WCS installation and activation

Installation archives of WCS are available for download at this link.

You can download the installation archive directly to the server using wget, for example

```
wget https://flashphoner.com/downloads/builds/WCS/5.1/FlashphonerWebCallServer-5.1.2993.tar.gz
```

Installation

To install WCS you need to unpack the archive and execute the installation script install.sh:

```
tar -xvzf FlashphonerWebCallServer-5.1.2993.tar.gz
cd FlashphonerWebCallServer-5.1.2993
./install.sh
```

The installer will perform necessary checks and installs WCS to the following directory /usr/local/FlashphonerWebCallServer

Installation includes the following steps:

1. Reading and accepting of the license agreement
2. Specifying IP addresses in case the script was unable to discover them automatically (seeDiscovering the IP address)
3. A request to add WCS to the Linux server autostart

As a result, a successful installation message will be shown. The following folders will be created in the /usr/local/FlashphonerWebCallServer directory:

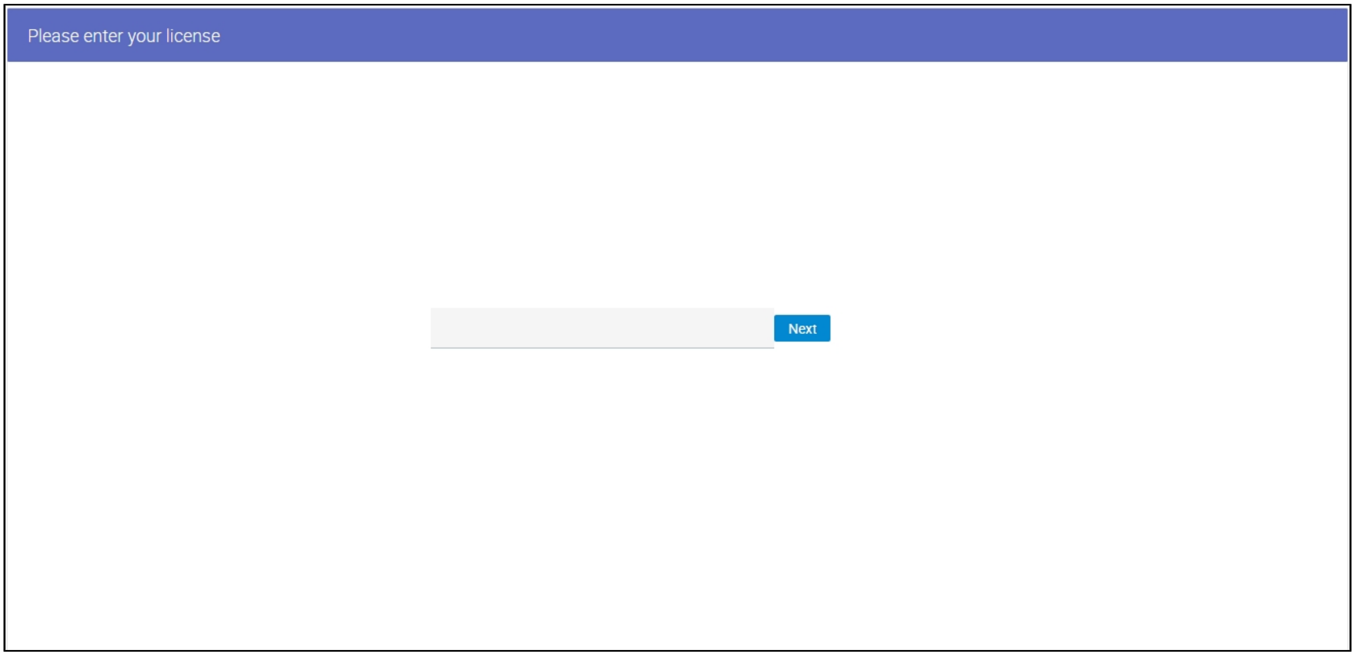
bin - WCS executables
client - WCS JavaScript API 1.0, usage examples and stress-tests
client2 - WCS JavaScript API 2.0 and usage examples
conf - configuration files
lib - required libraries
tools - tools to debug WCS

