



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Imagine Soft Meteor with Avaya IP Office 500 R8.1 - Issue 1.0

Abstract

These Application Notes describe the compliance testing of Imagine Soft Meteor with Avaya IP Office 8.1. Meteor is used in hospitality industries to assist with check-in check-out and telephone usage authorization.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Imagine Soft Meteor server provides various telephony capabilities which help meet the needs of the hospitality industry. Meteor has the following capabilities which interact with Avaya IP Office:

- Meteor provides a check-in/check-out facility which changes telephone access privileges, providing telephone access to guests immediately upon check-in, and preventing unauthorized use after check-out.
- Meteor can assign a name to the telephone upon check-in, so that hotel or hospital staff can immediately recognize guests or patients from whom they receive telephone calls.
- Meteor allows hotel personnel to update room status via telephone to indicate the state of the room (i.e. it has been serviced by housekeeping, etc.).
- Meteor allows hotel guests to retrieve voicemail messages via external telephones attached to the Public Switched Telephone Network (PSTN).
- Meteor allows each hotel guest to program WAKEUP in his own language (6 languages) and hotel staff to verify wakeup status.
- Meteor can assign Direct Inward Dial (DID) extensions to hotel guests to enable them to have a telephone number independent of their room number which can be called from PSTN telephones, allowing guests to be reached by the same number, even though they may change hotel rooms.

2. General Test Approach and Test Results

The general test approach was to configure the Imagine Soft Meteor (Meteor) to communicate with the Avaya IP Office (IP Office) as implemented on a customer's premises. See **Figure 1** for a network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The testing included:

- Perform a guest check-in and verify that the guest's name is assigned to the telephone assigned to the guest's room, and that the guest is able to make calls via the PSTN.
- Perform a guest checkout and verify that the guest's name no longer assigned to the telephone, that the telephone can no longer make external calls, that the MWI light goes out if it was on prior to checkout, and any wakeup calls pending for that guest are removed.
- Verify that a room change causes the guest's messages, MWI status, calling privileges, station name, and wakeup calls to be assigned to the new extension.

- Verify that the system administrator can manually turn on or off a guest telephone's MWI lamp.
- Verify that local and external calls can leave messages for guests, and the guest can retrieve these messages, and that the state of the MWI lamp changes correctly.
- Verify that wakeup calls can be created or erased by either guests or administrators, and the wakeup calls are signaled correctly to guests.
- Verify that guests are billed correctly for local and external calls.
- Verify that DND can be activated or deactivated correctly by the administrator, and the incoming calls are blocked correctly.
- Verify that DID's can be assigned to guests, and can be called correctly from external telephones.

2.2. Test Results

Tests were performed to insure full interoperability between Meteor and IP Office. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

Technical support from Imagine Soft can be obtained through the following:

Phone: +33 491327432
E-mail: hotline1@imaginesoft.fr
Fax: +33 491327401

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an IP Office 500 which is configured to output SMDR. 4 analog lines between Meteor SE and the IP Office are used to access Voicemail and send announcements and wake-up messages to guest telephones. The number of lines required is dependent on the number of guest extensions. Digital 2420, and 9640G H323 extensions were configured on the IP Office as Guest phones. A QSIG trunk was configured to connect to the PSTN over which external calls can be made and received. During compliance testing the Meteor server was used to host the Meteor Console application which is browser based.

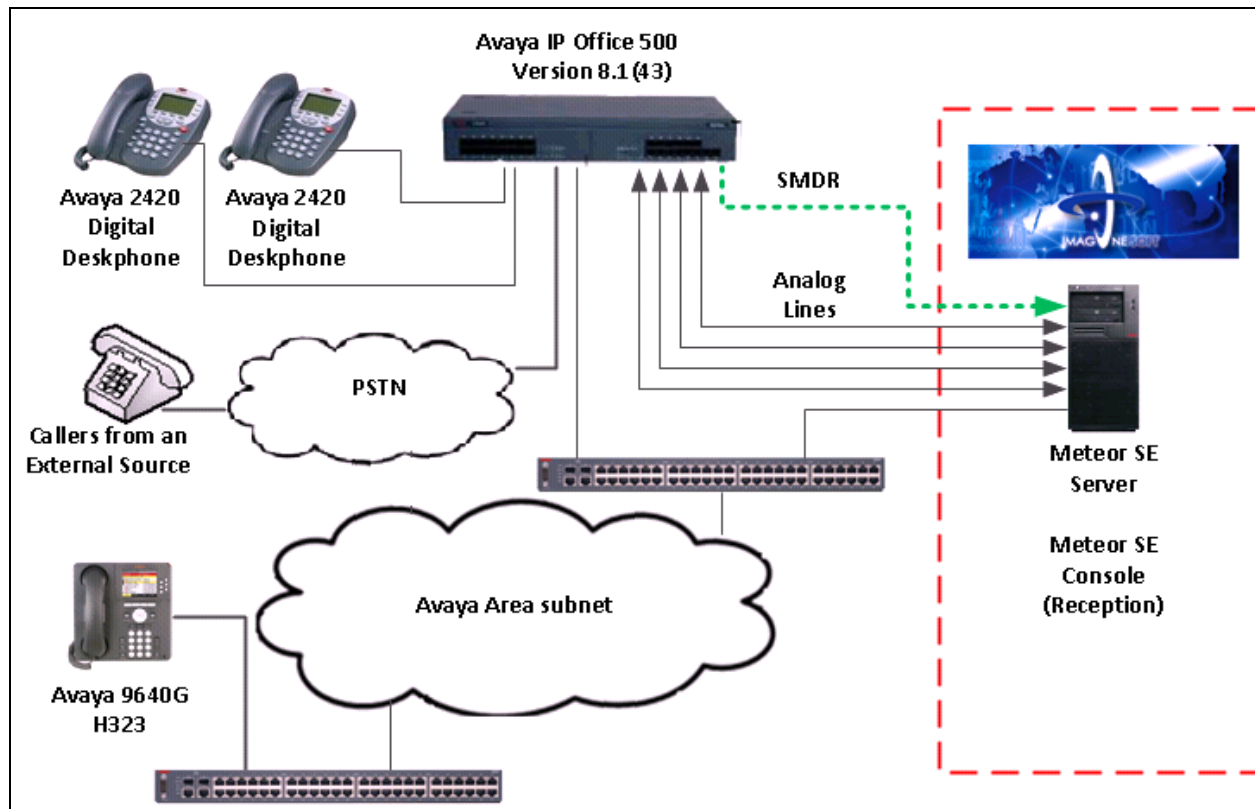


Figure 1: Avaya IP Office and Imagine Soft Meteor Reference Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Equipment	Software / Firmware Version
Avaya IP Office 500	8.1(43)
Avaya 9640G IP Telephone	H323 S3.104S
Avaya 2420 Digital Telephones	--
Avaya IP Office Softphone	3.2.3.48
Imagine Soft Equipment	Software / Firmware Version
Fujitsu Esprimo running Microsoft Windows 7 Professional SP1	Meteor 5.00 Microsoft Internet Explorer 9 (Meteor client) MySQL 4.0.18 Tomcat 6.0.14 MS C++ Runtime 2005 SP1 MS.net Framework 4.0
Dialogic D4PCI Analog Telephone Interface	D/4PCI e

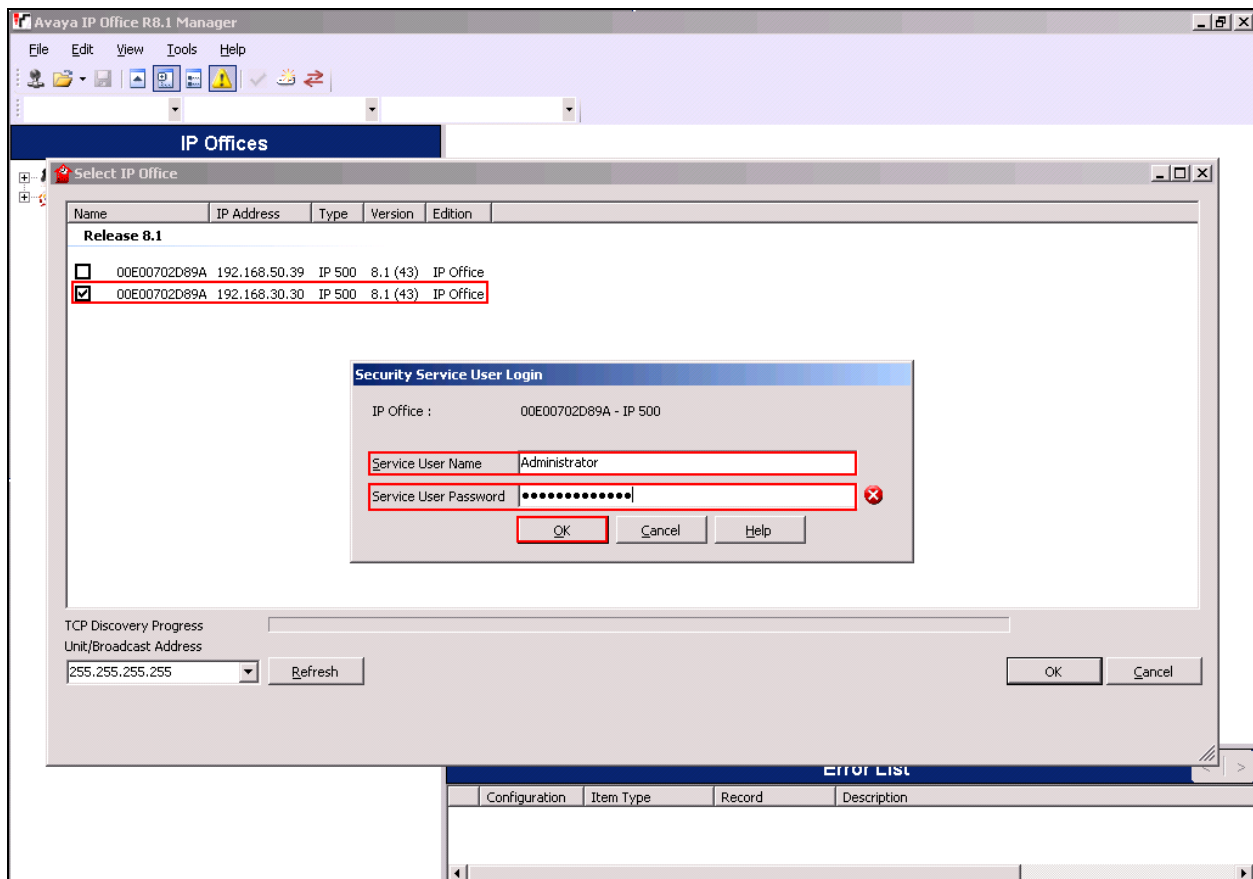
5. Avaya IP Office Configuration

Configuration and verification operations on the Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration of the Avaya IP Office for this solution. It is implied a working system is already in place. During compliance testing Guest users/Extensions, Hunt groups, Virtual Users for DDI, User Rights Short Codes and analog extensions (for IVR and Voicemail) were configured but are outside the scope of this Application Note. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

