

# Remote Service Platform v2

RSP.sl Connection Troubleshooting (Issue 1.1)

1.	Overview	3
1.1.	Registrar	3
2.	Generic customer network requirements	4
2.1.	Customer network requirements	4
3.	Buffalo routers	5
3.1.	IP Config Wizard does not connect	5
3.2.	Date/Time settings	5
3.3.	Date lost after a reboot	6
3.4.	WBM not working from RSP	6
3.5.	Additional customer LAN routes needed	7
3.6.	SPoA connections are not working	8
3.7.	Diagnostic logs	9
4.	OpenScape Business	9
4.1.	Error messages in WBM	9
4.2.	Diagnostic logs	10
5.	Windows	11
5.1.	Firewall settings	11
5.2.	Diagnostic logs	11
6.	SLES 11-12 Linux systems	11
6.1.	SPoA routes	11
6.2.	Diagnostic logs	12
7.	Ticket content requirements	13
8.	List of abbreviations in the document	14

# 1. Overview

Connecting a system to the RSP.sl should be straightforward, but there are some scenarios, that can block a successful connection. This document is the result of several years of experience with troubleshooting RSP.sl connections, collecting possible causes and solutions.

There are currently following clients available for RSP.sl connections:

- Buffalo routers
- OpenScape Business
  - X systems (embedded)
  - S and Booster Server systems (SLES Linux based)
- Windows
- SLES 11-12 systems

## 1.1. Registrar

The OpenScape Business systems have an additional feature, the Registrar. The Registrar can register an OpenScape Business system to RSP without having to manually access to the RSP system to create a device entry. Registration is done based on MAC Address, SIEL-ID and Registration ID (called Customer ID within SIRA).

Of course, the final steps (providing credentials, description, changing Customers) still need to be done within RSP manually.

## 2. Generic customer network requirements

### 2.1. Customer network requirements

The RSP.sl technology is based on OpenVPN connections.

OpenVPN is a flexible secure tunneling software, that can work over NAT networks, but there are important network settings, that are required to get a working connection.

The most important settings are enlisted below:

- **Date settings**
  - Please always make sure, that your date and time settings on your device are correct. You should be able to use NTP on your devices, or if that is not available, ensure you have correct time and date set on it. Without correct date and time settings the system might not validate the connection certificates on either side, causing inability to connect to RSP.
- **Firewall and/or Proxy settings**
  - **IP addresses and ports**
    - RSP.sl uses following IP and port combinations for initiating the tunnel from the clients to the RSP.sl load balancers:
      - 188.64.18.50:443 – primary LB
      - 188.64.17.50:443 – secondary LB
    - RSP.sl uses following IP and port combinations for initiating the tunnel from the clients to the RSP.sl Registrar servers:
      - 188.64.18.51:443 – primary Registrar server
      - 188.64.17.51:443 – secondary Registrar server
  - **SSL**
    - SSL must be enabled through the FW to the specific IP addresses using the specified ports, as OpenVPN uses SSL/TLS connections to build up the secure tunnel
  - **OpenVPN Protocol check**
    - Some FW/Proxy servers are set up to check the protocol trying to pass through. As the RSP.sl uses the port 443, it could expect to see HTTPS traffic, but it is in fact OpenVPN traffic. So, if OpenVPN protocol can be explicitly allowed within the FW/Proxy, then this must be enabled.
  - **Package inspection**
    - Some strict FW/Proxy servers might want to check the content of the encrypted packages, like a MITM. RSP.sl (OpenVPN) does not allow MITM setup, to ensure end-to-end security between the client and the servers. If you have such kind of a setup, you must disable it for the RSP.sl connections.
  - **Last resort FW checks**
    - Should everything else fail, you still can check a few facts:
      - Please ensure, that not only outbound, but related inbound traffic is also enabled to be able to build up the RSP.sl connections,
      - While it seems to be obvious, in a setup, where there are multiple FW/Proxy servers it is always a good idea to check, if the system tries to communicate through the one you are investigating (e.g. check for both blocked/allowed traffic),
      - As a very last resort, you should try to disable all the Proxy/FW rules for a few minutes and retest the connection. If it works with disabled Proxy/FW, then you should look further for blocked content, even, if it does not seem to be there.

## 3. Buffalo routers

There are some specific issues/fixes, that apply for Buffalo routers.

