



**UPDATE04-V6.1**

## 0 Index

1 Update04-v6.1.....	3
1.1 UCoIP Page – Video Calls.....	3
1.2 Email security improvement.....	3
1.3 Web Interface – New Menu.....	4

# 1 Update04-v6.1

## 1.1 UCoIP Page – Video Calls

The video call feature on IPBrick is implemented by WebRTC, which is an open-source web-based application technology that allows users to make real time communications using a browser. The supported browsers are Google Chrome (recommended), Firefox and Opera.

Due to some security requirements, it's necessary to guarantee the following configurations:

- IPBrick must have a valid SSL certificate for the services "Web Server (HTTPS)" and "WebRTC (Web Real-Time Communication)".

This configuration is available on: **"Advanced Configurations » IPBrick » Certificates"**.

- The web site for UCoIP Pages, ucoip.<DOMAIN> must only be set with HTTPS protocol. Check this configuration on : **"UCoIP » Web Server"**.

Web site definitions	
URL address:	<input type="text" value="https://"/> <input type="text" value="ucoip.domain.com"/>
Alternative URL addresses:	<input type="text"/> (one per line)
Site administrator email:	<input type="text" value="administrator"/>
Internet Availability:	<input type="checkbox"/> Yes

- The default UCoIP Page, ucoip.<DOMAIN> must be available on the Internet. For this requirement, the DNS record "ucoip.<DOMAIN>" must be configured on the public DNS. This configuration is necessary to access UCoIP Pages with the URL format "https://ucoip.<DOMAIN>/<LOGIN>", which is a requirement when the login of the Users has the special character "." (ex: john.smith).
- A WebRTC Proxy was added on IPBrick to enable external users, behind firewalls with restriction policies, to make videocalls using the users' UCoIP Page.

To enable this feature on the internet, the DNS record webrtcproxy.<DOMAIN> must also be configured on the public DNS!

## 1.2 Email security improvement

- To improve security on the email server, a new option was added to the anti-virus to block dangerous attachments. This option is enabled by default!

This new feature blocks only attachments with compressed files such as 7z, Rar, Zip, Arj, Cab, whenever they have the following executables inside: ade, adp, bat, chm, cmd, com, cpl, exe, hta, ins, isp, jse, lib, mde, msd, msp, mst, pif, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc, wsf, wsh.

- This configuration is available on: **“Security » E-Mail Relay » Anti-Virus » ClamAV”**.

ClamAV Definitions		Modify
Enable configuration:	Yes	
Block dangerous attachment:	Yes	
Databases updated:	<input checked="" type="checkbox"/>	
Action when a virus is detected:	Reject E-Mail	

## 1.3 Web Interface – New Menu

- Due to the new menu organization based on the "Magic Quadrant", IPBrick's web interface needs to be refreshed in order to reload the new menu.

This operation occurs when applying configurations for the first time after installing update 04-v6.1, and it may also result on the disappearance of message "Successfully updated!".

**2016 IPBRICK INTERNATIONAL**

[www.ipbrick.com](http://www.ipbrick.com) | [mail@ipbrick.com](mailto:mail@ipbrick.com)

Rua Passos Manuel, nº 66/76 | 4000-381 Porto | PORTUGAL  
TEL. +351 221 207 100 | FAX +351 225 189 722