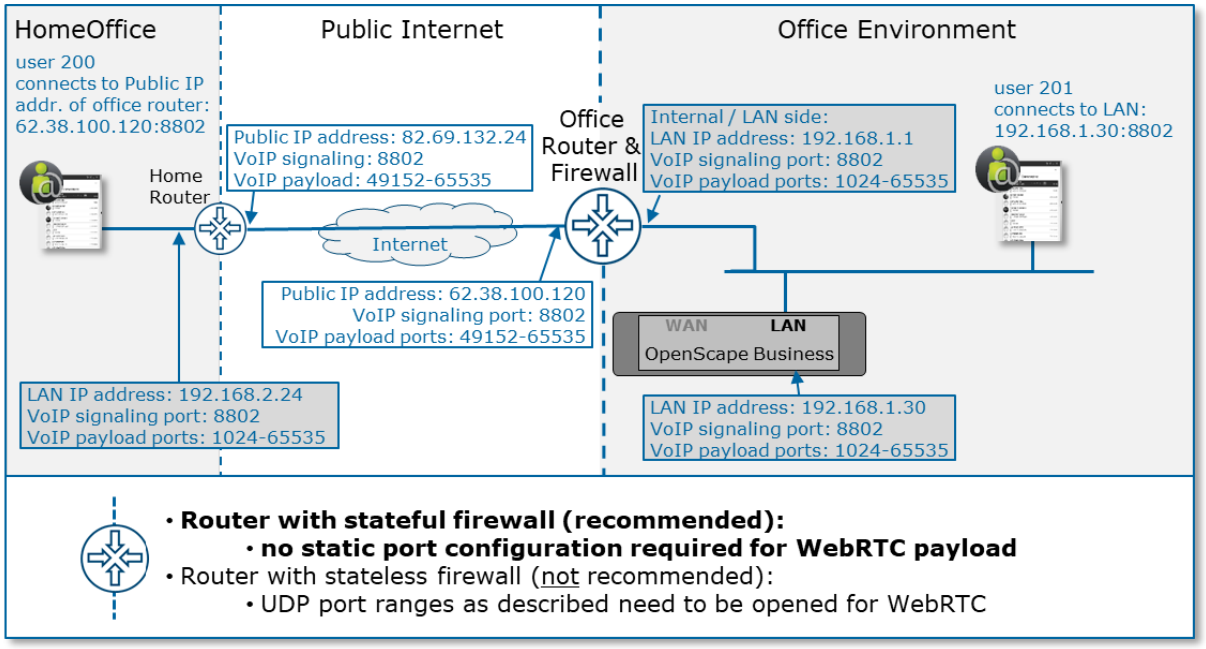
For further information on those firewall types please refer to the internet or relevant technical literature as a source of information.

Atos Unify assumes that a stateful firewall/NAT device is going to be used in order to better protect private customer networks means that this device needs to allow internal outbound connections towards their destination.

The firewall/NAT device will block any packets in the inbound direction, unless it belongs to an already established session (on an ephemeral/dynamic port) which was previously established outbound.

In terms of the port usage nothing needs to be configured within the firewall/NAT device since this will be handled and negotiated automatically when using a stateful firewall.

Using a stateful firewall is the recommended and more secured path to run WebRTC based VoIP solutions.



In terms of a stateless firewall (which is not going to be recommended for VoIP) the following range of UDP source ports for devices inside the customer network needs to be opened for internal payload traffic: 1024-65535.

For all payload traffic which is exchanged via the internet the WebRTC technology uses ports from the UDP port range of 49152-65535. For further information please refer to relevant technical literature as a source of information.

Each networking device on the path between the involved payload endpoints needs to be configured accordingly (e.g. router, firewall, NAT, proxy,..).

Due to the broad port range which needs to be opened, stateless firewall cannot be recommend for VoIP.

	Stateful firewall	Stateless firewall to be opened statically
WebRTC / VoIP signaling port	8802	8802
WebRTC / VoIP payload *UDP port range within local LAN i.e. within customer environment*	dynamic*	1024-65535
WebRTC / VoIP payload *UDP port range used over the public internet*	dynamic*	49152-65535

**: no configuration action needed; ports will be taken dynamically from same UDP port range as listed for stateless firewall*

3.5 Restrictions on VoIP

- In scenarios with multiple calls (e.g transfer, conference, camp on) we recommend disabling the headset integration in case of an error. By deactivating the headset integration flag within myPortal @work only the headset's call control functionality cannot be used, but the headset can still be used as audio device.
- myAgent's "Free Seating" functionality (the agent can select the phone to be used via a drop-down menu during the logon process) i.e. free selection of a physical device by an agent is not supported in combination with myPortal @work.
- Symmetric NAT configuration is not supported.
- Strict firewalls are not supported

4 Troubleshooting Guide

4.1 Connection Timeout

- **As a home user with VPN connection**, should ensure that the user can access the **LAN** address of the system and connect to the LAN address:8802 port.