### 3.1. IP Config Wizard does not connect

Should the IP Config Wizard not be able to connect to the Buffalo to transfer the configuration data, please follow this procedure:

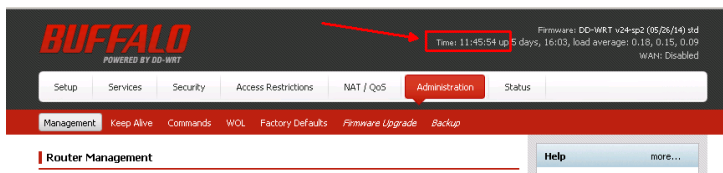
- do a 30/30/30 reset, to reset to factory settings
  - meaning, you keep pressing the reset on the router for 90 seconds
    - The first 30 seconds the router should be switched on (plugged in to the power outlet)
    - The second 30 seconds the router should be switched off (without power)
    - The third 30 seconds the router should be switched on (plugged in to the power outlet)
- Reboot the router (power off-on)
- After the router is up, wait 6 Minutes, and reboot it again
  - In this first 6 minutes after the reset the SSH public/private keypair is generated, to make it possible to connect via SSH, making it available for IP Config Wizard

If you did all the above correctly, and still cannot connect to the router, chances are high, that you've got a non-custom firmware router, or it does not work.

### 3.2. Date/Time settings

Buffalo has a Linux console like interface, where you can set the current date and time, or if you are familiar with Linux environments, you can also do it via console.

- Buffalo routers do not have an internal clock, you should always set up NTP for the Buffalo, where possible, to avoid issues
- You can check the current date/time setting on the Buffalo
  - on the WBM



**Figure 1 – Checking the time on WBM**

- o or running the **date** command on the console:

```
[SSH] Server Version dropbear_2014.63
[SSH] INFO: Host Banner
DD-WRT v24-sp2 std (c) 2014 NewMedia-NET GmbH
Release: 05/26/14 (SVN revision: 20026)

[SSH] Logged in (password)

=====
!! WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING !!

      This system is managed remotely
Unauthorized access and use of this system is strictly prohibited.

!! WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING !!

=====

BusyBox v1.21.0 (2014-05-26 09:40:52 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

root@A13B69:~# date
Wed Apr  3 11:48:41 UTC 2019
root@A13B69:~# _
```

**Figure 2 – Checking the time on console**

### 3.3. Date lost after a reboot

As the Buffalo router does not have an internal clock, it does not store the current date and time between restarts. As the system in some exceptional cases might not have an NTP setup, then the RSP.sl server is used through the tunnel to provide a safe NTP date.

However, an initial date is necessary, to be able to connect at all. For this workaround there is an NVRAM variable called **no\_ntp\_time** that is used as a reference date at startup of the router. To check or update the value of this variable, you can use following command line commands:

- Check current value of the NVRAM variable:

```
nvramp get no_ntp_time
```

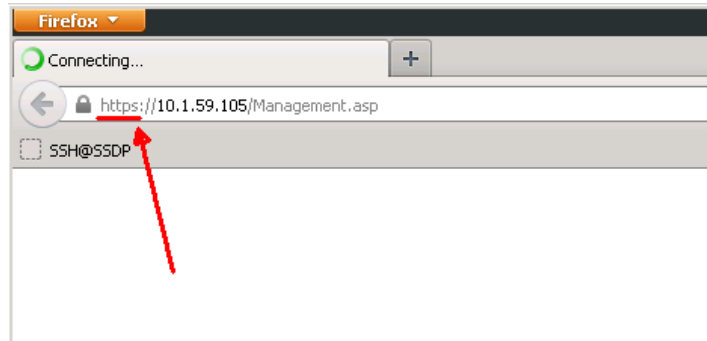
- Update the value of the NVRAM variable with the following 2 commands:

```
nvramp set no_ntp_time="201904040600"
nvramp commit
```

