CALLN

CALLN HOSTED CALL RECORDING
LG IPECS PORT MIRRORING SETUP

Created by Chris Lane

15 November 2017

Version 1.1.0

Table of Contents

1. Introduction

This document describes how to configure your LG iPECS switch and PBX to work with CallN.
There are two steps to configuring the iPECS switch. The first is to setup port mirroring on the switch which allows CallN to record calls. The second step is to turn off RTP Security in the PBX on devices if call recording quality is affected by encryption of RTP data.

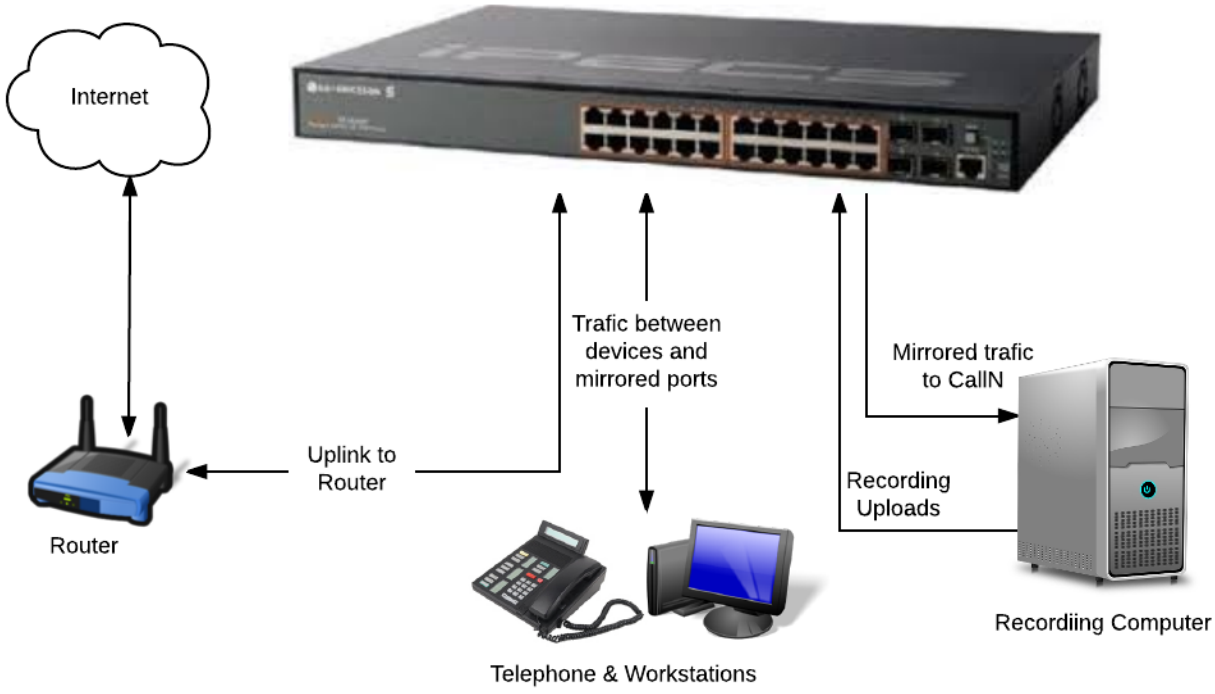
2. Connectivity

To successfully record calls, CallN recording computer requires two network connections.