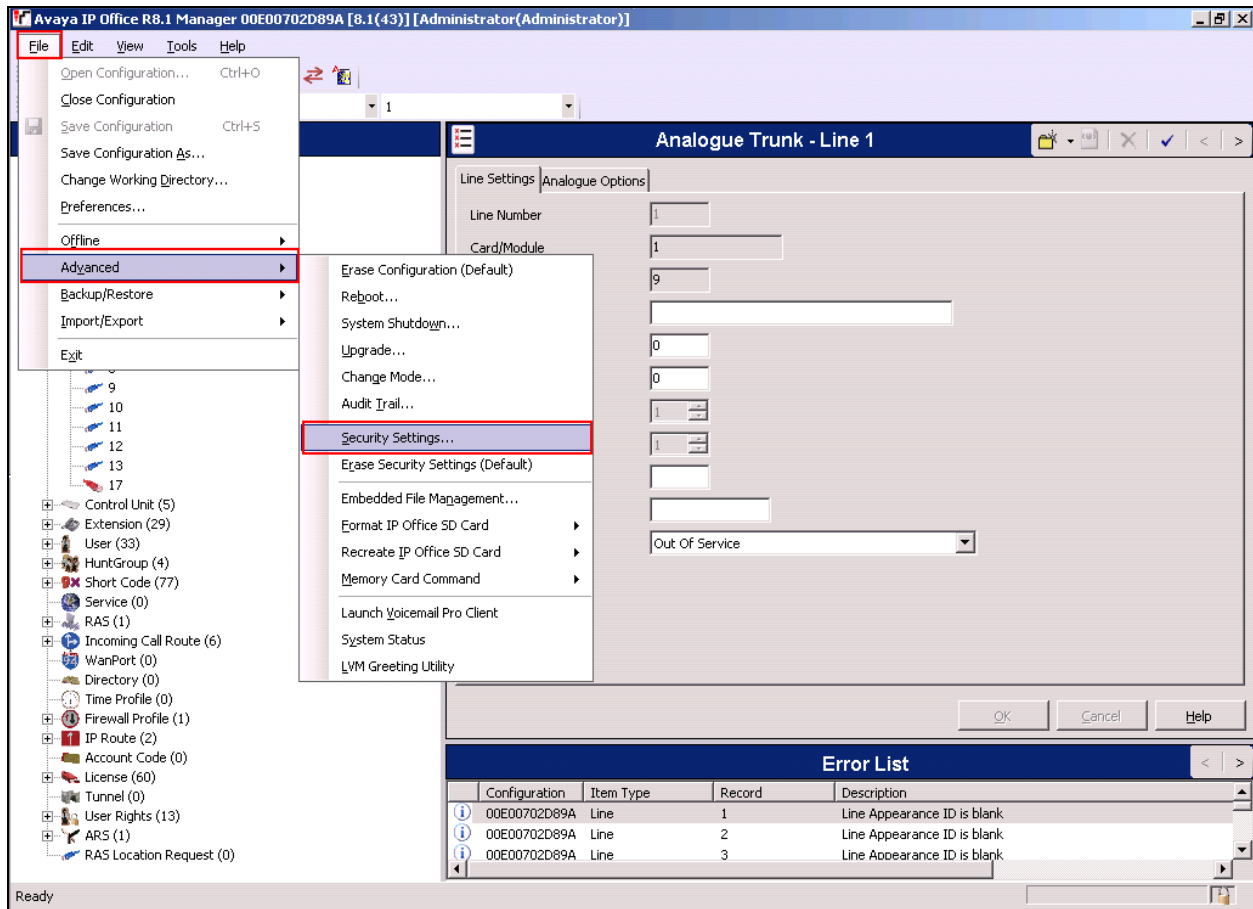
- Launch Avaya IP Office Manager (Security)
- Security Level
- Launch Avaya IP Office Manager (Administration)
- System configuration
- Voicemail Configuration
- SMDR Configuration
- Save Configuration

5.1. Launch Avaya IP Office Manager (Security)

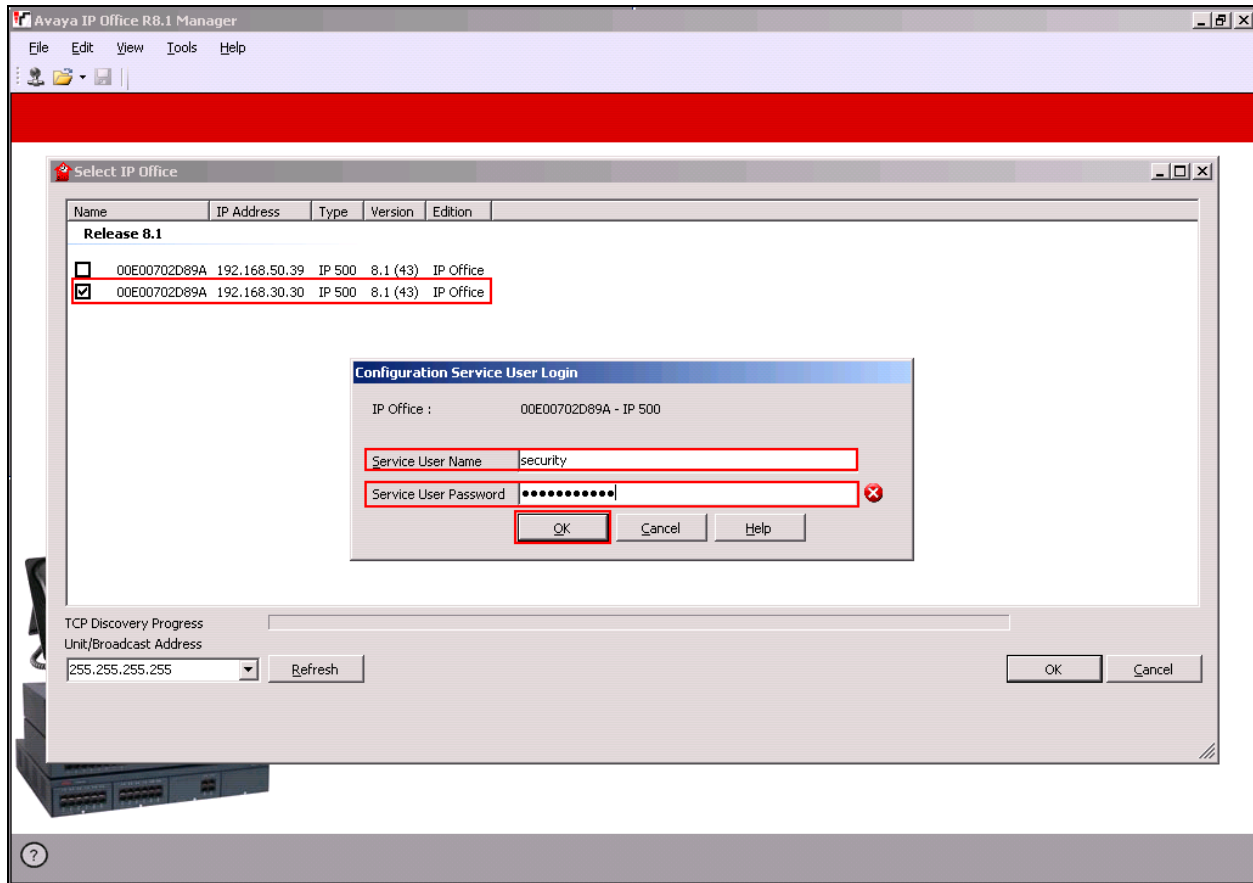
To Log in as a Security administrator first Log in as Administrator. From the IP Office Manager PC, go to **Start→Programs→IP Office→Manager** to launch the Manager application. Select **File →Open Configuration** then select the appropriate IP Office. Log in to IP Office using the **Service User Name** of **Administrator** and the appropriate **Service User Password** and click on the **OK** button. During compliance testing the System was called **00E00702D89A**.



Once the Configuration is opened select **File → Advanced → Security Settings**.