### 3.4. WBM not working from RSP

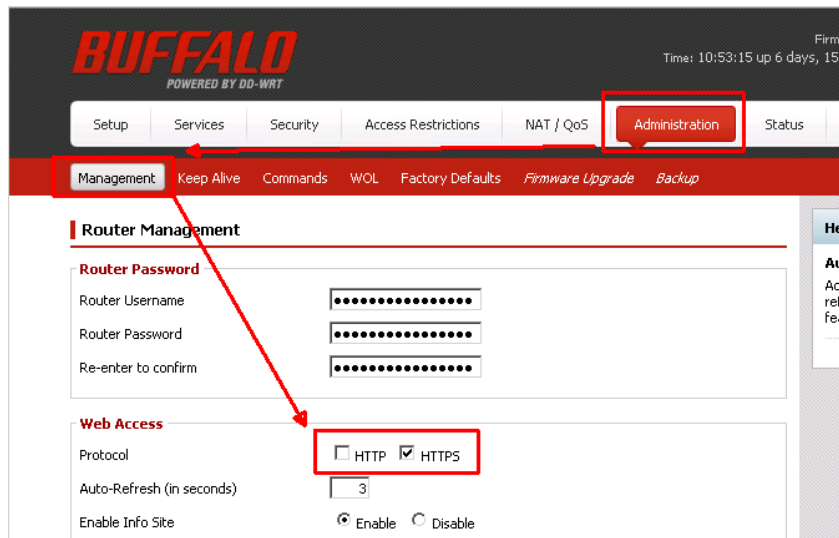
RSP tries to access the Buffalo router's WBM using the HTTPS protocol. On older version of router firmware, it might happen that the HTTP access is enabled, but the HTTPS is not. In that case the connection from RSP will fail to the system.

You should be able to connect to the router, if you change the **https://** prefix to **http://** in the browser, as seen on the screenshot below:




**Figure 3 – Access through HTTP instead of HTTPS**

After loading the WBM of the router, you should set the correct properties to avoid the need of this workaround in the future:



**Figure 4 – Set correct web access protocol**

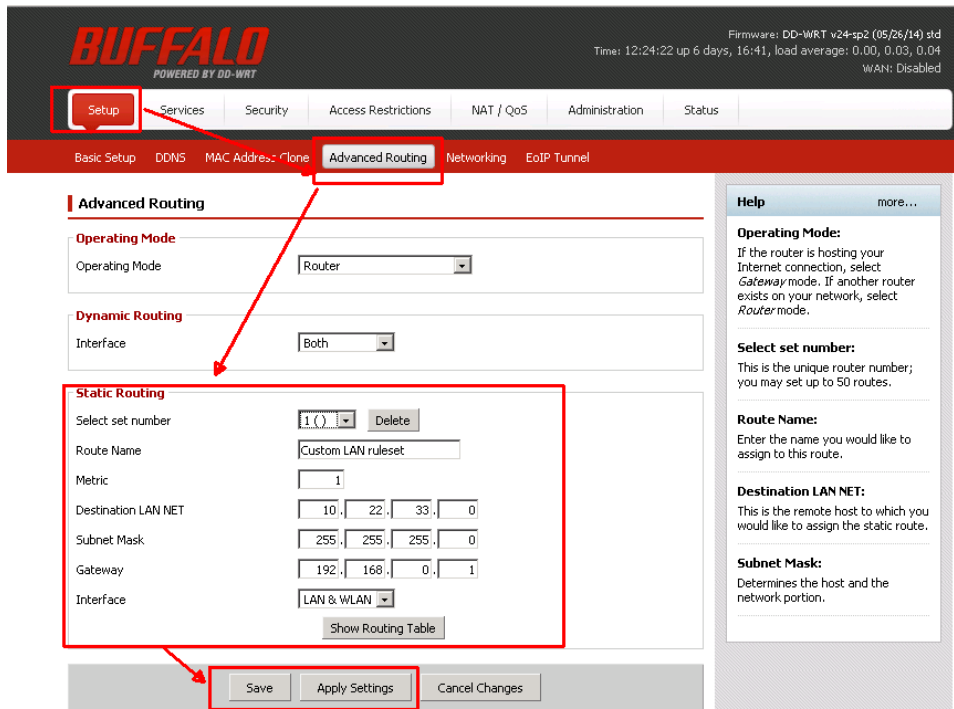


If you do changes on the WBM, do not forget to always save the settings at the bottom of the page, to make the changes persistent even after reboot.