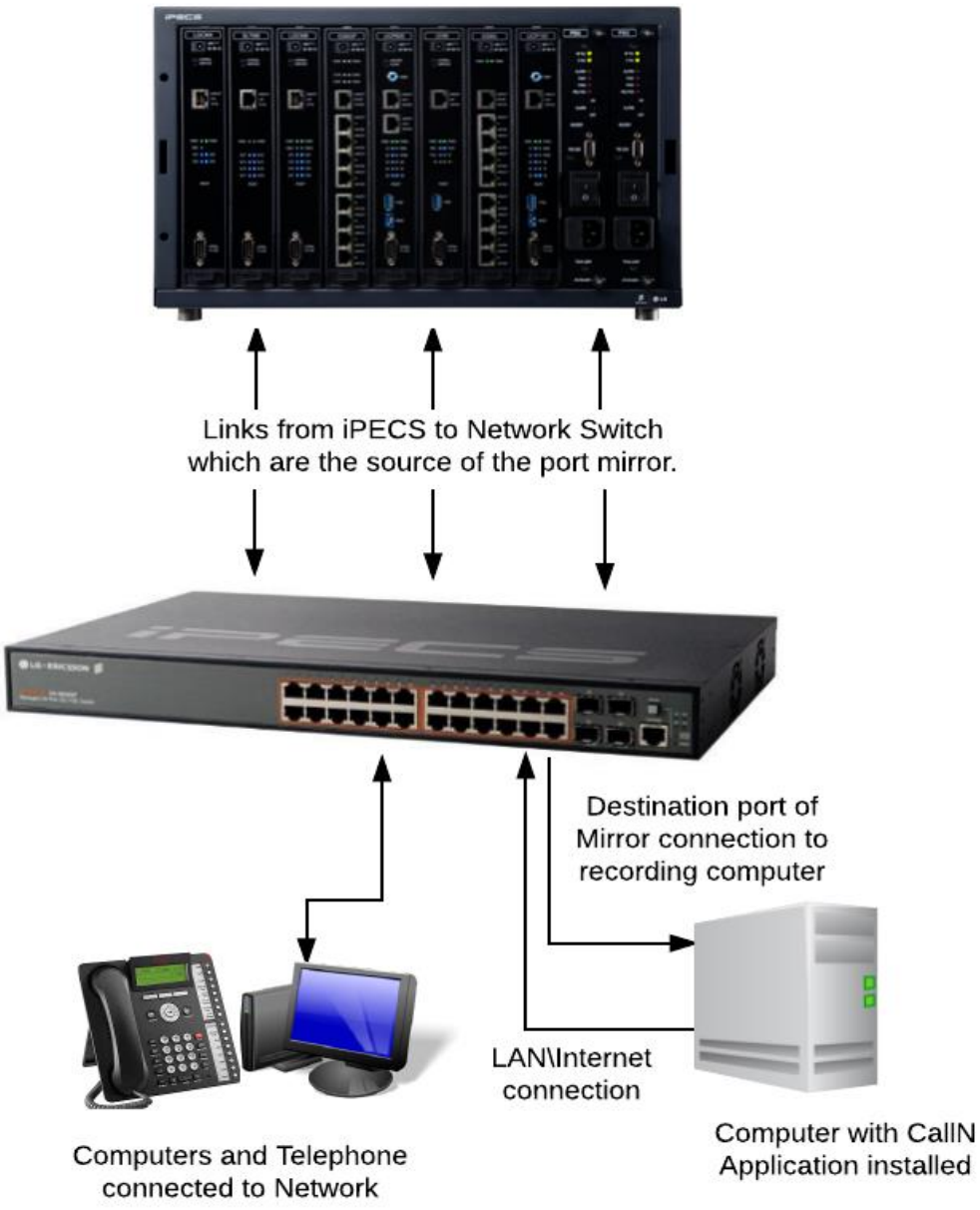
One network connection is connected to the destination port of the port mirror configuration. Typically, this will be the last port on your switch, but can be a nominated port at the time of configuring port mirroring.

The second port is a standard connection to the LAN which provides internet connectivity to allow CallN client to upload voice recordings to your CallN portal.

If using a iPECS eMG80 or similar PBX, you must either be using IP handsets or a SIP trunk to be able to record calls using CallN. It should be noted that if recording on SIP trunks, that the call data presented to CallN is not the same as recording at a handset level. A SIP trunk will typically not pass individual handset extension numbers to CallN, so all calls may appear inbound or outbound from the one main number.



If you are using a iPECS UCP Series PBX, by port mirroring each port on the network switch that connects back to a module in the PBX, telephony traffic can be captured. All external calls will be captured using this method but internal calls may not be captured as the call occurs on the module and traffic never passes through the port mirror to be captured. An example of this may be an internal call between two digital handsets that use the same module in the PBX.

