



SOLUTION GUIDE

Wave 3 | April 2016 | 2998-0068-002 Rev B

---

# PortSIP<sup>®</sup> WebRTC Gateway User Guide



Copyright ©2016, PortSIP Solutions, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of PortSIP Solutions, Inc.

## Trademarks



PortSIP<sup>®</sup>, the PortSIP logo and the names and marks associated with PortSIP products are trademarks and/or service marks of PortSIP Solutions, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of PortSIP.

## End User License Agreement

By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the [End User License Agreement](#) for this product.

## Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by PortSIP Solutions, Inc.

## Open Source Software Used in this Product

This product may contain open source software. You may receive the open source software from PortSIP up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to PortSIP of shipping or distributing the software to you.

## Disclaimer

While PortSIP uses reasonable efforts to include accurate and up-to-date information in this document, PortSIP makes no warranties or representations as to its accuracy. PortSIP assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

## Limitation of Liability

PortSIP and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall PortSIP and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if PortSIP has been advised of the possibility of such damages.

## Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to [support@portsip.com](mailto:support@portsip.com).



Visit the [PortSIP<sup>®</sup> WebRTC Gateway](#) for information on PortSIP software versions and administrative documentation, and PortSIP release notes.

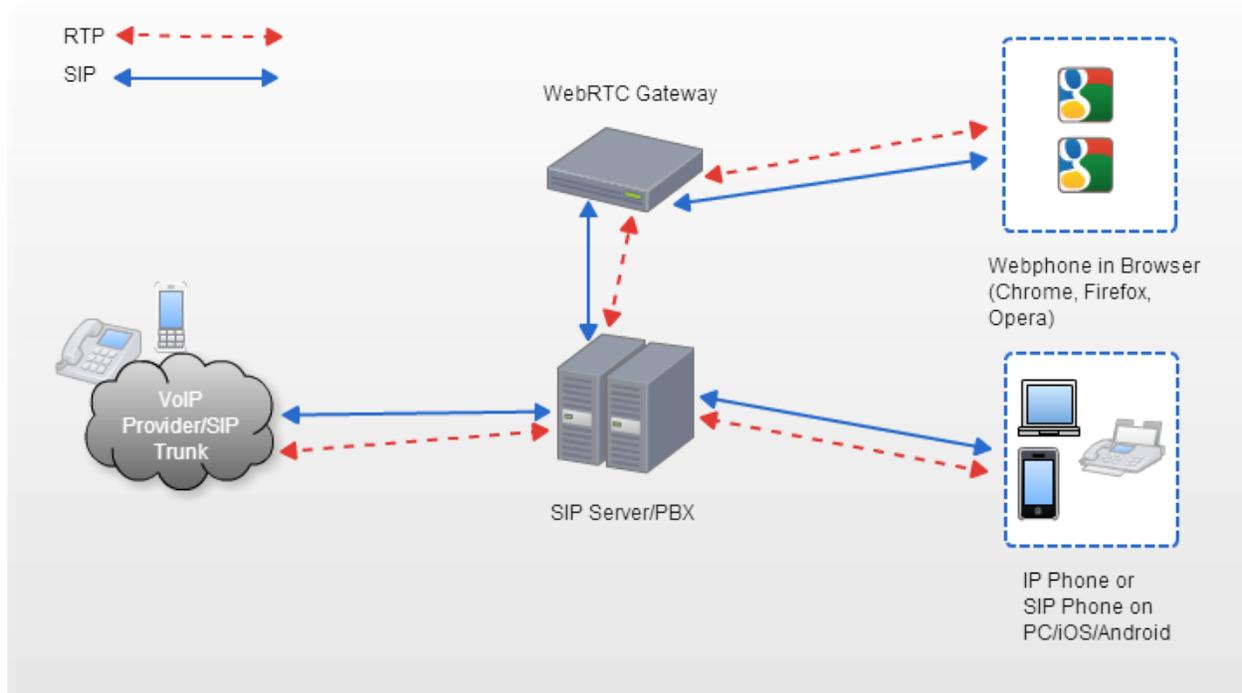
# Contents

---

- PortSIP® WebRTC Gateway User Guide ..... 1**
- 1. The WebRTC Gateway Architecture ..... 4**
- 2. How it works? ..... 4**
- 3. Install WebRTC Gateway ..... 5**
- 4. Manage WebRTC Gateway ..... 5**
  - 4.1 Configuring WebRTC Gateway by Wizard ..... 5
  - 4.2 Settings ..... 6
- 5. Run WebRTC Web Client ..... 8**
- 6. Deployment Practices ..... 10**
  - 6.1 Deploy WebRTC Gateway with official certificate ..... 10
  - 6.2 Deploy WebRTC Gateway with Self-signed certificate in LAN..... 11

# 1. The WebRTC Gateway Architecture

Typically, the WebRTC Gateway architecture as below:



This document assumes that the Windows OS are already deployed and that Microsoft administrators are available to administrators PortSIP WebRTC Gateway.