### 3.5. Additional customer LAN routes needed

If you need custom LAN routes to manage different gateways for different address ranges, you can use the WBM to create persistent routes:

1. Head to **Setup -> Advanced Routing**
2. Select a free **set number**
3. Fill necessary data (**Router name, Metric, ...**)
4. Press **Save** and **Apply Settings**



**Figure 5 – Custom LAN routing**

### 3.6. SPoA connections are not working

SPoA connections use the iptables (netfilter package) on the router to automatically create the forwarder rules. Should your routes get inconsistent, you should be able to reset the SPoA routes on your router.

1. Depending on which version of connection plugin you have installed, you might need a different set of commands.
  - a. To check, which commands you need, you need to check, where the routes are coming from, by running the following command:

```
ls /jffs/openvpncl/cp-spoa-routes.sh
```

If you find such a file, you should simply execute:

```
/jffs/openvpncl/cp-spoa.sh -r
```

- b. If you did not find that file, you will have to execute following set of commands:

```
nvrn set spoa_history=""
nvrn commit
grep '\-action delete' /tmp/openvpncl/cp-spoa-history.sh | sh -x
cat /dev/null > /tmp/openvpncl/cp-spoa-history.sh
```

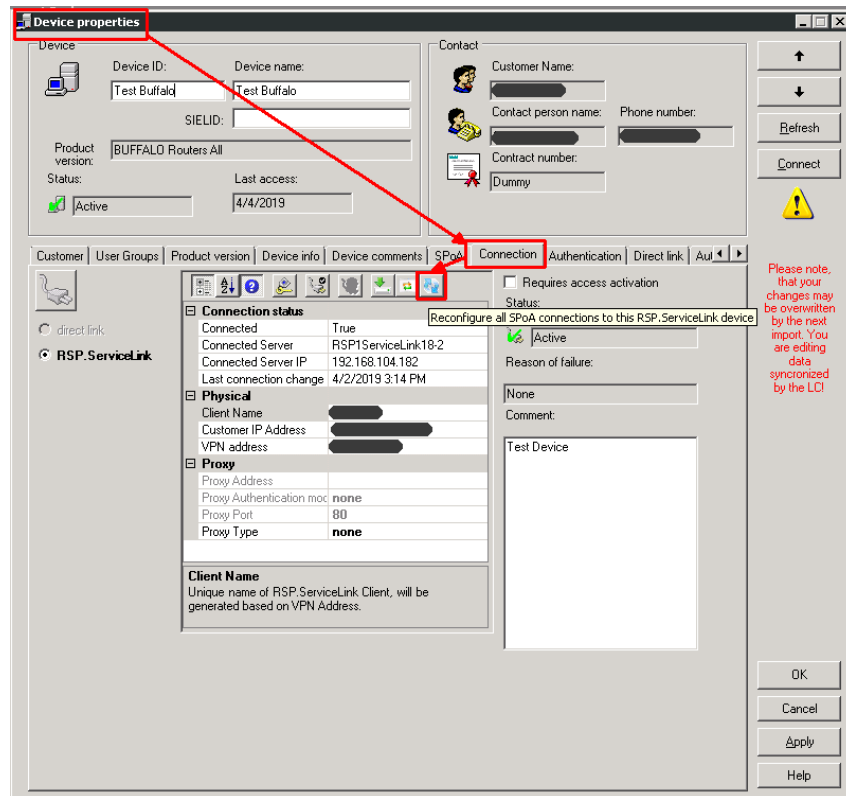
This will remove all the stuck rules on your router. If you want, you can also do a reboot of the router at this point, while it is not necessary.

2. Reconfigure all SPoA connections

Go to the RSP, open Equipment Explorer, navigate to your device, open the device properties.



There you need to go to the **Connection** tab, and press the "Reconfigure all SPoA connections to this RSP.ServiceLink device"



**Figure 6 – Reconfigure all SPoA connections**

### 3.7. Diagnostic logs

If the above sections did not help you to get the router online, you can still check the OpenVPN log file for any errors.

The log file is **/var/log/openvpncl**

## 4. OpenScape Business

With Openscape Business systems it is important to have up-to-date system, as several issues of previous versions got already corrected in new releases.

If you have the latest version, and are still struggling getting it connected to RSP, then you should check the Chapter 2 for possible generic issues.

### 4.1. Error messages in WBM

During registration or connection activation you might experience different behaviour based on the specific issue you are facing.

Here is a list about the most common messages OpenScape Business reports during a failed registration/activation attempt:

- **Configuration error**

The system could not connect to the RSP. This happens most of the cases because something in the customer LAN configuration is invalid.