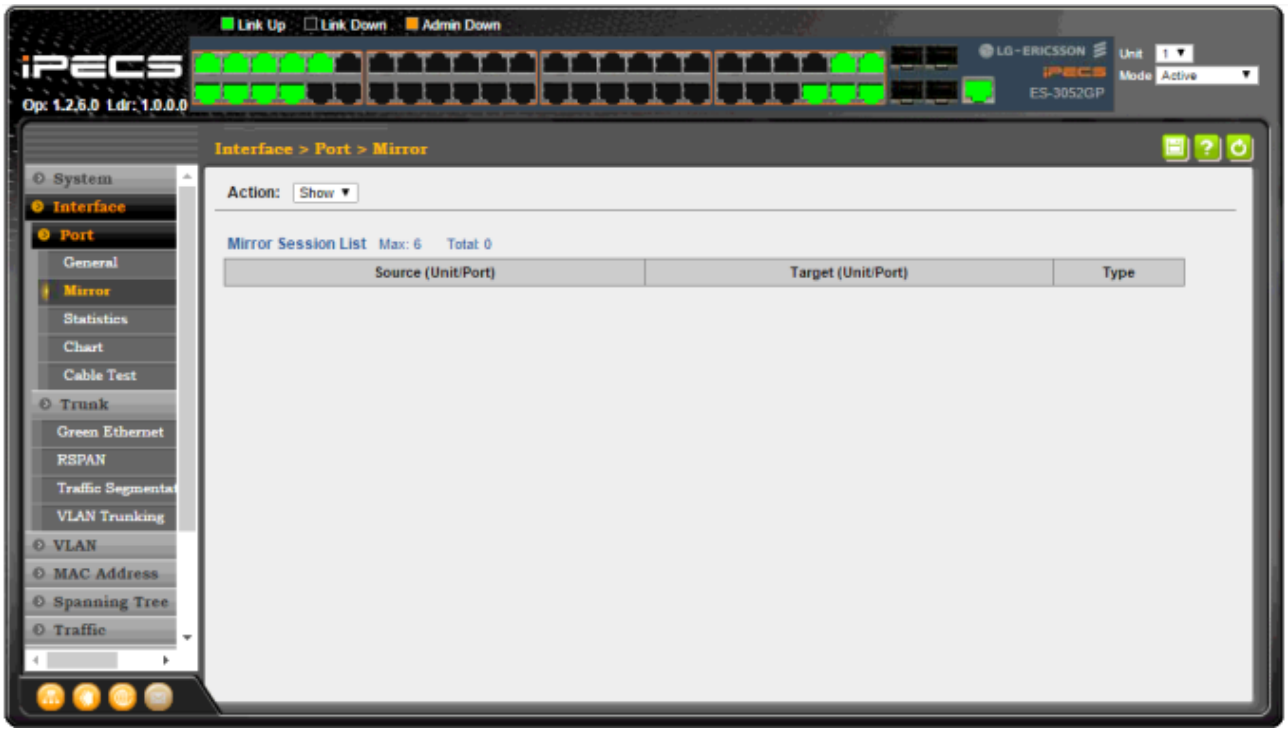

Links from iPECS to Network Switch
which are the source of the port mirror.
Destination port of
Mirror connection to
recording computer
LAN\Internet
connection
Computers and Telephone
connected to Network
Computer with CallN
Application installed