## 2. How it works?

PortSIP WebRTC Gateway sits at the network edge to bridge the traditional operator network (PSTN/VoIP Provider/SIP Trunking/IP PBX) with the Web Browser, letting carriers build Web services on top of it. The gateway essentially turns any Web page into a telephone that the network can dialogue with as it would a phone.

Since the traditional operator network (PSTN/VoIP Provider/SIP Trunking) and SIP devices (IP Phone, Softphone) don't support the newest WebRTC standards such as TURN, DTLS-RTP, RTC-FB, ICE, therefore we need the WebRTC Gateway to transform the signaling and RTP streams. That's why the Gateway is works like a bridge.

When the user make calls in Web Browser, the WebRTC Gateway will transform the Signaling to standard SIP message and route calls to PSTN/VoIP Provider/SIP Trunking/IP PBX. After the call established, the WebRTC Gateway receive RTP stream from browser and transcode it then send to PSTN/VoIP Provider/SIP Trunking/IP PBX and vice versa.

## 3. Install WebRTC Gateway

After you downloaded PortSIP WebRTC MSI installer just double click it and follow the instructions to install.

You can set the WebRTC Gateway HTTP and HTTPS listen port during installation, the default HTTP port is 9288, HTTPS ports is 9287 – Please **ensure the port that doesn't using by other applications** otherwise the HTTP/HTTPS service will fails.

## 4. Manage WebRTC Gateway

After the WebRTC Gateway successfully installed, you can double click the Management Console on your Windows desktop, which will open the Management Console.

You can also use this URL remotely to manage the Gateway: <http://gatewayIP:port/manager/index.html> (the gatewayIP is the IP of the server which you installed the Gateway, the port is the HTTP port which you specify during your install the gateway).

Please use below credentials to sign in the Admin Management Console:

Username: admin  
Password: admin

### 4.1 Configuring WebRTC Gateway by Wizard

After signed in the Management Console, click the “**Wizard**” menu in left.

#### 4.1.1 WebRTC settings

This page settings are for the WebRTC Gateway, please follow below instructions:

1. Click the **Next** button.
2. Gateway IP Address: you can specify the WebRTC Gateway IP address here, if the gateway is run in Lan please enter local private IP address; If run on the internet please enter the static public IP. This filed IP can not be empty.
3. Default WS port for WebRTC Gateway has been listening, and the WS transport port is 10080.
4. Listen WSS: The Google Chrome requires the WSS in order to access the camera and microphone. You must select this option if you want use Google Chrome.

Once the “**Listen WSS**” is selected, you should set below fields:

WSS port: set a port which is for the WSS, for example 10443.

Domain Name: Your WebRTC Gateway domain name, it's must resolvable, if you don't have domain name of Gateway server, enter the Gateway IP.

Certificate File: for WSS, you must upload the certificate file. You can generate the SSL certificate file by yourself or purchase a certificate from provider such as [Thawte](#) or [Digicert](#). The certificate must match the WebRTC Gateway domain.

Private Key File: It will be generated with certificate together.

Password of Private key: the password of private key file which is you entered when you generate the certificate file. If no password for private key then leave it blank.

**Note:** If you haven't a valid certificate, and don't know how to create a Self-signed certificate, you can upload the sample certificate(server.crt and server.key) which is in Gateway installed folder, e.g.: "C:\Program Files\PortSIP\WebRTC".

Click the **Next** button.

## 4.1.2 SIP Server/PBX settings

This page settings are for the SIP Server/PBX.

1. SIP Domain: specify your SIP Domain here here, it's can be an IP address or domain.
2. Use DNS SRV records: If your SIP Domain support DNS SRV, you can select this option. If the DNS SRV is enabled, next steps will be skipped.
3. The server address is same as SIP domain: this option default is selected. Please un-selected it if your SIP server address is not same as SIP Domain.
4. SIP Server Address: if your SIP Server address is not same as SIP Domain, you MUST specify your SIP server address here.
5. SIP Transport: your SIP server transport, usually is UDP.
6. Server Port: your SIP server port.

Click the **Save** button to complete the wizard.

**Note:** after you clicked the **Save** button, the WebRTC Gateway will restart, you have to sign in the management console again.

## 4.2 Settings

### 4.2.1 Log

You can enable/disable WebRTC log by select/un-select "Enable SipMessage Logging" option, and choose the log level. The log file will be generated in WebRTC Gateway installed folder, the name is "webrtcgw.log". You must restart WebRTC Gateway to take effect.