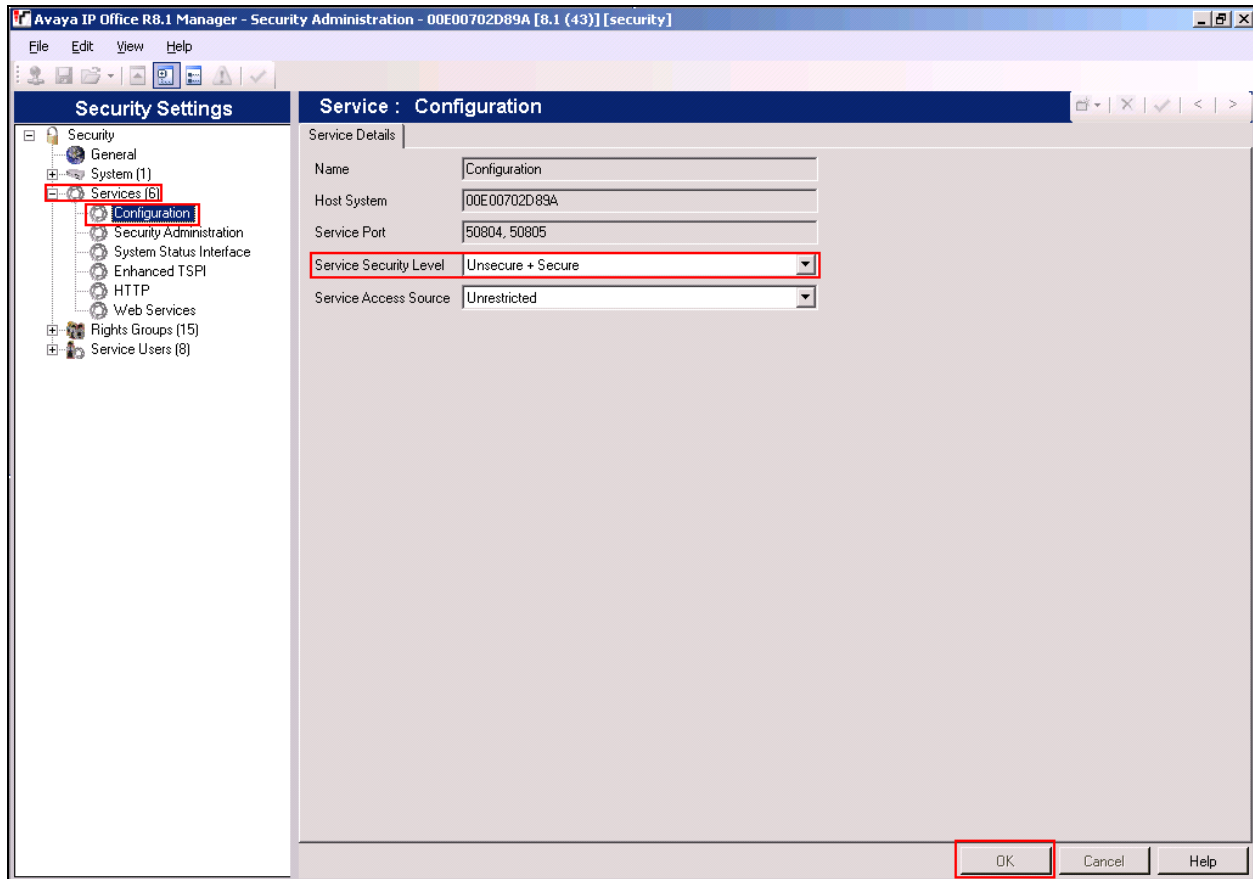


In the **Configuration Service User Login** window Log in using the **Service User Name** of **security** and the appropriate **Service User Password** and click **OK**.

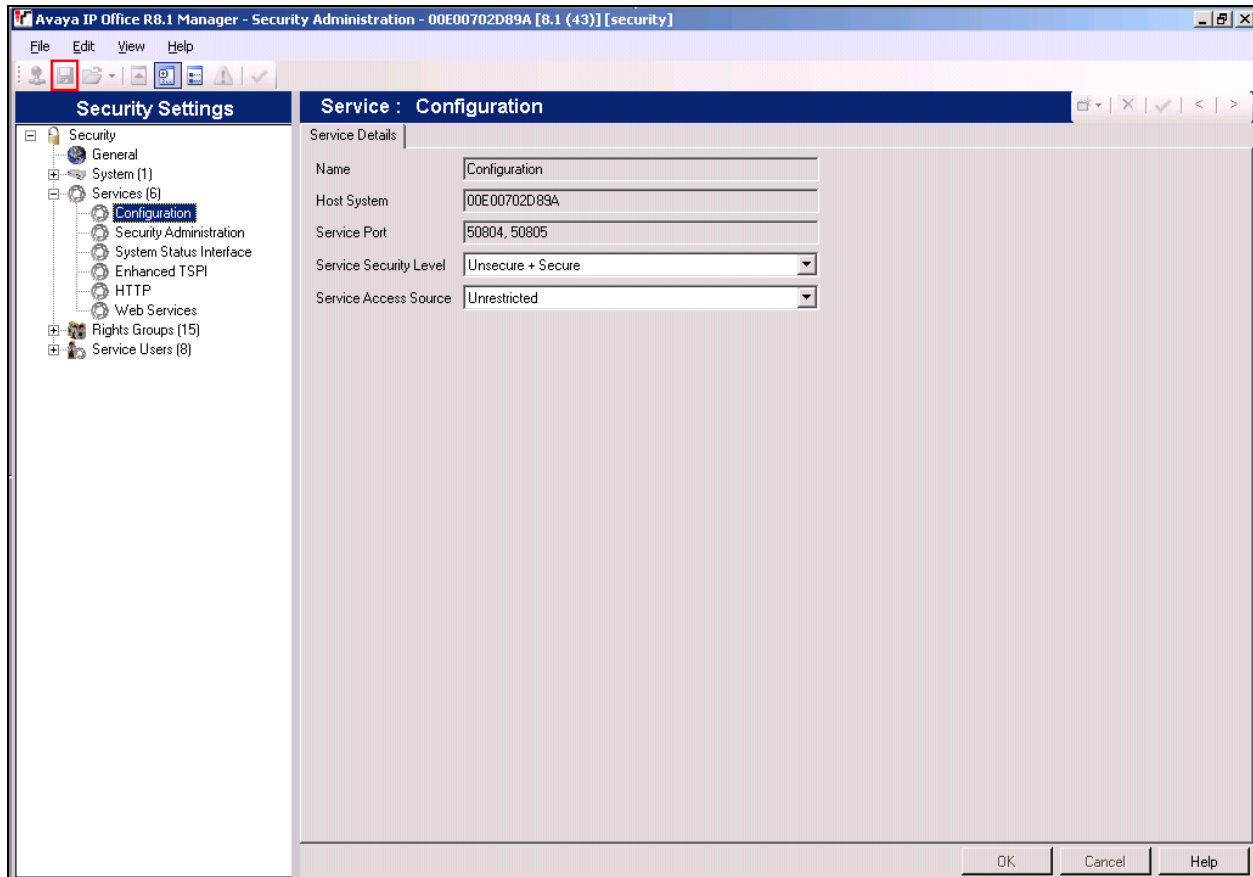


5.2. Security Level

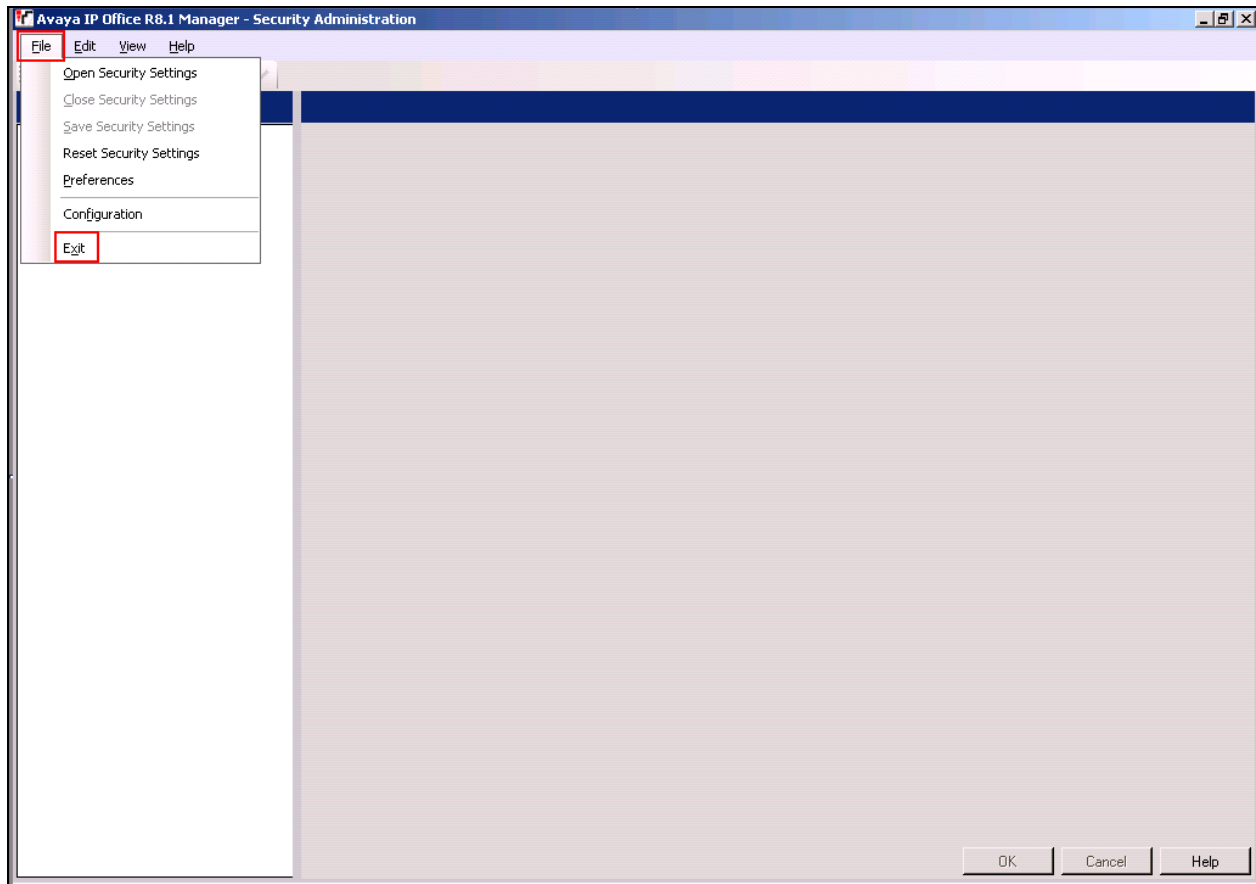
Once the **Security Administration** page opens, select **Services** → **Configuration** and select **Unsecure + Secure** from the **Service Security Level** drop-down box and click **OK**.



Click on the **Save** icon to save the new setting. Enter the appropriate the **Service User Name** and **Service User Password** and click on **OK** to complete (not shown).