3. Configuration of Port Mirroring

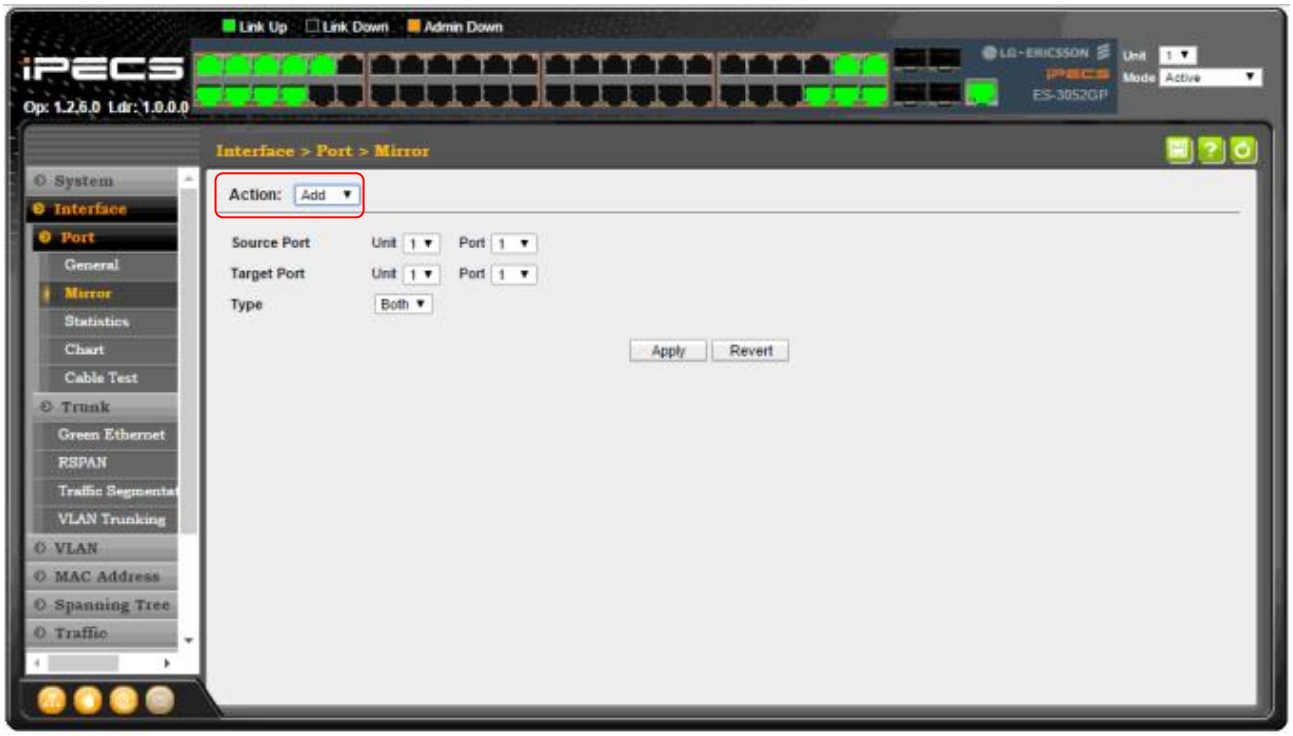
To configure the iPECS switch for port mirroring, log into the Administration Interface of the switch using an Internet Browser. Enter the IP Address of the switch in to the address field of the browser and press enter. Select the option for "Admin & Maintenance".

Enter the Administrators password to continue. If the password or IP address is unknown, the installer or PBX maintenance team should be able to provide details for you.

Once connected, select Interfaces from the menu on the left side.
Then select Port and Mirror.

