PCS 60 for Mac OS X v3.3.6

Installation & Configuration Notes

WARNING: When upgrading PCS 60 for Mac OS X IP Softphone/Phone Partner to v3.3.6 the following SpliceCom system components must also be simultaneously upgraded to the software levels outlined below;

- S716/S8000 Soft PBX – v3.3.73
- 4100/4140/5100/5108 Call Server – v3.3.73
- 5500 Network Service Gateway – v3.3.73
- SSL Gateway – v3.3.73
- PCS 5xx – 3.3.73
- Navigate – v1.0.70
- PCS 60 for Windows – v3.2.255

Failure to follow this procedure will result in the incorrect time being shown for voicemail/missed call information on PCS 5xx IP Phones and Navigate/PCS 60 IP Softphones & Phone Partners.

Introduction

SpliceCom's PCS 60 for Mac OS X has been designed to run as an IP Softphone and Phone Partner on Apple Mac OS X laptops and platforms, in conjunction Maximiser OS based business telephone systems; be they implemented as soft, hard or virtual PBXs.

The immediate availability of PCS 60 for Mac OS X v3.3.6 adds support for the following new feature;

- SSL for Secure Connectivity

SSL for Secure Connectivity

Through the addition of a Secure Socket Layer (SSL) connectivity option for PCS 60 for Mac OS X IP Softphones, SpliceCom have made their deployment for remote office, mobile and homeworking applications quicker and easier to roll-out, whilst simultaneously increasing voice security.

PCS 60 for Mac OS X v3.3.4 sees the introduction of a Secure Socket Layer (SSL) connectivity option for IP Softphone operation.

Please note: PCS 60 for Mac OS X does not currently support SSL connectivity when running in Phone Partner mode.

SSL support allows PCS 60 for Mac OS X IP Softphones deployed in remote office, mobile or homeworking environments where an on-site 5100 Call Server, S8000/S716 Soft PBX or 5500 Network Service Gateway does not exist, to create a secure SSL link back to the host PBX through the Internet. A Virtual Private Network (VPN) tunnel is not required when utilising SSL for site-to-site connectivity.

SSL is far more efficient than VPN for remote connectivity. Figures show SSL results in a 1% increase in CPU load, consuming a mere 10kB of memory per connection and adding just 2% to network bandwidth requirements. By contrast VPN connections can add up to 40% overhead on a standard voice call.

Once installed, configured and active a PCS 60 for Mac OS X IP Softphone running SSL operates in exactly the same manner as an IP Softphone connected directly over the LAN to a 5100 Call Server or S8000/S716 Soft PBX.

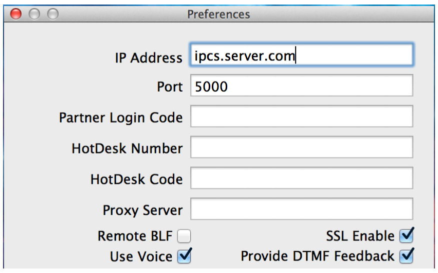
Configuring SSL Operation for PCS 60 for OS X Softphones

PCS60 for MAC now supports SSL in osftphone working. In order to configure open the Preferences window and enter the IP Address or Domain name of the SSL Gateway, set the port that the SSL Gateway uses (default is 5000) and tick the SSL Enable box. You config window should look similar to the below:

In order to configure PCS 60 for Max OS X for SSL operation;

1. Open the Preferences window
2. Enter the IP Address or Domain Name of the SSL Gateway
3. Set the port that the SSL Gateway uses (default is 5000)
4. Tick the SSL Enable box.

Your Preferences window should now look similar to the following:



Preferences

IP Address ipcs.server.com
Port 5000
Partner Login Code
HotDesk Number
HotDesk Code
Proxy Server
Remote BLF ☐ SSL Enable ☑
Use Voice ☑ Provide DTMF Feedback ☑

Restart PCS 60 or OS X. If this is the first time that the Apple Mac that PCS 60 for OS X is running on has been added to the system you should follow the normal procedure to allow a softphone access to the Soft PBX or CallServer. Once the softphone has been added to the system, a User is created and telephony operation can commence.