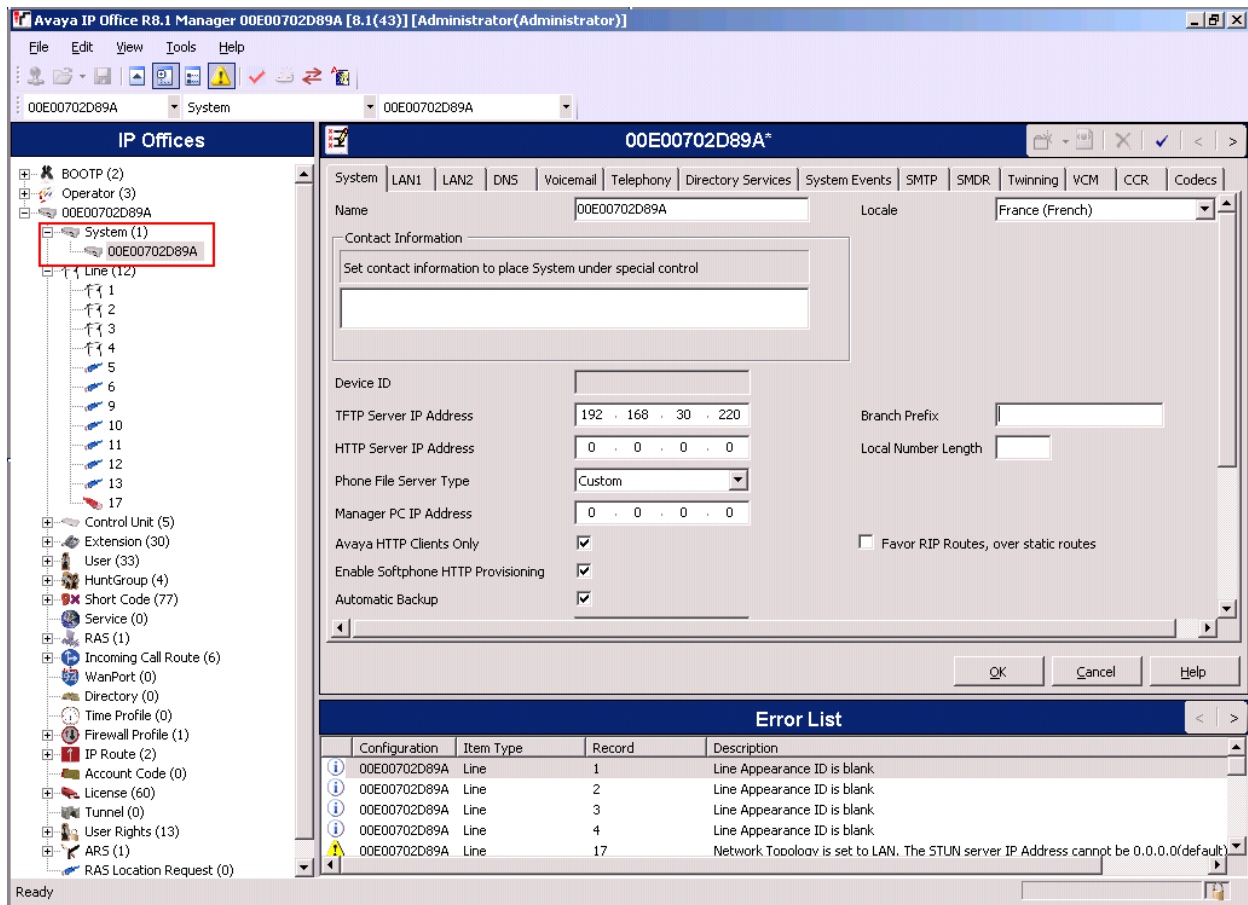


To log out of the **Security Administration** click **File → Exit**.



5.3. Launch Avaya IP Office Manager (Administration)

From the IP Office Manager PC, click **Start→Programs→IP Office→Manager** to launch the Manager application. Log in to IP Office using the appropriate credentials (not shown) to receive the IP Office configuration .



5.4. System Configuration

During compliance testing the Locale was set to France so as to interoperate correctly with the Dialogic D4PCI Analog Telephone Interface. Select the **System** tab and Select **France (French)** from the **Locale** drop box and click **OK**

The screenshot shows the 'System Configuration' window for device 00E00702D89A. The 'System' tab is active. The 'Name' field contains '00E00702D89A'. The 'Locale' dropdown menu is open, showing 'France (French)' selected. The 'Contact Information' section has a text box with the instruction 'Set contact information to place System under special control'. The 'Device ID' field is empty. The 'TFTP Server IP Address' is '192 . 168 . 30 . 220'. The 'HTTP Server IP Address' is '0 . 0 . 0 . 0'. The 'Phone File Server Type' is 'Custom'. The 'Manager PC IP Address' is '0 . 0 . 0 . 0'. The 'Avaya HTTP Clients Only' checkbox is checked. The 'Enable Softphone HTTP Provisioning' checkbox is checked. The 'Automatic Backup' checkbox is checked. The 'Branch Prefix' field is empty. The 'Local Number Length' field is empty. The 'Favor RIP Routes, over static routes' checkbox is unchecked. The 'OK' button is highlighted with a red box.

5.5. Voicemail Configuration

As Voicemail is part of the Meteor Solution the IP Office Voicemail must be switched off. Select the **Voicemail** tab and select **<None>** as the **Voicemail Type** and click **OK**.

The screenshot shows the 'Voicemail Configuration' window for a system identified as '00E00702D89A*'. The 'Voicemail' tab is active. The 'Voicemail Type' is set to '<None>'. The 'Voicemail Destination' is empty. The 'Voicemail IP Address' is 255.255.255.255. The 'Backup Voicemail IP Address' is 0.0.0.0. The 'Voicemail Channel Reservation' section shows 'Unreserved Channels' as 259. The 'SIP Settings' section has 'Anonymous' checked. The 'OK' button is highlighted with a red box.

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	Twinning	VCM	CCR	Codecs
Voicemail Type: <None>													
Voicemail Destination:													
Voicemail IP Address: 255 . 255 . 255 . 255													
Backup Voicemail IP Address: 0 . 0 . 0 . 0													
Voicemail Channel Reservation													
Unreserved Channels: 259													
Auto-Attendant: 0 Voice Recording: 0 Mandatory Voice Recording: 0													
Announcements: 0 Mailbox Access: 0													
SIP Settings													
SIP Name:													
SIP Display Name (Alias):													
Contact:													
Anonymous: <input checked="" type="checkbox"/>													
OK Cancel Help													

5.6. SMDR Configuration

Select the **SMDR** tab, and enter the following information and click **OK**:

- **Output** Select **SMDR Only** from the drop box
- **IP Address** Enter the IP Address of the Meteor Server
- **TCP Port** Enter **5010**
- **Records to buffer** Enter **3000**. This is maximum available
- Uncheck the **Call Splitting for Diverts** check box

00E00702D89A*

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | **SMDR** | Twinning | VCM | CCR | Codecs

Output: SMDR Only

SMDR

Station Message Detail Recorder Communications

IP Address: 192 . 168 . 30 . 35

TCP Port: 5010

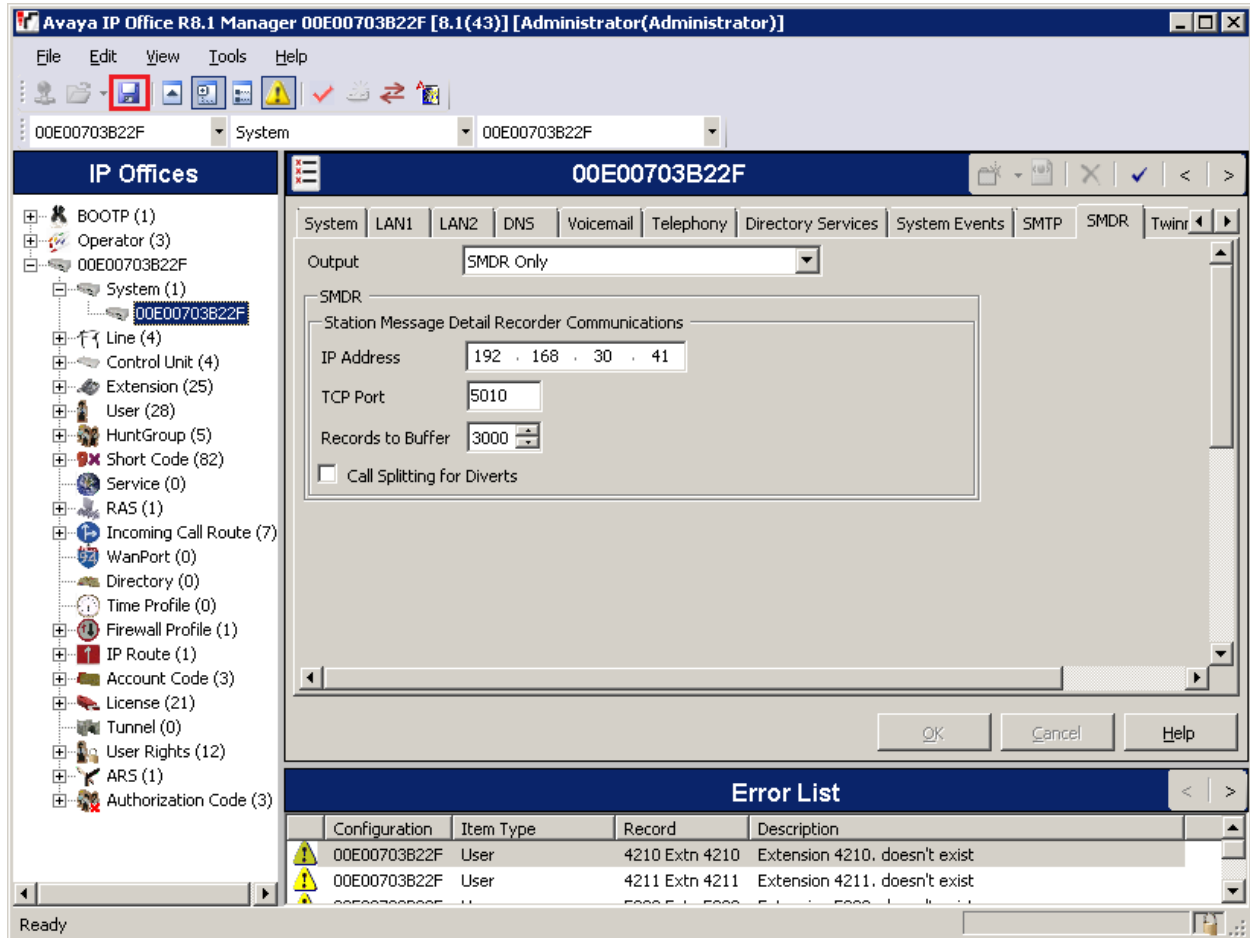
Records to Buffer: 3000

☐ Call Splitting for Diverts

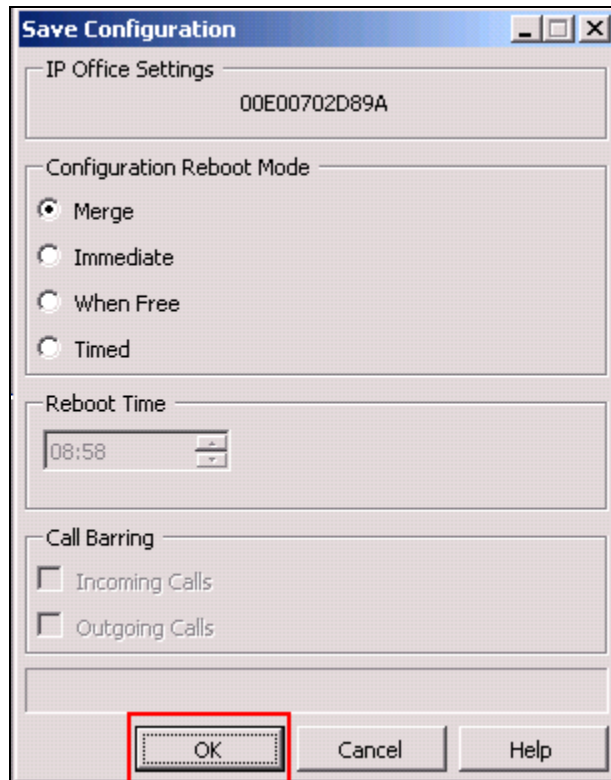
OK Cancel Help

5.7. Save Configuration

Once all the configurations have been made it must be sent to the IP Office. Click on the **Save** Icon as shown below.