## 4.2.2 STUN Server

If you deploy the WebRTC Gateway in LAN and can't access the default STUN server, you can try install a STUN Server. Download the [STUN Server](#) then extract **stunserver.zip** and run stunserver.exe.

Click the "**Settings**" in the WebRTC Gateway Management Console and set the stun server IP as the Run stunserver PC IP, the port default is 3478.

## 4.2.3 Web Server

The Web Server is use for manage WebRTC Gateway and deploy the Web Client.

https port default is: 9297

http port default is: 9298

You can change to any other port as you want. Https is request 4.1.1 step to upload a valid certificate.

## 5. Run WebRTC Web Client

Assume we have a SIP Server/PBX which SIP domain is portsip.net, it has SIP user 100.

Assume we installed the WebRTC Gateway on a server which IP is 192.168.0.28.

The WebRTC Gateway setting is:

HTTP port: 9288  
HTTPS port: 9287  
WS port: 10080  
WSS port: 10443

### 5.1 For Firefox:

Below settings are for last version Firefox.

1. Open <http://192.168.0.28:9288/portgo/index.html> by last version Firefox.
2. SIP Username filed: enter a name as 100.
3. SIP password filed: enter the password of SIP user 100.
4. SIP Domain in case is: portsip.net.
5. WS URI: in case is <ws://192.168.0.28:10080> (It's WebRTC Gateway IP and WS port).
6. Press **"enter"** button
7. Once the web client registered, you can make & receive calls with other SIP client.

### 5.2 For Firefox with HTTPS + WSS:

The Firefox also support HTTPS and WSS. In case you MUST set the HTTPS and WSS with certificate by WebRTC Gateway Management Console Wizard.

1. Open <https://192.168.0.28:9287/portgo/index.html> by last version Firefox,  
If you use a self-signed certificate, the Firefox alert "Your connection is not secure", click "Advanced" -> "Add exception..." -> "Confirm Security Exception".  
WSS port also need add to exception, Open <https://192.168.0.28:10443> by Firefox, the Firefox alert "Your connection is not secure", click "Advanced" -> "Add exception..." -> "Confirm Security Exception".
2. SIP Username filed: enter a name as 100.
3. SIP password filed: enter the password of SIP user 100.
4. SIP Domain in case is: portsip.net.
5. WS URI: in case is <wss://192.168.0.28:10443> (It's WebRTC Gateway IP and WSS port).
6. Press **"enter"** button

Once the web client registered, you can make & receive calls with other SIP client.

## 5.3 For Google Chrome:

The Google Chrome requires the HTTPS and WSS in order to access the Camera and Microphone. You MUST set the HTTPS and WSS with certificate by WebRTC Gateway Management Console Wizard.

1. Open <https://192.168.0.28:9287/portgo/index.html> by last version Google Chrome, If you use a self-signed certificate, the Chrome alert the certificate is unsafe, just allow this unsafe certificate (since it's self-signed certificate)
2. SIP Username filed: enter a name as 100.
3. SIP password filed: enter the password of SIP user 100.
4. SIP Domain in case is: portsip.net.
5. WS URI: in case is <wss://192.168.0.28:10443> (It is WebRTC Gateway IP and WSS port).
6. Press “**enter**” button

Once the web client registered, you can make & receive calls with other SIP client.

# 6. Deployment Practices

## 6.1 Deploy WebRTC Gateway with official certificate

You can purchase an official certificate from the certificate provider such [Thawte](#) or [Digicert](#) in order to avoid the security alert and don't need add the security exception manually.

During you purchase the certificate, you should generate the private key and CSR by yourself – please read the provider's instructions or ask the provider support. We recommend you don't set the password for private key file. You must keep the private key file by yourself.

Assume we purchased a certificate from Thawte (in case we use the Thawte SSL123 certificate as example) for domain **examplertc.com**. After you downloaded the certificate .zip file, just extract it, there has IntermediateCA.crt and ssl\_certificate.crt, you will need to use a plain text editor (for example Windows Notepad, don't use MS Word) to combine your two certs with them into one file: copy all text from IntermediateCA.crt and append to ssl\_certificate.crt, the ssl\_certificate.crt at the top and IntermediateCA.crt at the bottom.