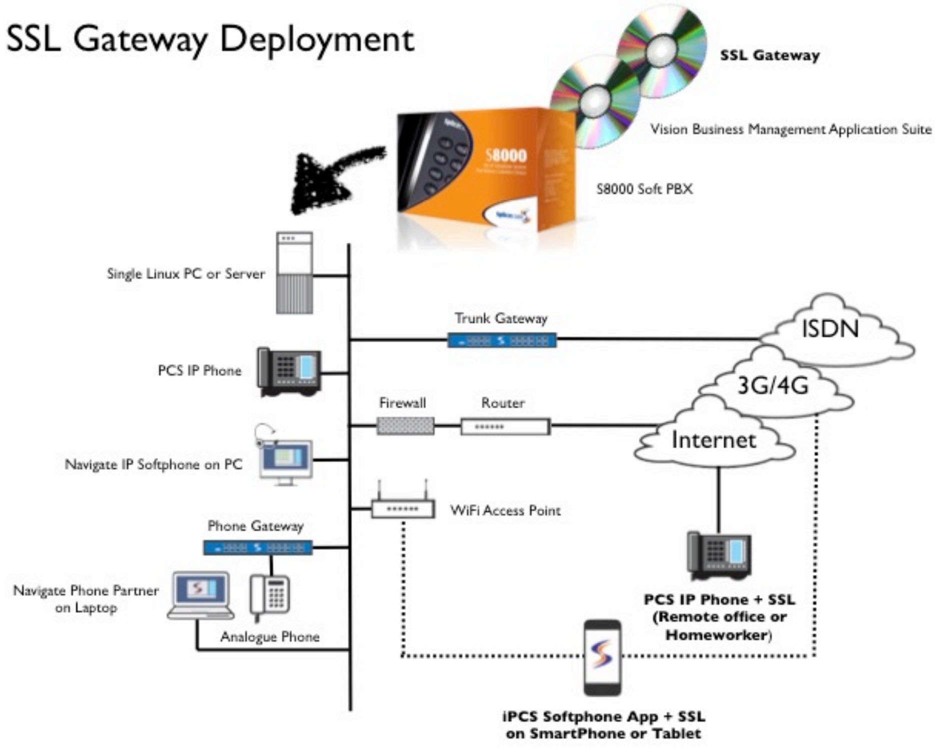
SSL Gateway

SSL operation on PCS 60 for Mac OS X IP Softphones also requires an SSL Gateway (formally known as the iPCS Gateway) to be provisioned on the site where the host soft/hard/virtual Maximiser OS PBX is located. The SSL Gateway app can be run on the same platform as a S8000/S716 Soft PBX or, alternatively, co-exist with the Vision Business Management suite server in a 5100 Call Server environment.

The SSL Gateway app comes pre-installed on SpliceCom's MultiApp Platform (MAP), or can alternatively be run on Linux or Apple Mac OS X platforms.

When MAP is not utilised to host the SSL Gateway app, SpliceCom's recommended specification for an entry-level Linux machine (HP Proliant Microserver - 1.5 GHz AMD processor, 2GB memory) can comfortably handle forty active SSL sessions, when running as a standalone SSL Gateway.

For details on how to install the SSL Gateway please refer to the "SSL Gateway Installation and Configuration Notes".


SSL Gateway Deployment
SSL Gateway
Vision Business Management Application Suite
S8000 Soft PBX
S8000
Single Linux PC or Server
Trunk Gateway
ISDN
PCS IP Phone
3G/4G
Firewall
Router
Internet
Navigate IP Softphone on PC
WiFi Access Point
Phone Gateway
Navigate Phone Partner on Laptop
Analogue Phone
PCS IP Phone + SSL (Remote office or Homeworker)
iPCS Softphone App + SSL on SmartPhone or Tablet

Availability

PCS 60 for Mac OS X v3.3.6 is available with immediate effect (July 2014).

Version 1.0, July 2014

SpliceCom
Britain's leading developer of telephone systems

The Hall Business Centre, Berry Lane, Chorleywood, Herts, WD3 5EX tel: 01923 287700 fax: 01923 287722
email: info@splicecom.com website: www.splicecom.com