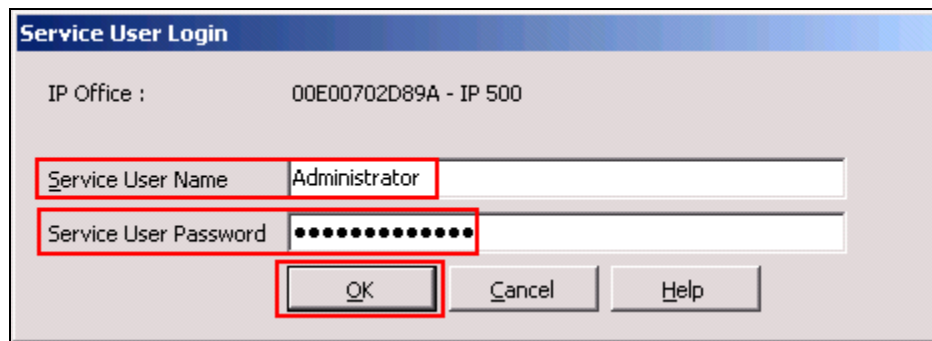


Once the **Save Configuration** window opens, click **OK**.



The **Save Configuration** dialog box is shown. It has a title bar with standard window controls. The main area contains four sections: **IP Office Settings** with the value 00E00702D89A; **Configuration Reboot Mode** with four radio buttons (Merge is selected, followed by Immediate, When Free, and Timed); **Reboot Time** with a time picker set to 08:58; and **Call Barring** with two unchecked checkboxes (Incoming Calls and Outgoing Calls). At the bottom, there are three buttons: **OK**, **Cancel**, and **Help**. The **OK** button is highlighted with a red rectangular box.

When the **Service User Login** Window opens enter the appropriate credentials and click **OK**.



The **Service User Login** dialog box is shown. It has a title bar with standard window controls. The main area contains: **IP Office :** 00E00702D89A - IP 500; **Service User Name** with the text Administrator; **Service User Password** with a masked password (represented by dots); and three buttons at the bottom: **OK**, **Cancel**, and **Help**. Both the password input field and the **OK** button are highlighted with red rectangular boxes.

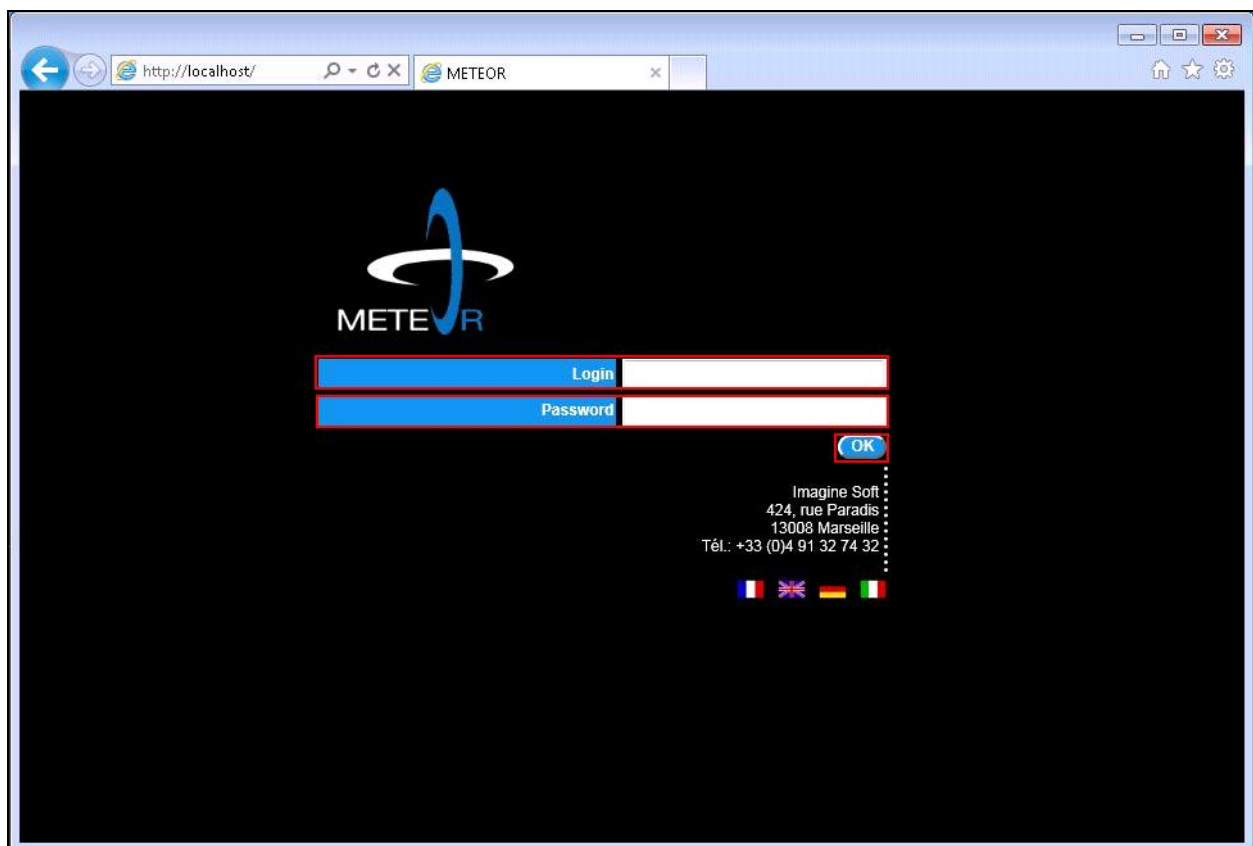
6. Configure Meteor Server

This section provides the procedures to configure the Meteor Server. It is implied that the Meteor is already in place, including license, Voice Mail and Hotel Configuration and is configured with an IP address on the same subnet as the IP Office. It is also implied that the Dialogic D/4PC1 is installed and configured. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Login to the Meteor server
- Configure Interface Parameters
- Restart Meteor server

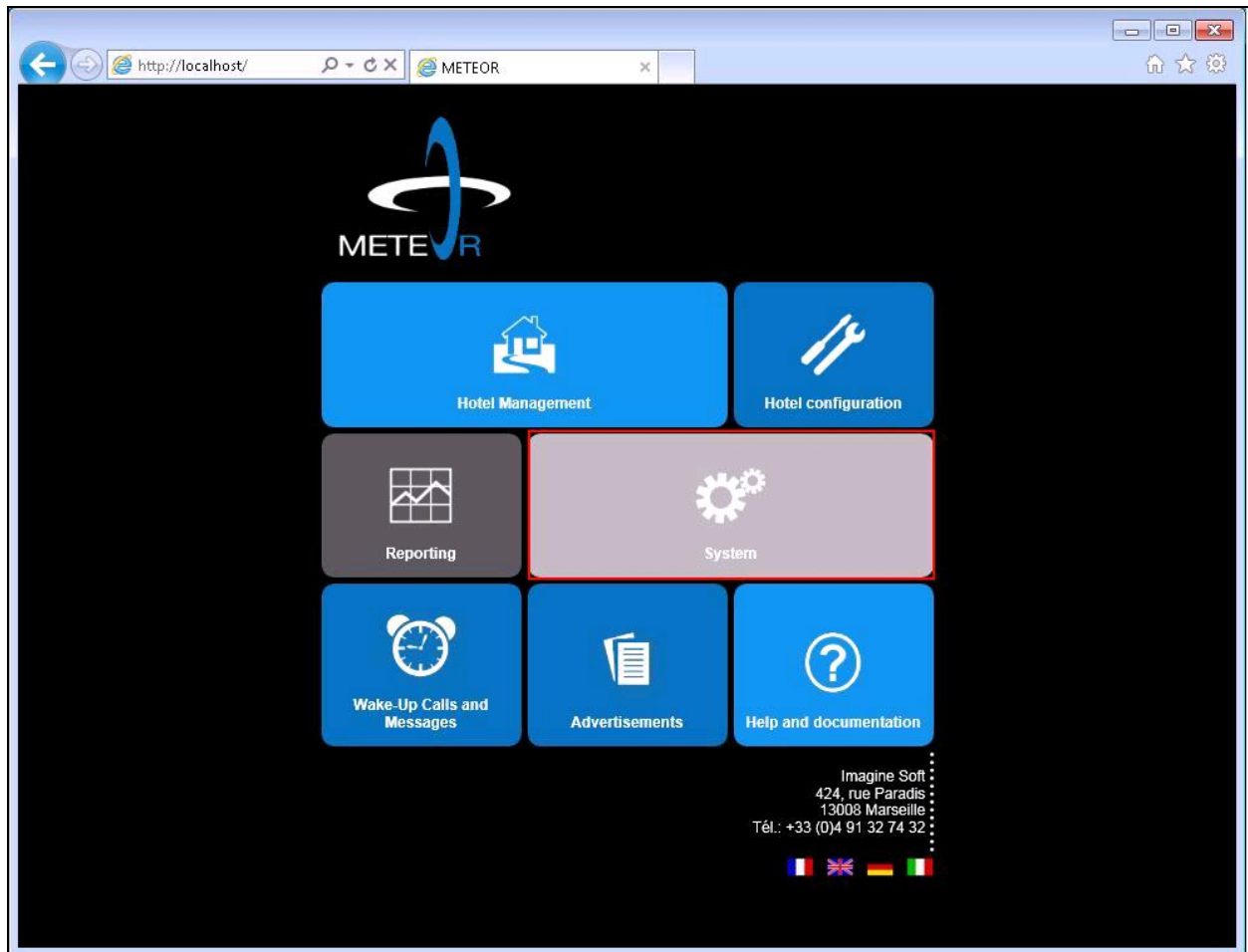
6.1. Login to the Meteor server

To access the web-based interface of the Meteor server use the URL **<http://x.x.x.x>**, where **x.x.x.x** is the selected IP address of the Meteor Server. Enter the appropriate **Login** and **Password** credentials and click **OK**.