Acquiring a license and activation

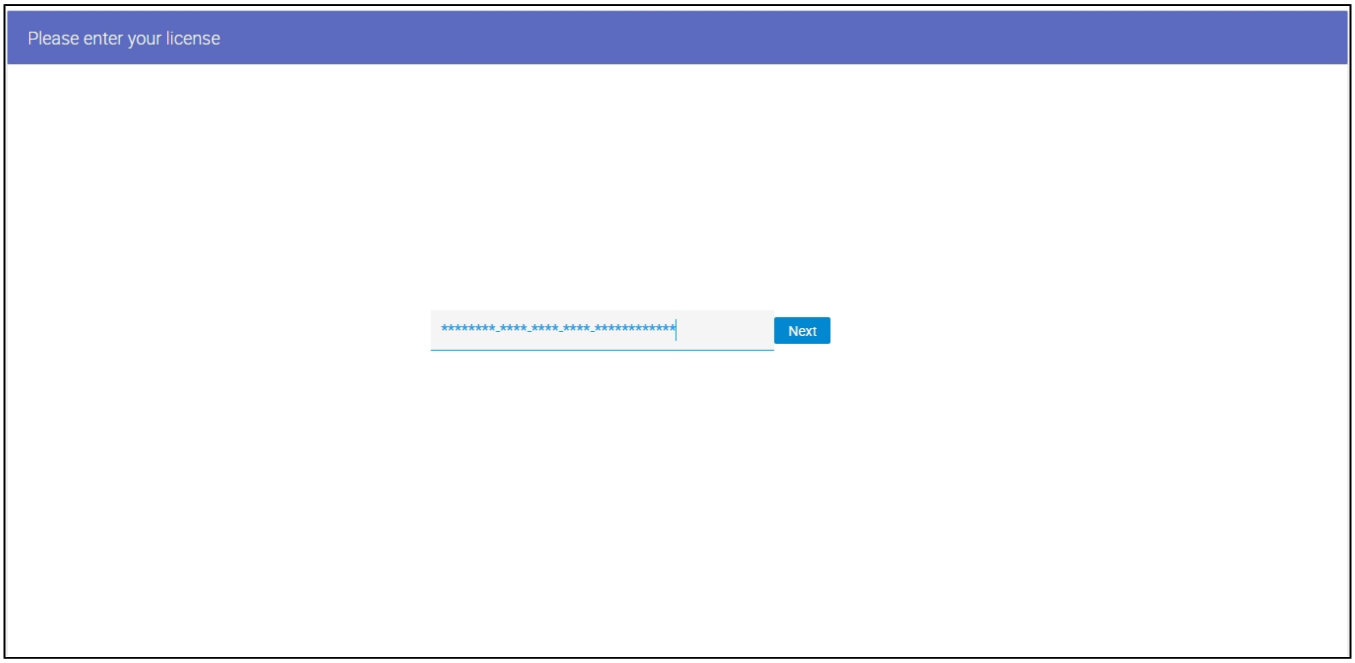
You can purchase a commercial license online here:http://flashphoner.com/prices. Also, a free 30-days trial version is available at this page:http://flashphoner.com/get_trial/?product=wcs5

Activation using web interface

On first logon to WCS web interface by address`http://yourserver:8888/`,where yourserver is your server hostname, the request for license number is displayed:



Enter your license number and press Next



********_****_****_****_************

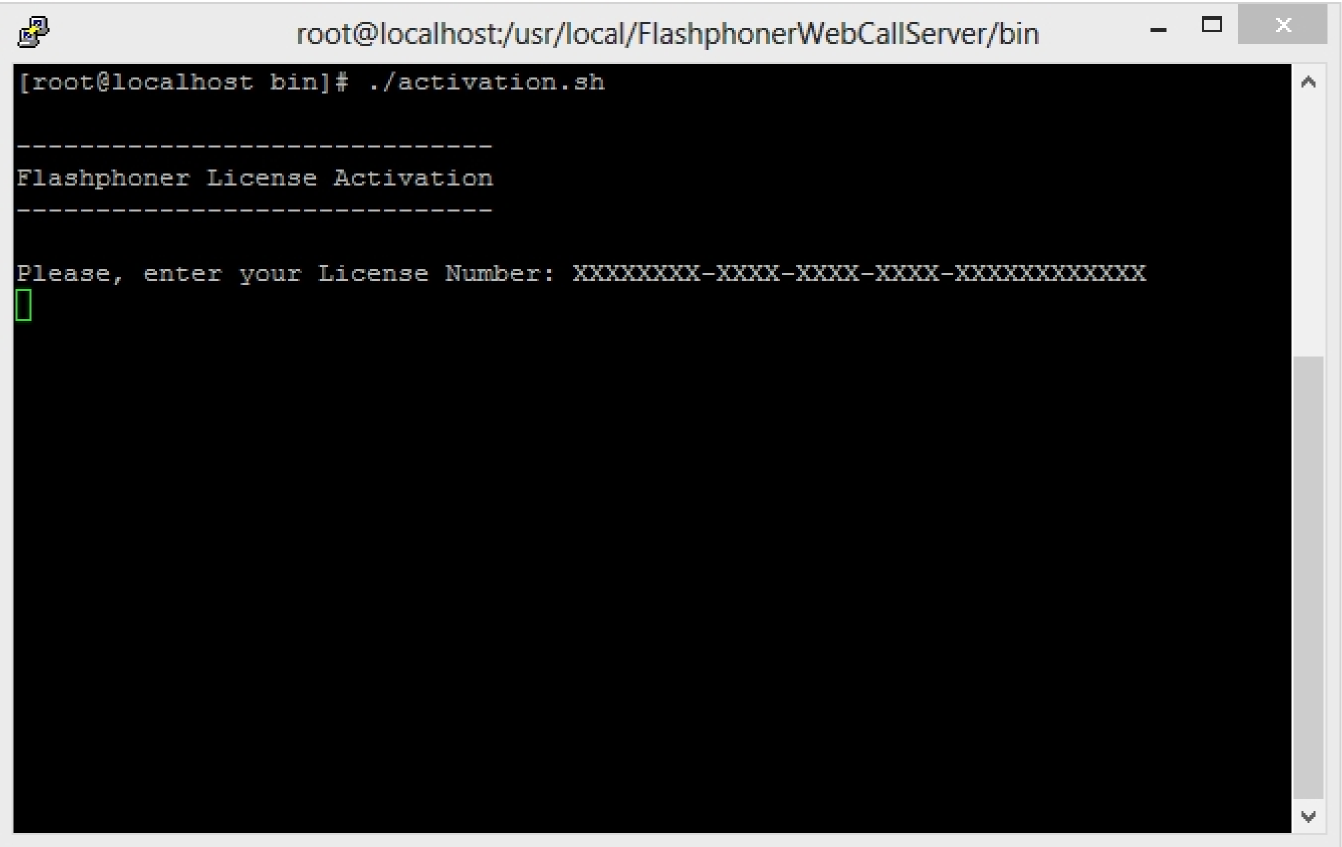
If activation was successfull, admin password request page will be displayed.

Activation using command line

Use this script to activate the license:

```
cd /usr/local/FlashphonerWebCallServer/bin
./activation.sh
```

The script asks you to enter the license number:



```
[root@localhost bin]# ./activation.sh

------------------------------
Flashphoner License Activation
------------------------------

Please, enter your License Number: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
```