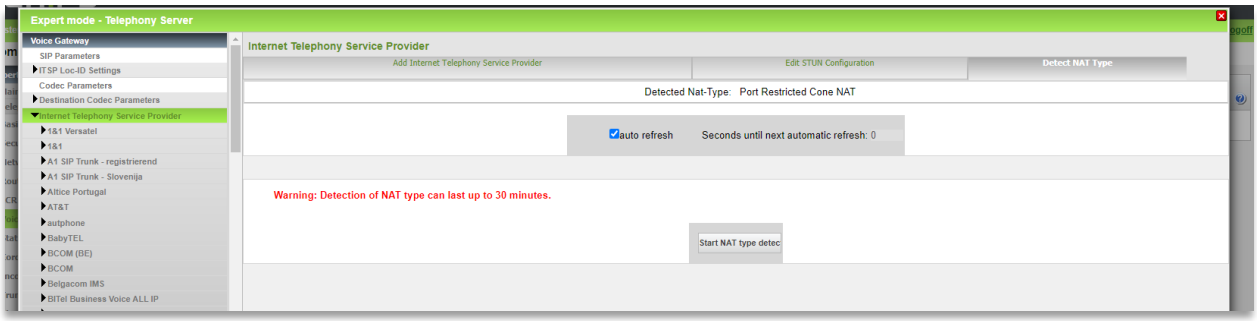
  Troubleshoot message: Error Message "connection time out", Action: check if the user when connected via VPN has a local IP from the VPN network.

- **As a standalone user** ensure that there is no other device or VoIP myPortal @work client registered with the same station number. Please check also in WBM> Expert Mode> Web Services Assistant for the open connections.

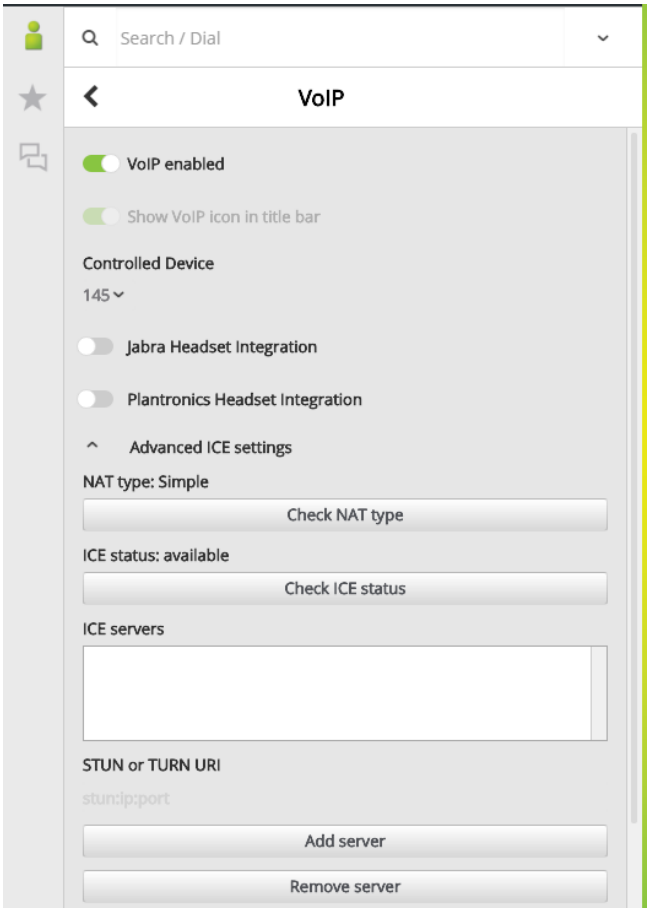
4.2 No Payload

In case of no payload permanent issue:

- Check that allowed ports are open on the firewall. Check chapter 3.4 "Ports and Firewall Settings"
- Check NAT firewall configuration. Symmetric NAT configuration is not supported
- You may detect NAT type from the system (Expert mode > Voice Gateway > Detect NAT type)
- Check stun server connectivity in the system



- Check ICE connectivity in myPortal @work Settings> VoIP > Advanced ICE settings. In case "NAT type" and/or "ICE Status" are not as seen below, network/firewall settings need to be checked by your administrator.



Run "Check NAT type" >

NAT type: ***Simple***

Run "Check ICE status" >

ICE status: ***available***

- Disable headset integration from myPortal @work and perform the scenario again
- Select again audio devices from VoIP settings

5 Further Hints

5.1 SIP ALG (Application Layer Gateway)

If you experience one of the following issues, please check if a SIP ALG is activated on one of the involved routers. There are a few categories of symptoms SIP ALG could affect VoIP connections. It's not always apparent, especially since these issues often happen silently without users knowing.

- One-way audio (only one person can hear the other)
- Client does not ring when called
- Calls drop after being connected
- Calls going straight to voicemail for no known reason

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and
Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us atos.net atos.net/career

Let’s start a discussion together