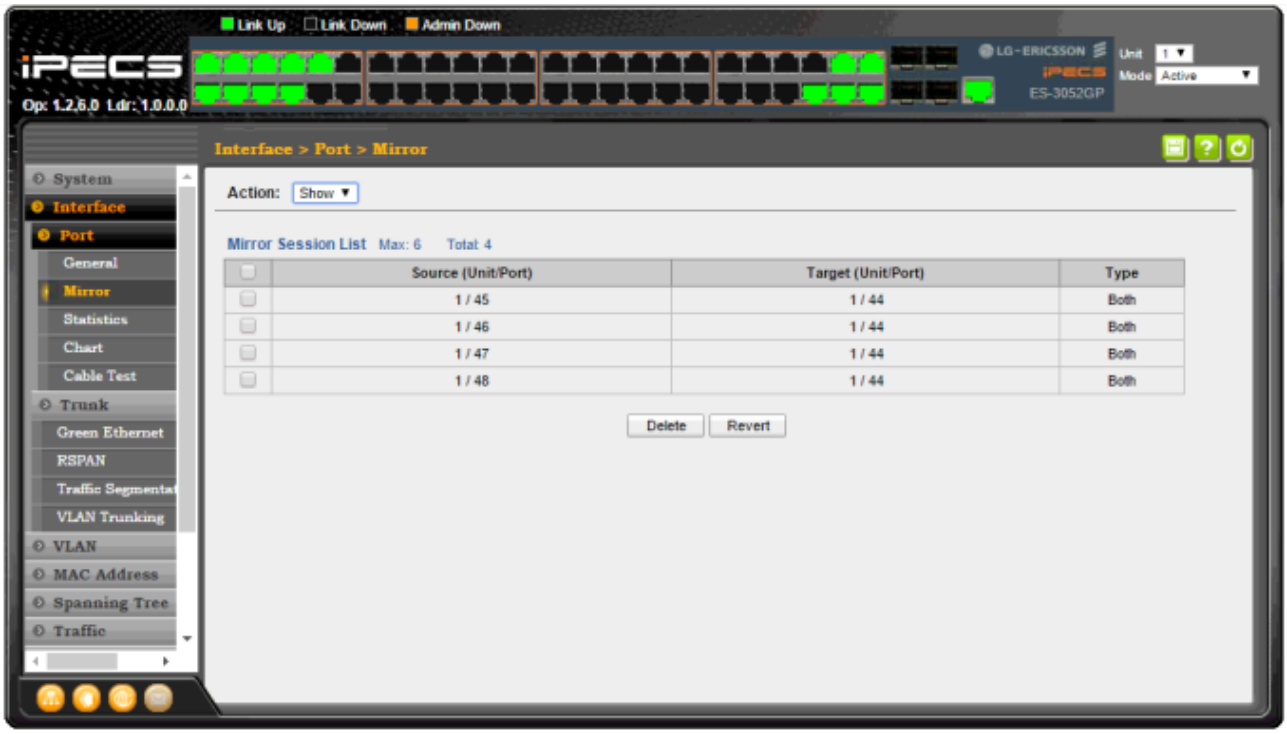


Set the "Action" field to "Add" by selecting add from the drop down menu.



Enter the source unit and source port from the drop down list. The source is the port that is to be mirrored. The Unit is the unit number show in the top right corner of the window and the port is the port number of the port to be mirrored.
Enter the target unit and target port from the drop down list. The Target refers to the destination of the mirrored traffic. The Unit is the unit number show in the top right corner of the window and the port is the port number that will receive the mirrored traffic. The CallN application is connected to this port.

Type refers to the type of traffic to be mirrored. CallN needs to see both parts of a conversation to record all parties on a call. Set Type to Both.
An individual entry must be added for each port that is required to be mirrored. All entries must have the same target port for CallN to work correctly.



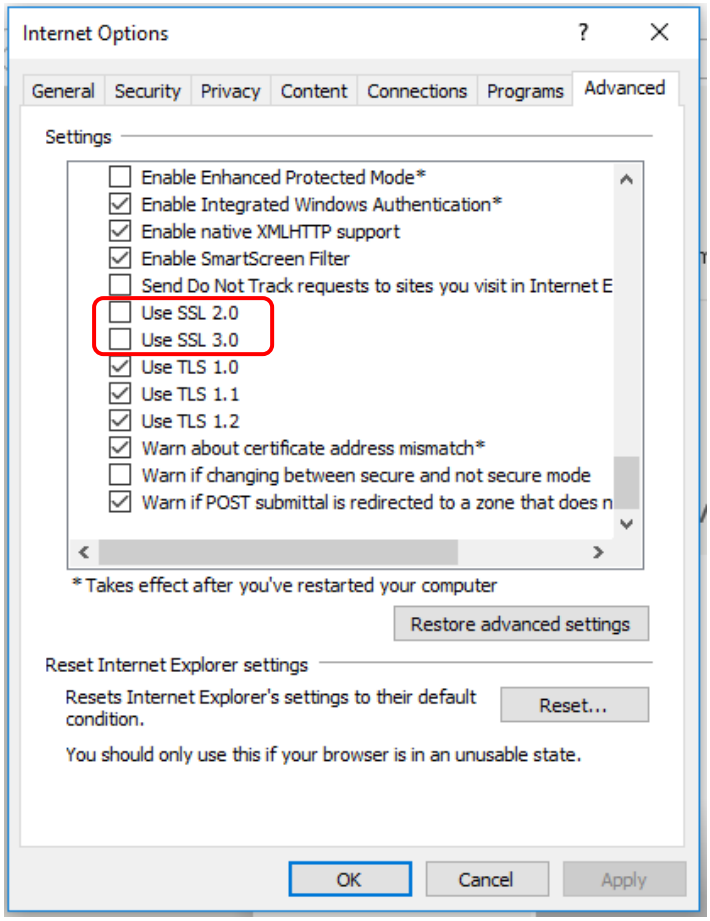
Port mirroring is now established. Place test calls to and from the mirrored ports from both internal and external sources. Log in to the CallN portal and check that recordings are being collected and play back recordings to check recording quality.