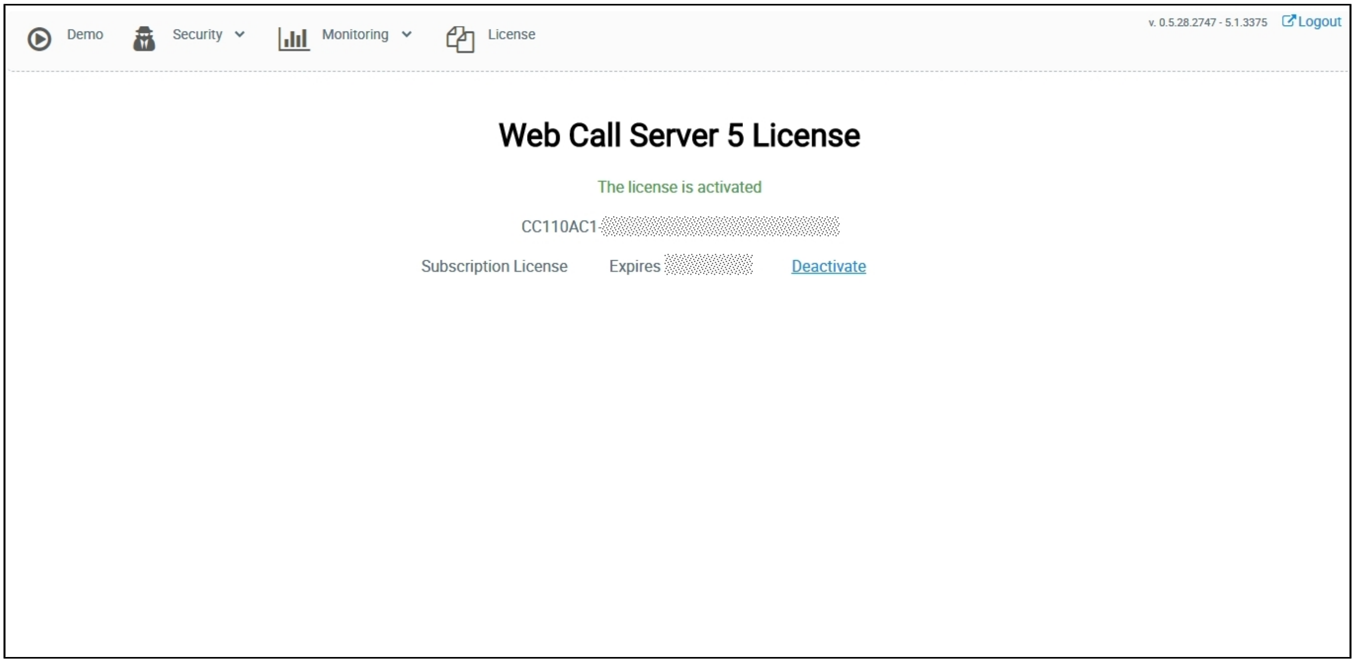
Enter the license number to finish the activation.

Deactivating a license

To activate the same license on another server, for example, if you transfer WCS to another server, deactivate the license on the old server and activate it again on the new server.

Deactivation using web interface

Log in to WCS web interface by address`https://yourserver:8888/`,where yourserver is your server hostname. Press "License" button. The license key page will be displayed:



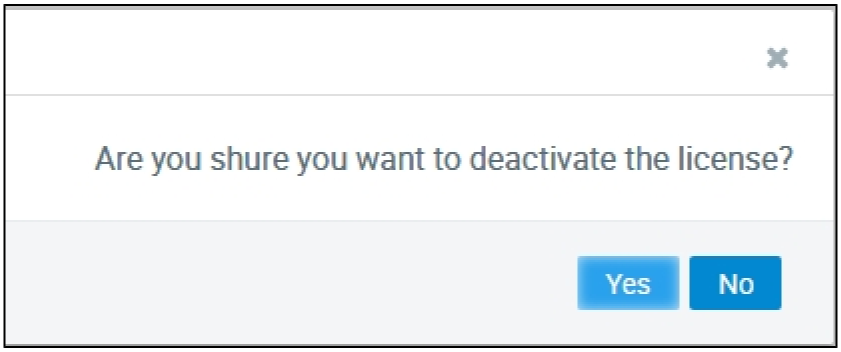
Web Call Server 5 License

The license is activated

CC110AC1-[redacted]