- **Certificate Error**

RSP stores a different certificate for given client name, like the one stored on the Openscape Business, or the certificate has been revoked on the OpenScape business. In such a case the registration has to be repeated.



Please note! There is a 10 minutes activation window after the registration of the OSBiz system, to get it to the *active* state within RSP. Should that not happen within 10 minutes, the registration will be considered failed, and the registered device entry gets deleted from the RSP, resulting a **Certificate Error**.

As there is also a few minutes sync delay in the status, please always remember to immediately press **activate** on the WBM after a successful registration of the OSBiz system..

- **Wrong Credentials**

Registration user id and password combination is invalid. Both can be checked by partner administrator users within the **Partner Administration** tool in RSP.

- **Device Already Exists**

Error message, that points to the fact, that either MAC address, SIEL-ID or Customer ID mismatches.

The main statement is, that during registration:

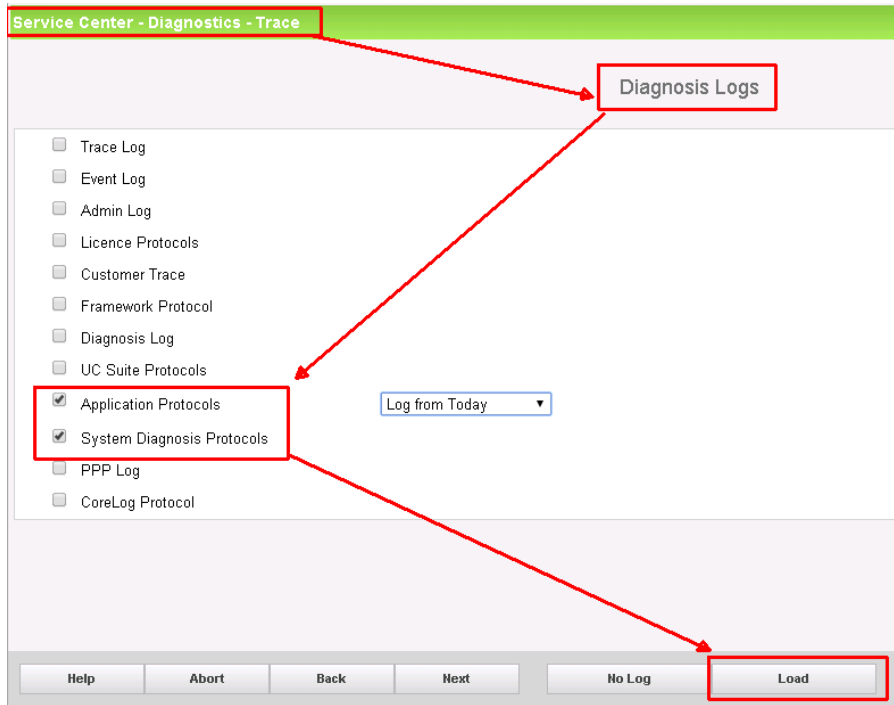
- SIEL-ID must be unique within RSP
- MAC address must be unique within RSP
- Device can only be re-registered, if SIEL-ID, MAC address and Customer ID is the same, as stored in SIRA, otherwise it is considered a duplicated registration attempt.

- **User Locked**

If there were several unsuccessful registration attempts (because of wrong registrar password), the registrar user gets locked. In that case no registrations can be done, till the registrar user is unlocked, either after *40-90 Minutes*, or manually in the **Partner Administration** tool in RSP.

## 4.2. Diagnostic logs

If you create a ticket, it is always helpful to provide diagnostic logs to the ticket. Related to the RSP.sl following logs should be provided:



**Figure 7 – OSBiz diagnostic logs for RSP.sl**

## 5. Windows

### 5.1. Firewall settings

We often have the report with Windows RSP.sl clients, that the client connects but the RDP session does not work for the specific system. This is most of the cases caused by Windows Firewall. Please keep in mind, that the TUN/TAP network interface might not be in the same Firewall group, as your LAN connection, thus it still might be blocked by it.