There will be situations where recordings are nothing but noise similar to **this**. This is most likely caused by encryption being active on a device, which then encrypts the data stream. CallN is unable to decrypt these data packets, but encryption can be turned off on the devices from the PBX.

4. Disabling Encryption

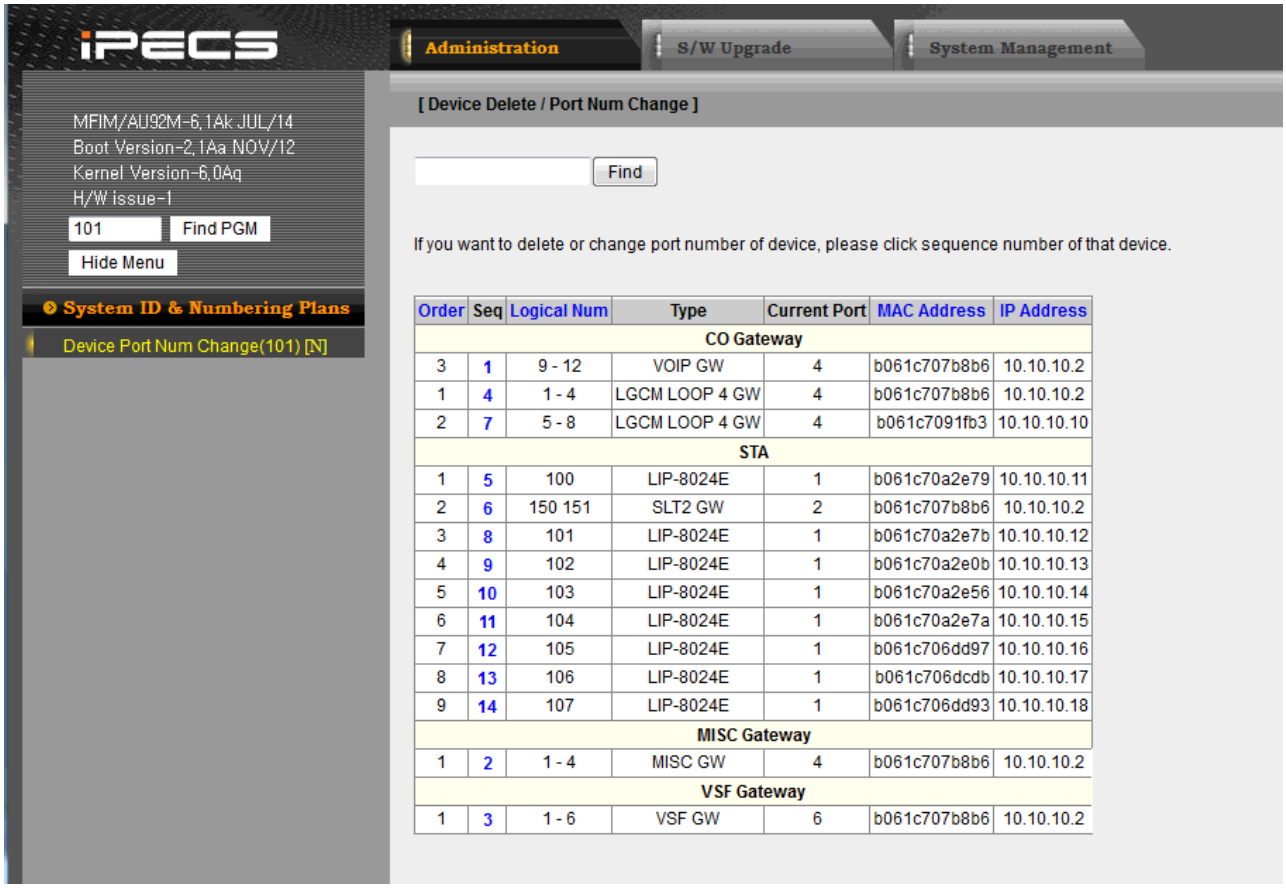
NOTE: Any active call on a device at the time RTP Security is disabled, will be disconnected. For this reason, please ensure there are no active calls on a device before changing this setting.