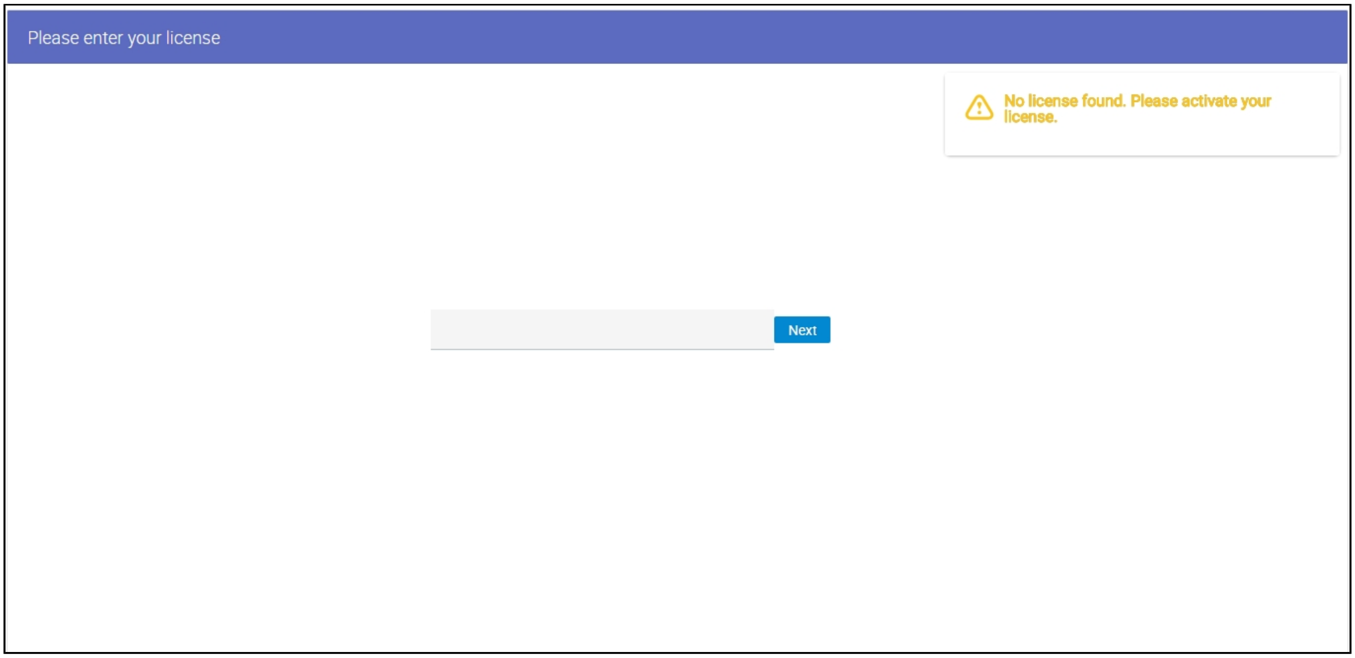
Subscription License Expires [redacted] Deactivate

Click to Deactivate link. Confirmation request will be displayed:



Are you shure you want to deactivate the license?

Press Yes to confirm deactivation. The license will be deactivated, and license key request page will be displayed:



Please enter your license

No license found. Please activate your license.

Deactivation using command line

Use this script for deactivation:

```
./deactivation.sh
```

If activation fails

Check your firewall and make sure the WCS-сервер is able to establish an HTTPS / TCP connection to the activation server my.flashphoner.com:443
If the activation server is unavailable, configure HTTP proxy as describedbelow.

Configuring HTTP proxy if the activation server is not available

Flashphoner license servers are behind AWS ELB (Elastic Load Balancer) at my.flashphoner.com. In case the ELB (and, correspondingly, the license servers) become unavailable for some reason, you will need to configure HTTP Proxy to make subscriptions work and to activate licenses.

Proxy settings can be found in theconfiguration filenamed /usr/local/FlashphonerWebCallServer/conf/wcs-core.properties:

```
# Proxy configuration
-Dhttp.proxyHost=proxy1.flashphoner.com
-Dhttp.proxyPort=3128
-Dhttps.proxyHost=proxy1.flashphoner.com
-Dhttps.proxyPort=3128
-Dhttp.nonProxyHosts=localhost|127.0.0.1|10.*|169.254.169.254
```

You can specify the address of your proxy server or the address of one of two Flashphoner proxy servers:

```
proxy1.flashphoner.com
proxy2.flashphoner.com
```

Important!Proxy settings do not allow quote symbols! The following example will NOT work:

```
-Dhttp.proxyHost="proxy2.flashphoner.com"
-Dhttp.proxyPort="3128"
-Dhttps.proxyHost="proxy2.flashphoner.com"
-Dhttps.proxyPort="3128"
-Dhttp.nonProxyHosts="localhost|127.0.0.1|10.*|169.254.169.254"
```

Configuring Firewall and NAT

For correct operation of the server, all ports listed in the table in theServer coresection must be open for incoming traffic (UDP) or for establishing connection (TCP).

The table below lists example NAT rules for routing of incoming traffic in case the traffic comes to the external IP address and has to be routed to the server where WCS is installed. The table shows the minimum required number of ports necessary for operation of the server. Depending on the specific functions and modules (see theArchitecturesection), the set of rules may be extended in accordance with the table in theServer coresection. The same ports must be opened in the firewall of the Linux server.

The table lists default ports. You can configure the WCS server to other other ports (see theSettingssection).