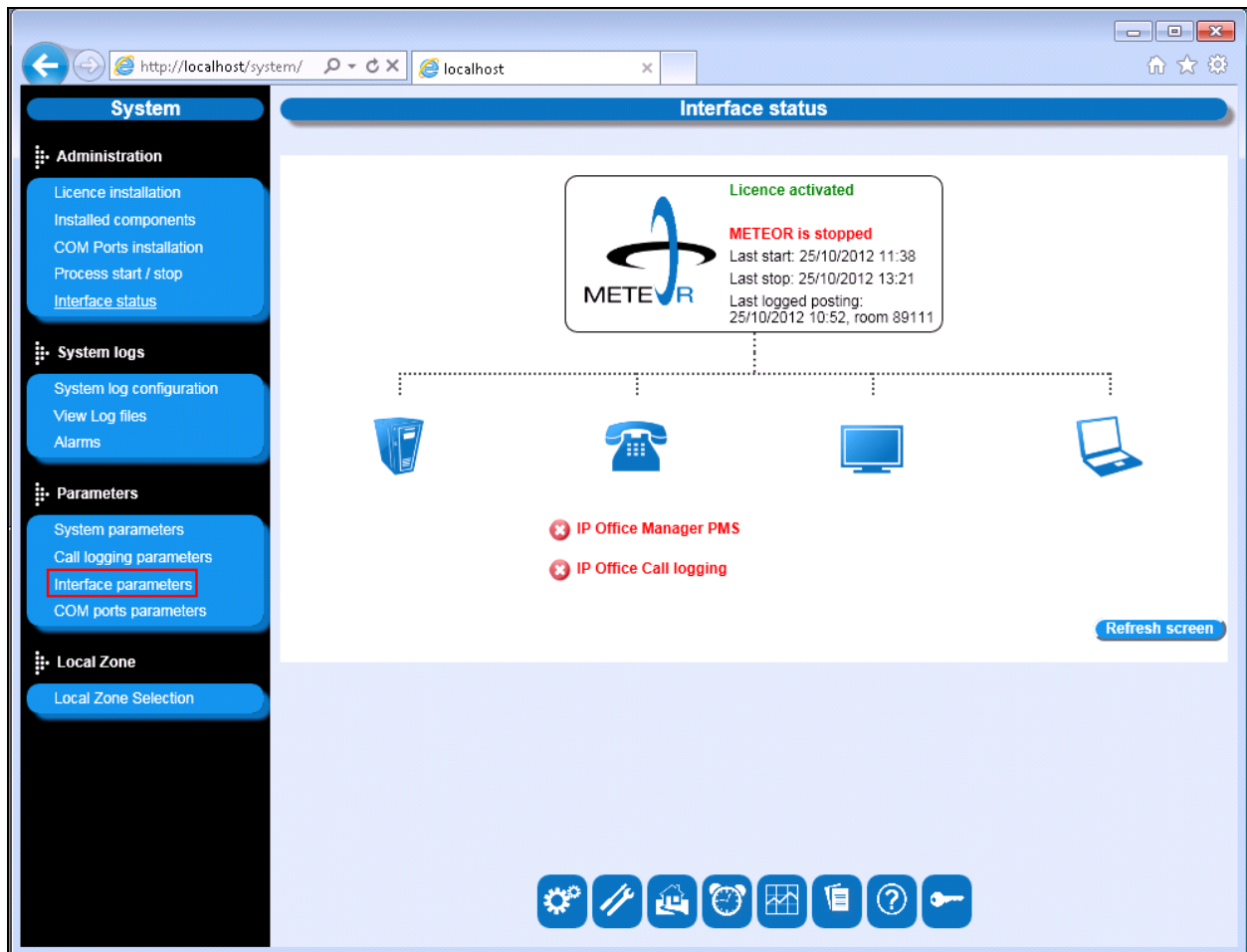


6.2. Configure Interfaces Parameters

Once the main page opens select **System**.

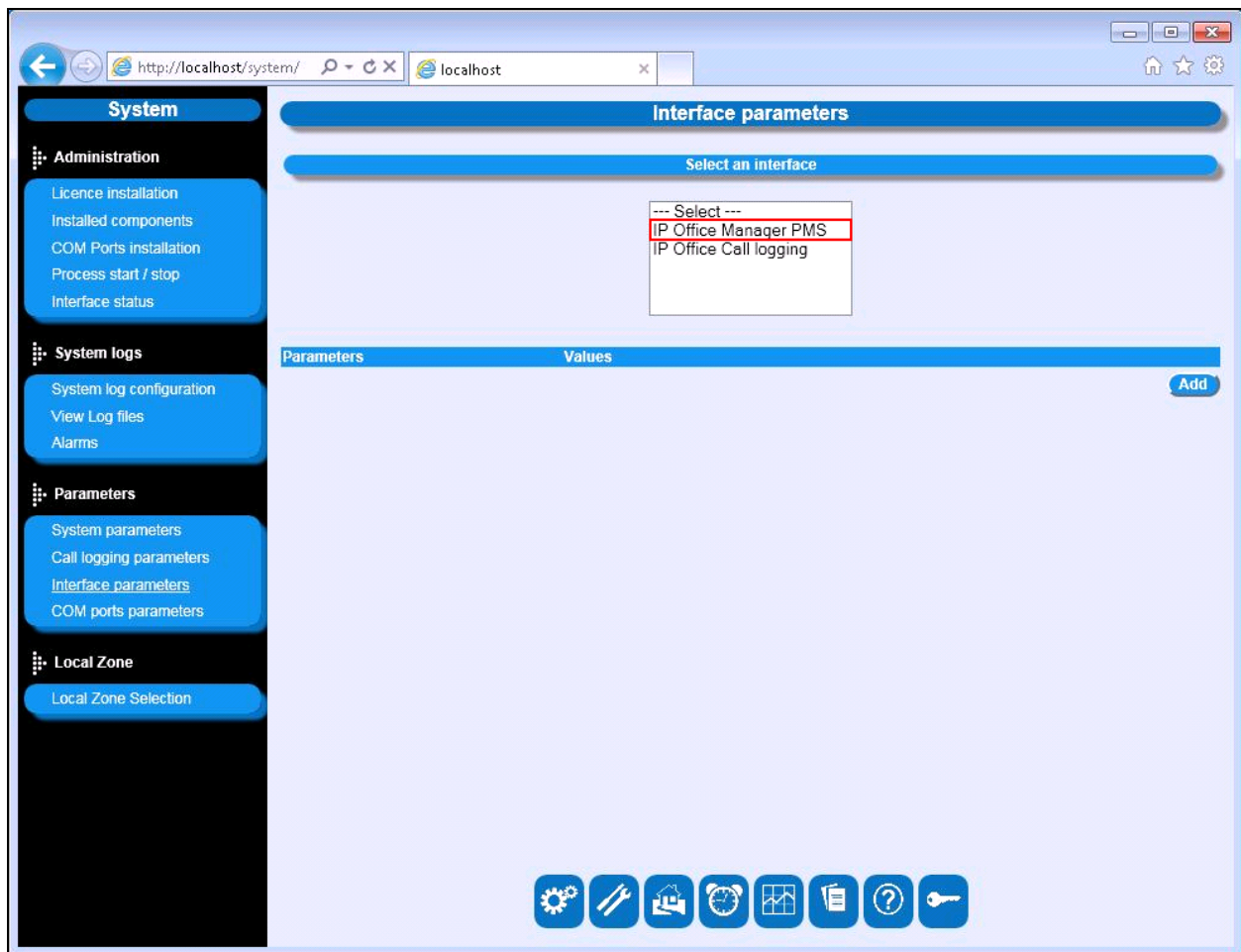


Once the next page opens select **Interface parameters** from the left frame.



6.2.1. Configure IP Office Manager PMS Parameters

On the **Select an interface** page select **IP Office Manager PMS**.



Once the **IP Office Manager PMS** Parameters page opens set the value for each parameter shown in the following table by selecting **Update** for each of the highlighted entries, one at a time. Enter the values indicated in the table. When these parameters have been configured, click the **Add** button.