Connect to the iPECS PBX Administration interface from your web browser. The browser will need to have SSL2 and SSL3 active to connect to the PBX. This is done differently in each browser. In Internet Explorer, click the cog symbol in the top right corner of the browser. From the menu, select Internet Options. Check the boxes on the Advanced Tab to make SSL2 and SSL3 active.



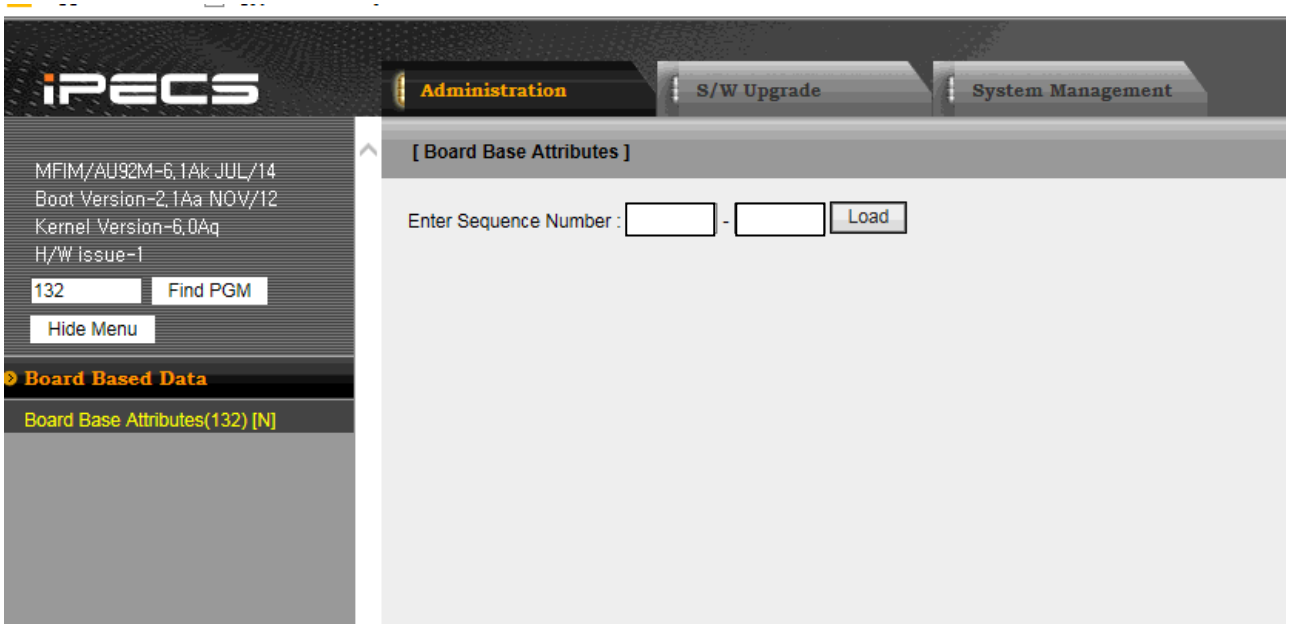
Connect to and log in to the iPECS PBX.

Select "System ID and Number Plan" from the list on the left.
In the vacant field in the top left, enter 101 and click the "Find PGM" button. A list of devices will be displayed.