### 5.2. Diagnostic logs

Diagnostic logs for the Windows RSP.sl plugins are in the installer folder, under the "**openvpn\_logs**" subfolder. If the installation path has not been altered, it is usually here: "**C:\Program Files (x86)\Unify\RSP.servicelink Plugin\openvpn\_logs\**"

## 6. SLES 11-12 Linux systems

If you have troubles with the SPoA routing, please always check if you are using the latest released connection plugin (at the time of writing of this document, the latest released version is 1.3.0.4). If you have an older one, please update to the latest first, and re-test.

We do not provide support for older releases.

### 6.1. SPoA routes

Should the SPoA routes get inconsistent, you can use the same procedure, as described at the Buffalo Router in the Chapter "*3.6 SPoA connections are not working*", with the difference, that you can reset the SPoA routes on the SLES by running

```
/opt/rsp-slp/cp-spoa.sh -r
```

After that you should do a *“Reconfigure all SPoA connections to this RSP.ServiceLink device”* exactly like with the Buffalo router, as shown in the figure *“Figure 6 – Reconfigure all SPoA connections”*

## 6.2. Diagnostic logs

Diagnostic logs of the RSP.sl plugin on SLES is stored at the following folder:

**`/opt/rsp-sl/openvpn_logs`**

## 7. Ticket content requirements

If you could not find help within this document, you should probably create a new ticket.

If you do, you need to put as much information into the ticket, as possible, to make analyse more effective, and faster.

RSP is a complex system with over hundred servers, hundreds of thousands of managed devices, several hundred users, etc.

It will be much harder to provide help (if possible at all) without detailed description.



Please keep in mind our technicus terminus is probably different from yours.  
e.g. the statement "RSP access does not work" might be trivial in your world, but it has as good, as no information for us about the actual issue.

This chapter is about, what you should include in the ticket to be able to identify the device, issue, and possibly the solution.

### 1. **Device identification**

Please, always provide information, like

- a. Device Identifier in RSP
- b. SIEL-ID (for OSBiz based systems)
- c. MAC Address (for OSBiz based systems)

### 2. **Describe the issue in detail**

- a. What happened,
- b. What would be expected instead
- c. If the issue is reproducible, and if so, how

### 3. **Provide screenshot if possible**

A picture is worth a thousand words

### 4. **Logs and traces**

Please always provide log and trace files, if possible.

### 5. **Connectivity with/without RSP, and contact person(s)**

It would be important to know, if we have the possibility to access the systems from remote to analyse issues. Please let us know, if your system

- a. is in the same network, as another SPoA device (Buffalo Router, OSBiz, ...), which we could use to connect to he device in the customer LAN
- b. if we can contact someone to take a look on the system via Webcollaboration, Circuit, etc.



### **IMPORTANT!**

Please do fill the **authentication** tab in **EqE** for every registered device. Without correct stored credentials the issue analyse is at least problematic, but mostly rather impossible.

Also coming up features – like certificate renewal – require to have remote access to the systems on the servers, to be able to update the expiring RSP.sl certificates!

## 8. List of abbreviations in the document

Abbreviations	Explanation
<b>FW</b>	Firewall
<b>EqE</b>	Equipment Explorer, a central component of the RSP/SIRA environment
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>LAN</b>	Local Area Network
<b>LB</b>	Load Balancer
<b>MITM</b>	Man-in-the-middle, a common form of attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Is also used by strict company FW/Proxy servers to check encrypted communication content.
<b>NVRAM</b>	Non-volatile random-access memory
<b>OpenVPN</b>	OpenVPN is an open-source commercial software that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.
<b>OSBiz</b>	OpenScape Business
<b>RSP</b>	Remote Service Platform
<b>RSP.sl</b>	RSP Service Link – an OpenVPN based connection in RSP
<b>SIRA</b>	Secure Infrastructure Remote Access, a central SW package of the RSP.
<b>SLES</b>	SUSE Linux Enterprise Server
<b>SPoA</b>	Single Point of Access
<b>SSL</b>	Secure Socket Layer, predecessor of TLS
<b>SUSE</b>	“Software und System-Entwicklung”
<b>SW</b>	Software
<b>TLS</b>	Transport Layer Security, successor of SSL
<b>VPN</b>	Virtual Private Network

# 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](https://atos.net)  
[atos.net/career](https://atos.net/career)

Let's start a discussion together



For more information: [rsp@atos.net](mailto:rsp@atos.net)

Atos, the Atos logo, Atos|Syntel, and Unify are registered trademarks of the Atos group. April 2021. © 2021 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.