Parameter	Usage
Configuration Web Services port	Enter the port to be used by Web Services
IP Office PBX IP	Enter the IP address of Avaya IP Office LAN interface
Login	Enter the Avaya IP Office administrator user ID
Password	Enter the Avaya IP Office administrator user password
DDI Prefix	Set the value to the leading digit which is used for DDI extensions
Timeout	Enter the Timeout value

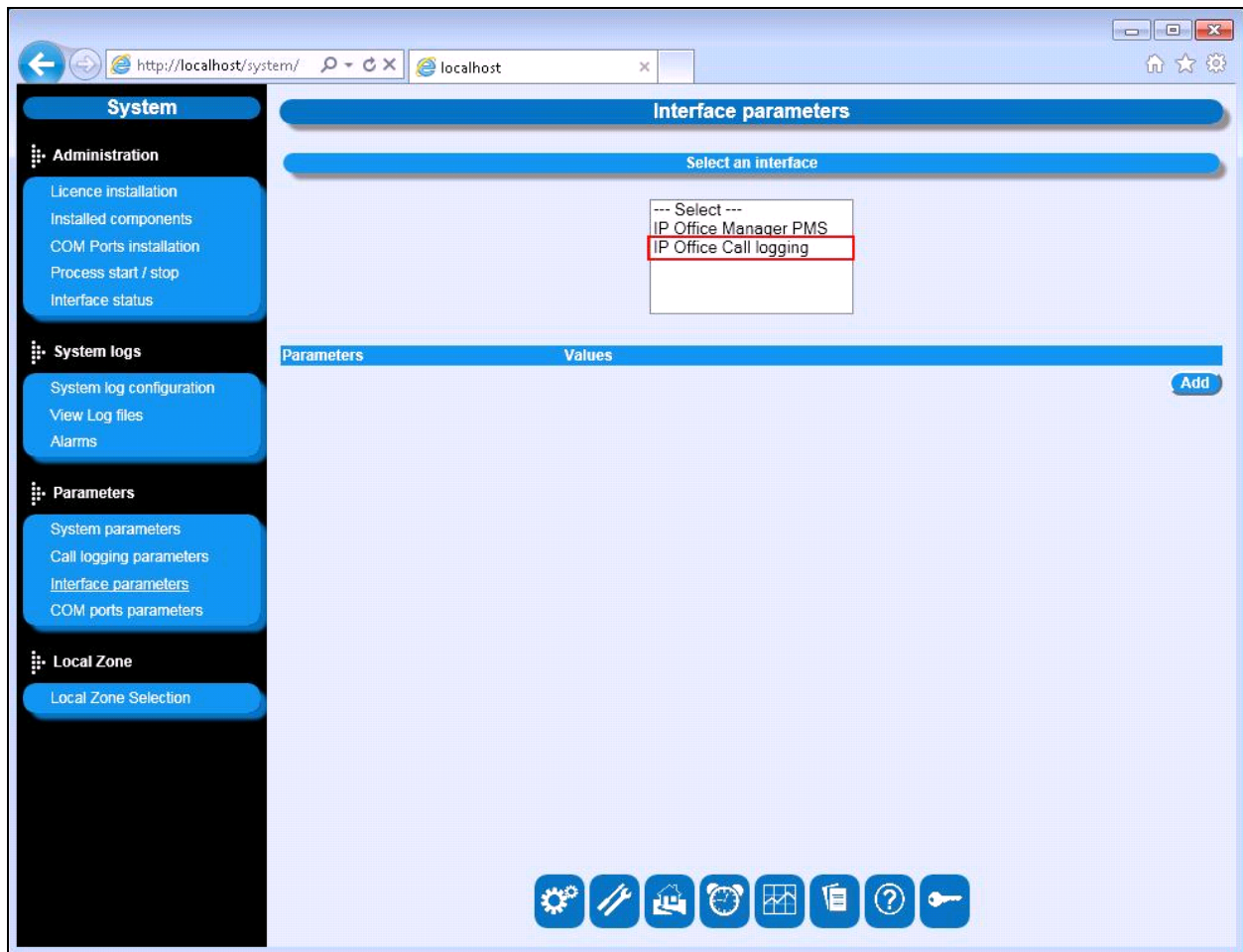
The screenshot shows the 'Interface parameters' section of the IP Office Manager PMS web interface. The browser address bar shows 'http://localhost/system/'. The left sidebar contains navigation links for 'System', 'Administration', 'System logs', 'Parameters', and 'Local Zone'. The main content area features a dropdown menu for 'Select an interface' with 'IP Office Manager PMS' selected. Below this is a table of parameters with 'Update' and 'Delete' buttons for each. The 'Add' button is located at the bottom right of the table.

Parameters	Values	Update	Delete
Configuration Web Service IP	127.0.0.1	Update	Delete
Configuration Web Service port	8085	Update	Delete
IP Office PBX IP	192.168.30.30	Update	Delete
IP Office PBX port	50805	Update	Delete
Login	Administrator	Update	Delete
Password	Administrator	Update	Delete
XML Configuration file path	c:/Meteor/backup/POCf9.xml	Update	Delete
DDI prefix	7	Update	Delete
DND user right	dnd	Update	Delete
Checkin user right	checkin	Update	Delete
Checkout user right	checkout	Update	Delete
Timeout	30000	Update	Delete

Add

6.2.2. Configure IP Office Manager PMS Parameters

On the **Select an interface** page select **IP Office Call logging**.



Once the **IP Office Call logging** Parameters page opens set the value for each parameter shown in the following table by selecting **Update** for each of the highlighted entries, one at a time. Enter the values indicated in the table. When these parameters have been configured, click **Add**.

Parameter	Usage
Port	Enter the SMDR port of the IP
Traffic analysis	Enter 1 to activate call logging after the first call

http://127.0.0.1/system/ 127.0.0.1

System

- Administration
 - Licence installation
 - Installed components
 - COM Ports installation
 - Process start / stop
 - Interface status
- System logs
 - System log configuration
 - View Log files
 - Alarms
- Parameters
 - System parameters
 - Call logging parameters
 - Interface parameters
 - COM ports parameters
- Local Zone
 - Local Zone Selection

Interface parameters

Select an interface

--- Select ---
IP Office Manager PMS
IP Office Call logging

Parameters	Values		
Port	5010	Update	Delete
PBX Id	1	Update	Delete
Traffic analysis	1	Update	Delete
SMDR call log	1	Update	Delete
Max. idle time	28800	Update	Delete

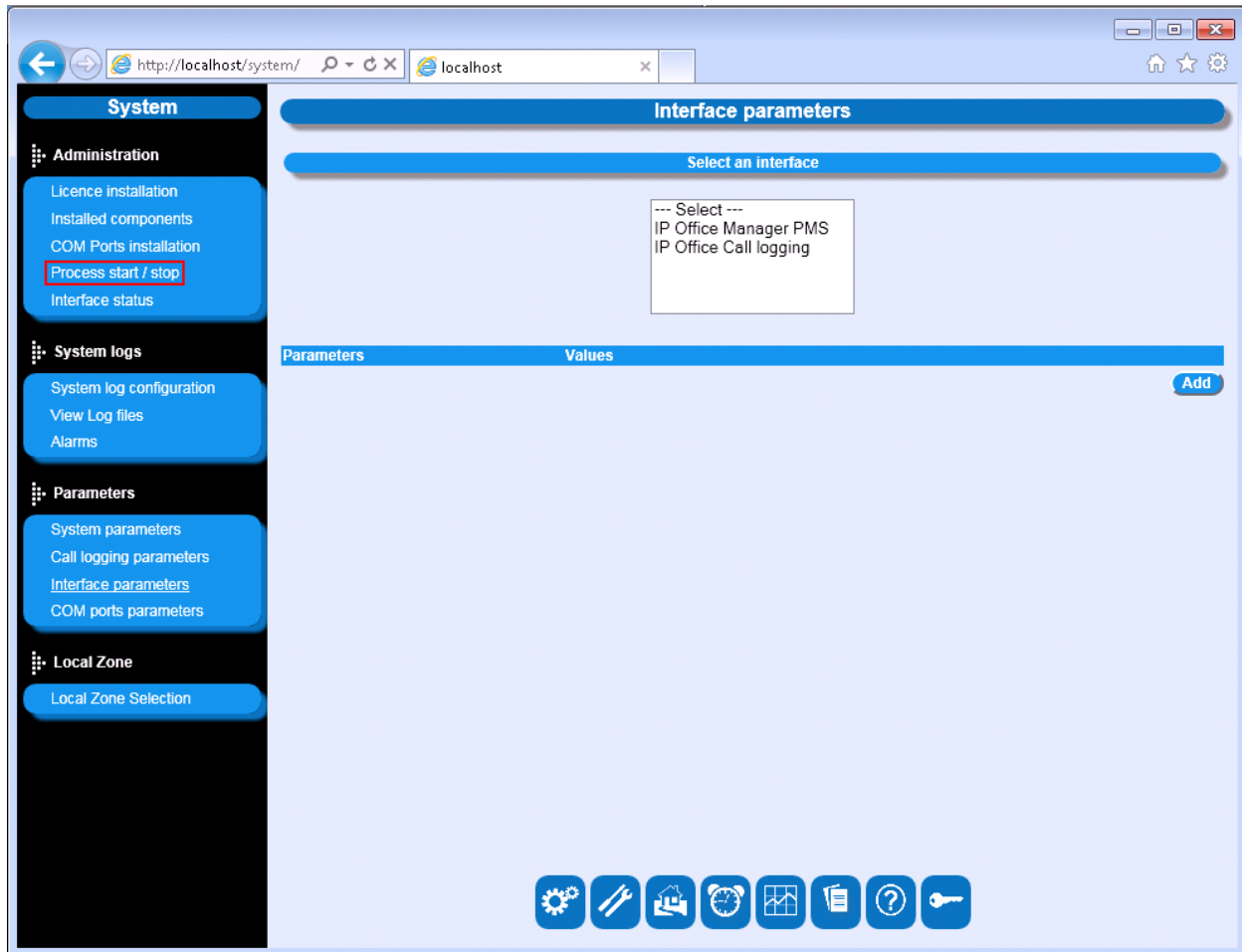
Add

21/11/2012 13:18 PMS link is lost

Settings, Tools, Home, Clock, Map, Document, Help, Key

6.3. Restart Meteor server

Once the interface Parameters are made the Meteor server must be restarted. Select **Process start / stop** from the left frame.



Once the **Process start / stop** page opens select the **Red** button highlighted to stop the system.

The screenshot shows a web browser window at <http://localhost/system/>. The page title is "Process start / stop".

System Status: METEOR is running
 Last start: 25/10/2012 13:25
 Last stop: 25/10/2012 13:21

Below the status, there are two buttons: a red button with a white grid icon (highlighted) and a green button with a white grid icon.

Processes List

Process Name	Description	Status	Control	Action
IF_IPOFFICE_RHM	IP Office Manager PMS	Running	Activated	Deactivate
IF_IPOFFICE_TAX	IP Office Call logging	Running	Activated	Deactivate
SW_IPOFFICE_RHM	Switch (Internal Process)	Running	Activated	Deactivate
SW_IPOFFICE_TAX	Switch (Internal Process)	Running	Activated	Deactivate
SW_PBXCMD	Pbx commands	Running	Activated	Deactivate
VM_MANAGER	Main voicemail process	Running	Activated	Deactivate
VM_V01	Channel 1	Running	Activated	Deactivate
VM_V02	Channel 2	Running	Activated	Deactivate
VM_V03	Channel 3	Running	Activated	Deactivate
VM_V04	Channel 4	Running	Activated	Deactivate

At the bottom right of the main content area, there is a "Refresh screen" button.