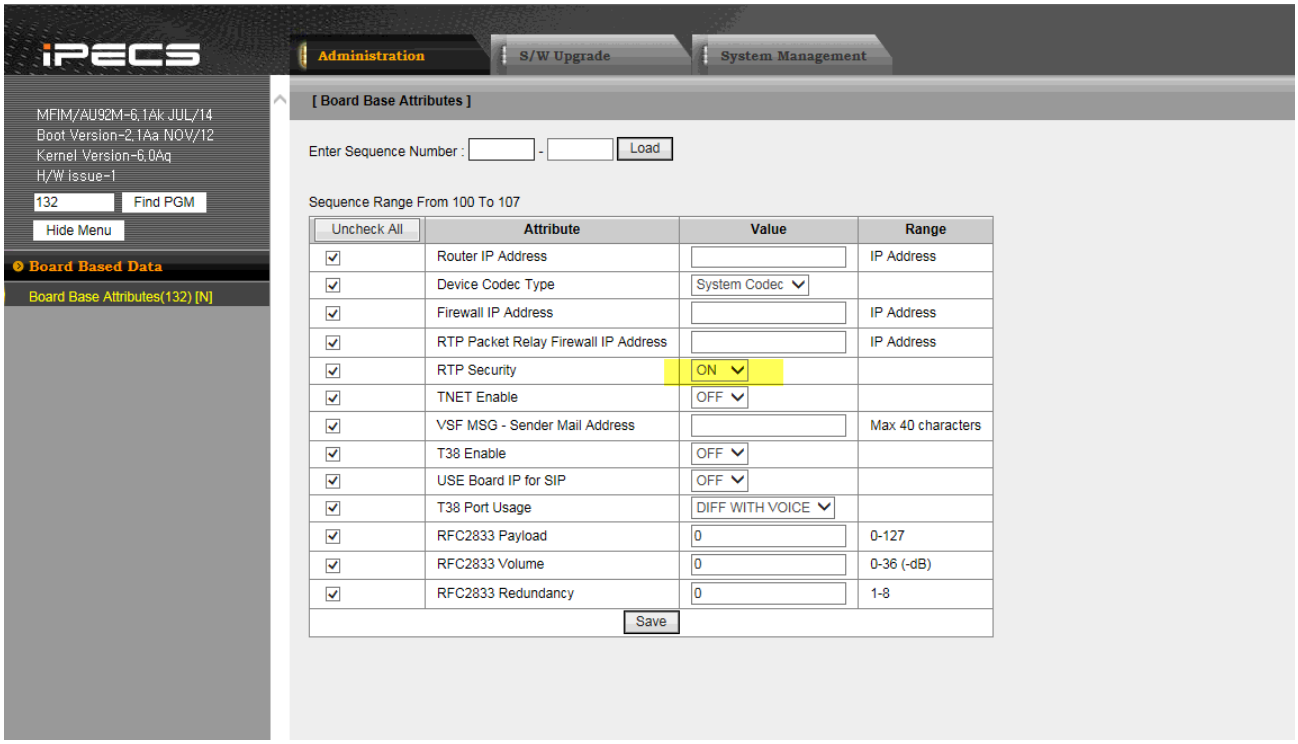


Order	Seq	Logical Num	Type	Current Port	MAC Address	IP Address
CO Gateway						
3	1	9 - 12	VOIP GW	4	b061c707b8b6	10.10.10.2
1	4	1 - 4	LGCM LOOP 4 GW	4	b061c707b8b6	10.10.10.2
2	7	5 - 8	LGCM LOOP 4 GW	4	b061c7091fb3	10.10.10.10
STA						
1	5	100	LIP-8024E	1	b061c70a2e79	10.10.10.11
2	6	150 151	SLT2 GW	2	b061c707b8b6	10.10.10.2
3	8	101	LIP-8024E	1	b061c70a2e7b	10.10.10.12
4	9	102	LIP-8024E	1	b061c70a2e0b	10.10.10.13
5	10	103	LIP-8024E	1	b061c70a2e56	10.10.10.14
6	11	104	LIP-8024E	1	b061c70a2e7a	10.10.10.15
7	12	105	LIP-8024E	1	b061c706dd97	10.10.10.16
8	13	106	LIP-8024E	1	b061c706dcdb	10.10.10.17
9	14	107	LIP-8024E	1	b061c706dd93	10.10.10.18
MISC Gateway						
1	2	1 - 4	MISC GW	4	b061c707b8b6	10.10.10.2
VSF Gateway						
1	3	1 - 6	VSF GW	6	b061c707b8b6	10.10.10.2

Each device listed must be checked to ensure "RTP Security" is turned off for that device.
Make a note of each of the sequence numbers listed for the devices.
Remove 101 from the field in the top left and enter 132, again pressing the "Find PGM" button.



Enter in a Sequence Number. The edit of devices can be done one at a time or over a range. Caution must be taken if entering a range of sequence numbers that no invalid values are part of the range. It is recommended to change RTP Security setting on one device at a time.



Deselect all check boxes.
Select only RTP Security.
Drop down the box for RPT Security and select off.
Before saving the setting for his device, check that there are no active calls on the device.
Click Save to save the settings, when no active calls are on the device. Any call active on the device when the “Save” button is pressed will be disconnected.

Once all devices have had RTP Security disabled, place some test calls from internal and external sources, checking the call recordings to see if the issue has been resolved.