Type	Protocol	Port Range	Source
Custom UDP Rule	UDP	30000-33000	0.0.0.0/0
Custom TCP Rule	TCP	8888	0.0.0.0/0
Custom TCP Rule	TCP	8443	0.0.0.0/0
Custom TCP Rule	TCP	30000-33000	0.0.0.0/0
Custom TCP Rule	TCP	1935	0.0.0.0/0

SSH	TCP	22	0.0.0.0/0

SSH access via the standard port 22 is specified here only to administer the Linux server itself. Hence, the minimum required set of ports is:

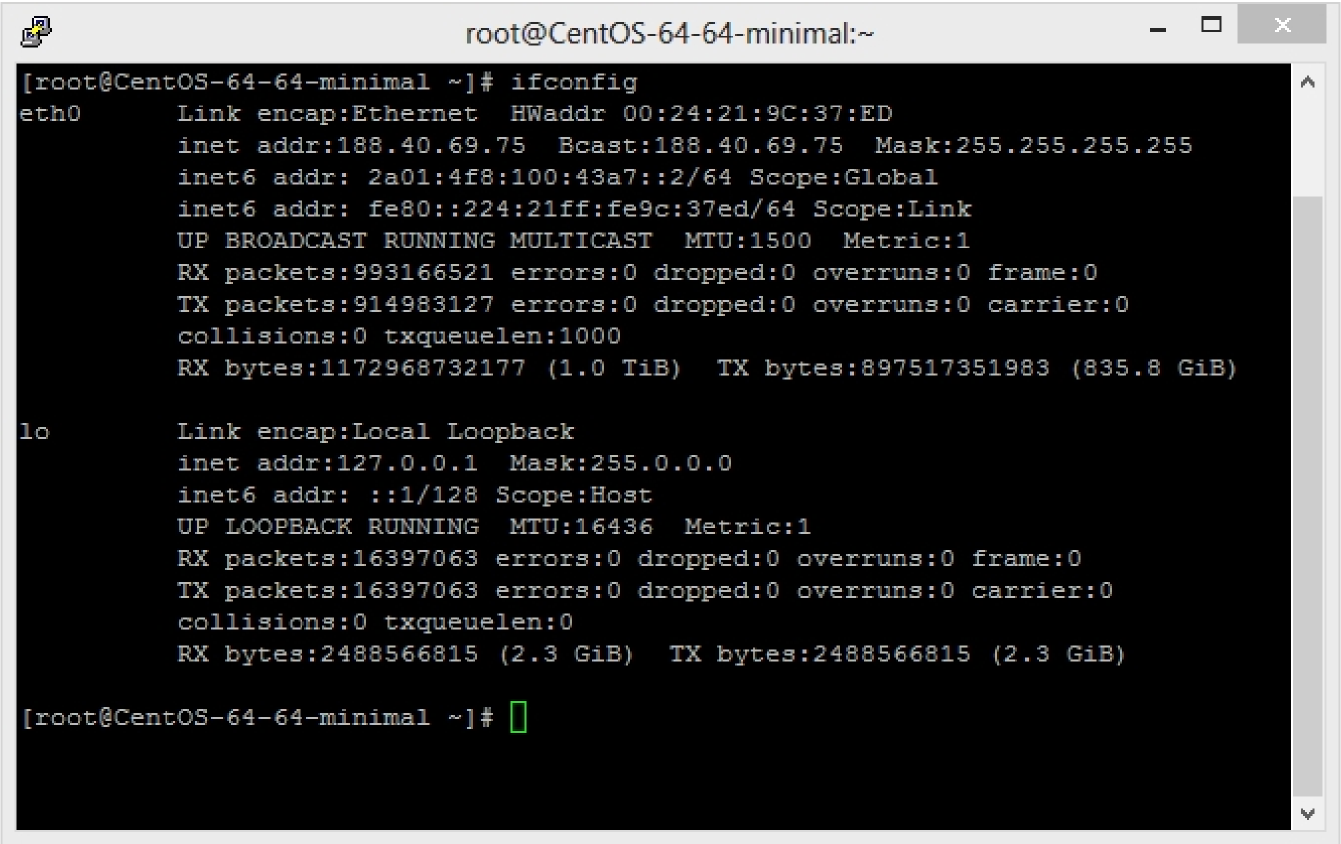
- 1935 - RTMP
- 8443 - Secure Websocket
- 8888 - built-in WCS web server that works via HTTPS
- [30000-33000] - SIP, Media, RTSP

Description of SSL certificate configuration for Secure Websockets and HTTPS can be found in this section:SSL-certificates management.