The sidebar on the left contains the following sections:

- System**
 - Administration
 - Licence installation
 - Installed components
 - COM Ports installation
 - Process start / stop
 - Interface status
 - System logs
 - System log configuration
 - View Log files
 - Alarms
 - Parameters
 - System parameters
 - Call logging parameters
 - Interface parameters
 - COM ports parameters
 - Local Zone
 - Local Zone Selection

At the bottom of the page, there is a row of icons: a gear, a wrench, a house, a clock, a calendar, a document, a question mark, and a key.

Once the system is stopped select the **Green** button highlighted to start the system.

The screenshot shows a web browser window at <http://localhost/system/>. The left sidebar contains navigation menus for System, System logs, Parameters, and Local Zone. The main content area is titled 'Process start / stop' and displays the status 'METEOR is stopped' with a red square icon and a green square icon. Below this, a 'Processes List' table is shown.

Process Name	Description	Status	Action	Deactivate
IF_IPOFFICE_RHM	IP Office Manager PMS	Not Running	Activated	Deactivate
IF_IPOFFICE_TAX	IP Office Call logging	Not Running	Activated	Deactivate
SW_IPOFFICE_RHM	Switch (Internal Process)	Not Running	Activated	Deactivate
SW_IPOFFICE_TAX	Switch (Internal Process)	Not Running	Activated	Deactivate
SW_PBXCMD	Pbx commands	Not Running	Activated	Deactivate
VM_MANAGER	Main voicemail process	Not Running	Activated	Deactivate
VM_V01	Channel 1	Not Running	Activated	Deactivate
VM_V02	Channel 2	Not Running	Activated	Deactivate
VM_V03	Channel 3	Not Running	Activated	Deactivate
VM_V04	Channel 4	Not Running	Activated	Deactivate

A 'Refresh screen' button is located at the bottom right of the table.

7. Verification Steps

Use the following steps to verify that Meteor and IP Office are each configured correctly.

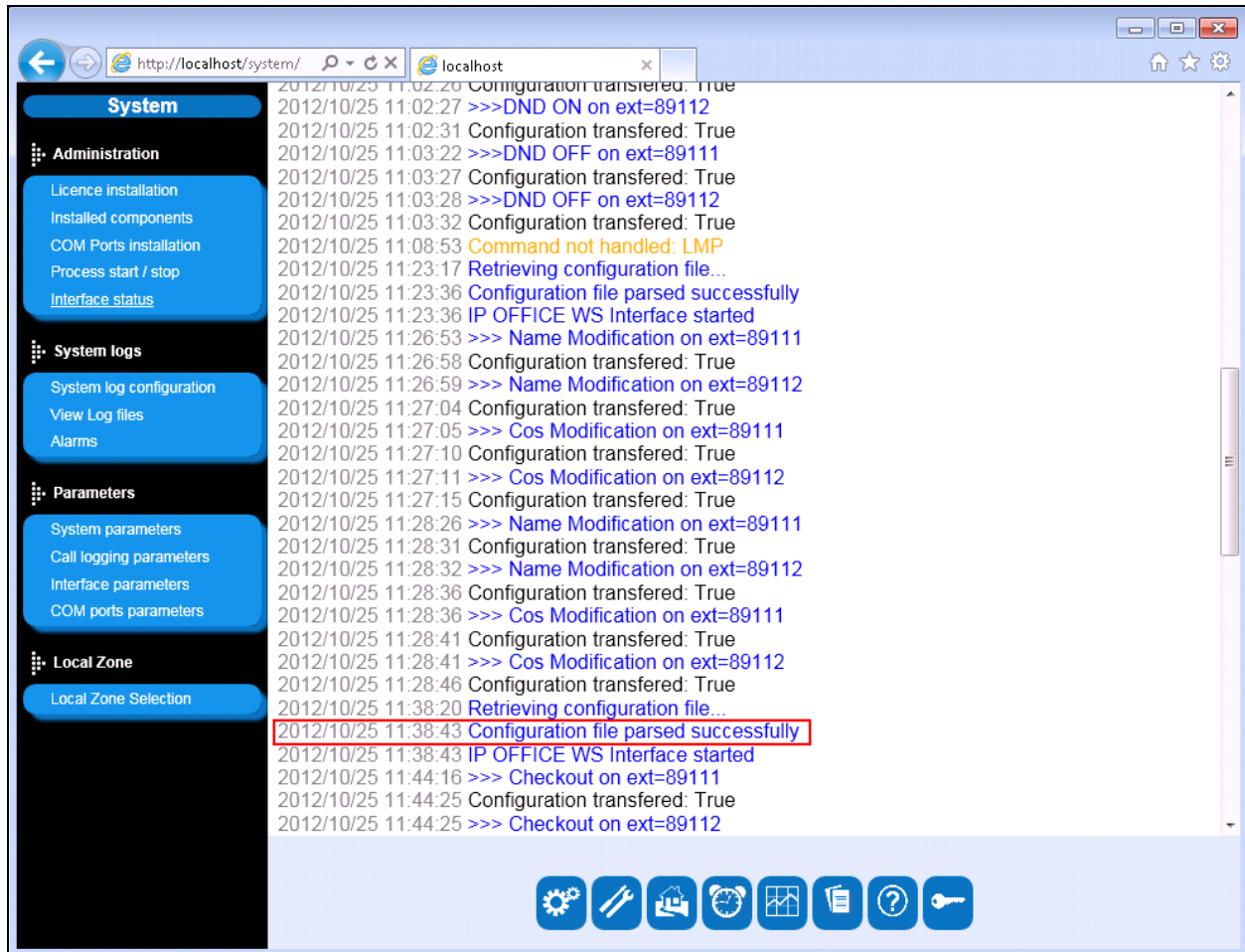
7.1. Verify Meteor Interface status

After making at least one outgoing call, verify that Meteor is running and the PMS and Call Logging controls are both green by logging into the Meteor Server and selecting **Interface status**.



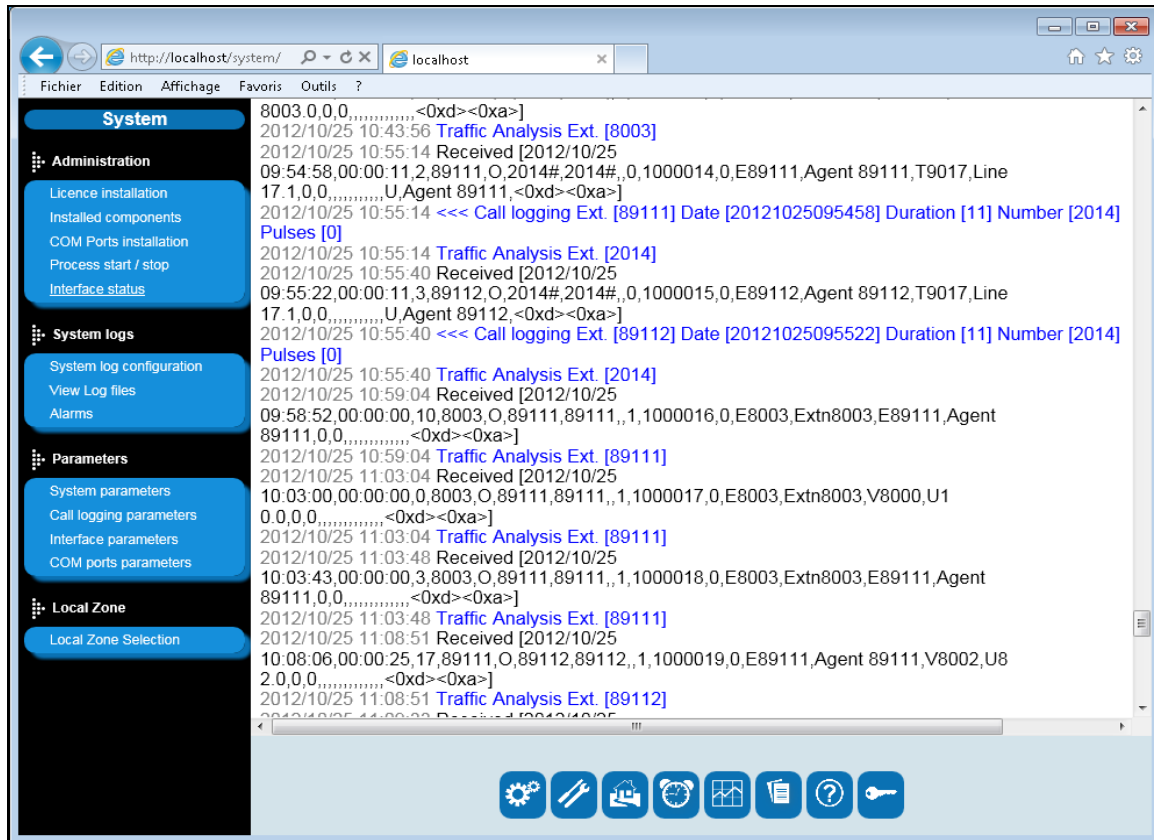
7.2. Verify Meteor IP Office Manager PMS

Click on the **IP Office Manager PMS** link shown in **Section 7.1** and verify that the message **Configuration file parsed successfully** is displayed, as shown in the following screen.



7.3. Verify Meteor Call logging retrieves Call Records

To ensure that Meteor is retrieving Call Records make some calls to and from the IP Office, click on the **IP Office Call Logging** link shown in **Section 7.1**. Verify that records relevant to the actual call activity are displayed.



8. Conclusion

A full and comprehensive set of feature functional test cases were performed during Compliance testing. Imagine Soft Meteor 5 is considered compliant with Avaya IP Office 8.1 All test cases have passed and met the objectives outlined in **Section 2.2**.

9. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from an Avaya representative.

[1] Avaya IP Office R8.1 Manager 10.1, August 3rd 2012, Issue 29o, Document Number 15-601011

The Meteor documentation is contained in the following directory after the product has been installed: C:\Meteor\tomcat\webapps\ROOT\help. This documentation is also available on the installation medium prior to installation.

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.