1. Ensure the domain **examplertc.com** has been resolve correct to the server which you installed the PortSIP WebRTC Gateway.
2. Assume the SIP server address is 69.164.210.98, the SIP Domain is: **sip.testsip.com**, the transport is UDP on port 5060, it has SIP user 100, 101, 102, 103, 104.
3. Use browser open <http://examplertc.com:9288/manager/index.html>, sign in the Management Console with admin/admin.
4. Enter ip of **examplertc.com** to "**Gateway IP Address**".
5. Click "**Listen WSS**" to select it.
6. Set WSS port, for example: 10443
7. Set **examplertc.com** for "**Gateway Domain Name**" filed.
8. Click the up arrow icon to choose the combined "**ssl\_certificate.crt**" file for "**Certificate File**".
9. Click the up arrow icon to choose the private key file which you generated when you purchase the certificate.
10. If you have set the password when you generate the private key, then please enter it for "**Private key password**". If don't set the password just leave it empty.
11. Click the "**Next**" button.
12. Set the "**SIP Domian**" as **sip.testsip.com**
13. Un-select the "**The server address is same as SIP domain**".
14. Enter the SIP Server Address, in case it is 69.164.210.98.
15. Select the SIP Transport as UDP.
16. The Server port is: 5060.
17. Click the "**Save**" button, the WebRTC Gateway will be restart automatically, you will need to sign in management console again.
18. Open <https://examplertc.com:9287/portgo/index.html> by last version FireFox or Google Chrome.
19. SIP Username filed: enter a name as 100.
20. SIP password filed: enter the password of SIP user 100.
21. SIP Domain in case is: sip.testsip.com.
22. WS URI: in case is <wss://examplertc.com:10443> (It is WebRTC Gateway IP and WSS port).
23. Press your "**enter**" button
24. Once the web client registered, you can make & receive calls with other SIP client.

## 6.2 Deploy WebRTC Gateway with Self-signed certificate in LAN

### For Firefox:

Below settings are for last version Firefox.

1. Assume we have a SIP Server/PBX which IP 192.168.0.98 and SIP domain is 192.168.0.98, this server/PBX use the UDP transport on port 5060, it has SIP user 100, 101, 102, 103, 104.
2. Assume we installed the WebRTC Gateway on a server which IP is 192.168.0.28.
3. Use browser open <http://192.168.0.28:9288/manager/index.html>, sign in the Management Console with admin/admin.
4. Click the **“Wizard”** on left and click the **“Next”** button.
5. Enter 192.168.0.28 for the **“Gateway IP Address”** filed.
6. Click the **“Next”** button.
7. Enter the SIP Domain, in case it is 192.168.0.98.
8. Select the SIP Transport as UDP.
9. The Server port is: 5060.
10. Click the **“Save”** button, the WebRTC Gateway will be restart automatically, you will need to sign in management console again.
  
11. If in LAN the WebRTC Gateway can't access the internet, Download the [STUN Server](#) then extract stunsrvr.zip and run stunsrvr.exe.
12. Click the **“Settings”** in the WebRTC Gateway Management Console and set the stun server as 192.168.0.28:3478.
13. Open <http://192.168.0.28:9288/portgo/index.html> by last version Firefox.
14. SIP Username filed: enter a name as 100.
15. SIP password filed: enter the password of SIP user 100.
16. SIP Domain in case is: sip.testsip.com.
17. WS URI: in case is ws://192.168.0.28:10080 (the IP is WebRTC Gateway IP and WS port).
18. Press **“enter”** button
19. Once the web client registered, you can make & receive calls with other SIP client.

### For Google Chrome:

The Google Chrome requires the HTTPS and WSS in order to access the Camera and Microphone. We MUST set the HTTPS and WSS with certificate for WebRTC Gateway and Gateway Web Service.

1. Use browser open <http://192.168.0.28:9288/manager/index.html>, sign in the Management Console with admin/admin.
2. Enter 192.168.0.28 for the **“Gateway IP Address”** filed.
3. Click **“Listen WSS”** to select it.
4. Set WSS port, for example: 10443
5. Set 192.168.0.28 for **“Gateway Domain Name”** filed.
6. Click the up arrow icon to choose the **“server.crt”** file from the Gateway install folder, for example: **C:\Program Files\PortSIP\WebRTC**.
7. Click the up arrow icon to choose the **“server.key”** file from the Gateway install folder, for example: **C:\Program Files\PortSIP\WebRTC**.
8. Leave the **“Private key password”** empty.
9. Click the **“Next”** button.
10. Enter the SIP Domain, in case it is 192.168.0.98.
11. Select the SIP Transport as UDP.
12. The Server port is: 5060.
13. Click the **“Save”** button, the WebRTC Gateway will be restart automatically, you will need to sign in management console again.

14. If in LAN the WebRTC Gateway can't access the internet, Download the [STUN Server](#) then extract stunserver.zip and run stunserver.exe.
15. Open <https://192.168.0.28:9287/portgo/index.html> by last version Google Chrome, when the Chrome alert the certificate is unsafe, just allow this unsafe certificate (since it's self-signed certificate)
16. SIP Username filed: enter a name as 100.
17. SIP password filed: enter the password of SIP user 100.
18. SIP Domain in case is: sip.testsip.com.
19. WS URI: in case is wss://192.168.0.28:10443 (It is WebRTC Gateway IP and WSS port).
20. Press "**enter**" button
21. Once the web client registered, you can make & receive calls with other SIP client.