IP address configuration

Proper installation requires discovering of the external IP address of your server and the address of the network interface. The installation script attempts to detect the address automatically, and if this has failed for some reasons, the script asks you to enter addresses manually.
If you followed recommendation of the 'Requirements and preparations for installing' section and began with a server with a static and public IP address that matches the one of the network interface, the IP address of your server can be discovered with a simple command

```
#ifconfig
```

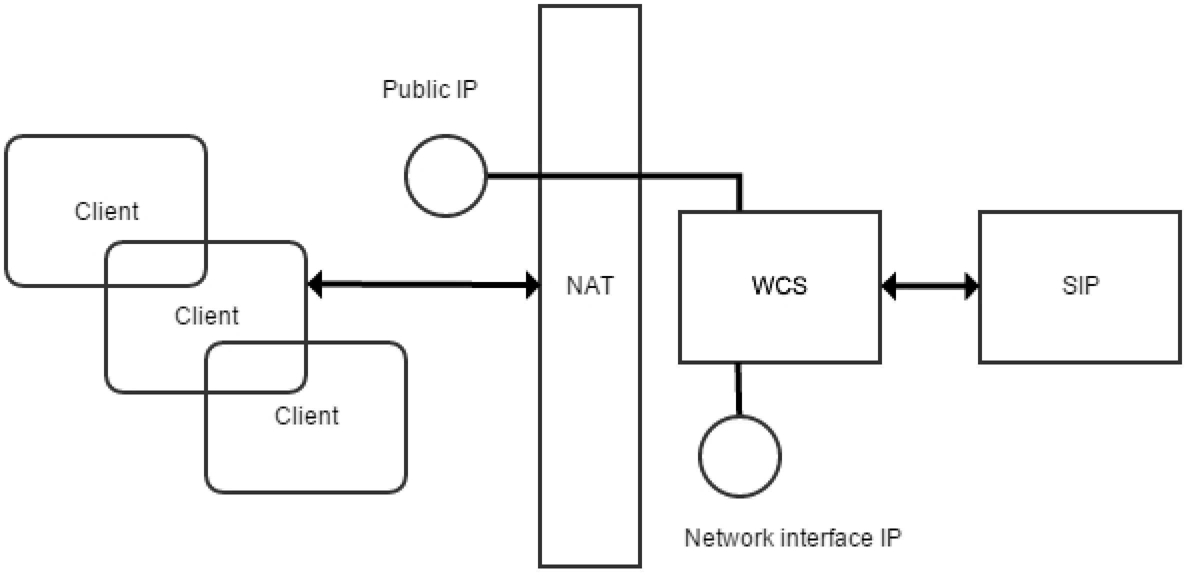


```
[root@CentOS-64-64-minimal ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:24:21:9C:37:ED
          inet addr:188.40.69.75  Bcast:188.40.69.75  Mask:255.255.255.255
          inet6 addr: 2a01:4f8:100:43a7::2/64 Scope:Global
          inet6 addr: fe80::224:21ff:fe9c:37ed/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:993166521 errors:0 dropped:0 overruns:0 frame:0
          TX packets:914983127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1172968732177 (1.0 TiB)  TX bytes:897517351983 (835.8 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16397063 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16397063 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2488566815 (2.3 GiB)  TX bytes:2488566815 (2.3 GiB)

[root@CentOS-64-64-minimal ~]#
```

In this example, the IP address of the server is 188.40.69.75. Write the address down or copy it. You will need it later on installing.

Discovering IP addresses in case of NAT

Often the WCS5 server has to be placed behind a corporate NAT or on the rented server in a data center that does not provide dedicated static IP addresses. A good example of this case is Amazon EC2, where servers are behind NAT.



When the WCS server is to deployed behind NAT, you need to discover two IP addresses.

1. The external IP address or Public IP not necessarily belongs to the WCS server, but traffic that goes to this external IP address should be obligatory redirected to WCS5.
2. Network interface IP address or Private IP - this is a real address assigned to the network interface. Here WCS will open sockets to interact with the network.

For example, a test server on Amazon EC2 has the external IP address of: 54.189.212.111, and the network interface address is: 172.30.21.25. If your server is behind NAT шт regard to browser clients, write down or copy these IP addresses. You will need them later, when you will configure the server.