OfficeServ 7000 Series IP PBX

OfficeServ
V4.60 Product Update Guide

February, 2012

Samsung Electronics (UK) Ltd.

Contents

V4.60 Introduction

As you will see in the following New Feature Matrix and in the rest of this document, Samsung Electronics has greatly enhanced and strengthened the feature set, security and flexibility of the OfficeServ 7000 range of IP PBXs. Making the OfficeServ one of the most powerful, easily managed and secure IP PBXs in the market today.

The enhancements in V4.60 do not only deliver increased feature sets and flexibility, but also a solution that greatly reduces the cost of ownership and deployment.

There are more than 30 new features, sub-features or feature enhancements, plus four brand new hardware modules that V4.60 supports; including the new in-skin voice messaging solution the SVMi-20i. The SVMi-20i brings a unified management package, allowing for easier deployment and easy expansion using licence upgrades, which allows for single port upgrades without the need to visit site, therefore reducing your engineering costs and eliminating customer down time.

Other hardware changes include the addition of three new SLI/COMBO modules. These modules deliver cost benefits as they carry some of the secondary services that have previously been contained on separate daughter modules:

1. 8SLI3
2. 16SLI3
3. 8COMBO3

V4.60 New Feature Matrix

	Supported System				
New Feature / Hardware Change	**OS7030**	**OS7100**	**OS7200S**	**OS7200**	**OS7400**
SVMi-20i Voice Messaging Solution[1]	No	No	Yes	Yes	Yes
Multiple SIP Provider Support	Yes	Yes	Yes	Yes	Yes
Enhanced MGI Resource Management	Yes	Yes	Yes	Yes	Yes
VoIP Security Enhancement - TLS	No	No	No	Yes	Yes
VoIP Security Enhancement - sRTP	No	No	No	Yes	Yes
SIP Trunk General Usage Enhancements	Yes	Yes	Yes	Yes	Yes
Advanced Plug n Play – IP Phones	Yes	Yes	Yes	Yes	Yes
Embedded DHCP Server	Yes	Yes	Yes	No	No
Multi-Cast Paging – IP Phones	Yes	Yes	Yes	Yes	Yes
OfficeServ Connect Enhancements	Yes	Yes	Yes	Yes	Yes
NTP Server Support (Net Time Protocol)	Yes	Yes	Yes	Yes	Yes
CNF24 Module Enhancements	No	No	Yes	Yes	Yes
SIP Extension DTMF Support	Yes	Yes	Yes	Yes	Yes
DDI Max Call Per Ring Plan	Yes	Yes	Yes	Yes	Yes
Max Call in Queue Support	Yes	Yes	Yes	Yes	Yes
Alarm & Major Fault Email Support	Yes	Yes	Yes	Yes	Yes
Phonebook Download to IP Phones	Yes	Yes	Yes	Yes	Yes
WAV File format upload to SVMi-20i	Yes	Yes	Yes	Yes	Yes
Admin Management Tool – New DM Tool	Yes	Yes	Yes	Yes	Yes
NMS Full OS7000 Support (v1.6)	Yes	Yes	Yes	Yes	Yes
New SLI3 modules[2]	No	Yes	Yes	Yes	Yes

[1] The SVMi-20i is not available until the end of June, 2012.

[2] The new SLI3 modules are not available until the end of June, 2012

New Feature Section Layout

This section describes how each new feature or feature enhancement will be displayed in this document.

Each new feature chapter will have four key components, which are designed to inform you about, describe and aid configuration of each new feature.

The four chapter components are:

1. **General Description**
   a. This section will describe in general terms, the new feature’s benefits and use
2. **Installation**
   a. This section will show how to install the new feature or new hardware application where required
3. **Programming**
   a. This section will show any Device Manager programming requirements needed to enable the new application or feature
4. **End-user instructions**
   a. For any features that are end-user related, this section will describe any user functions and steps

New SVMi-20i Voice Messaging Solution

GENERAL DESCRIPTION

The new SVMi-20i solution brings all the features and functionality of the SVMi-20E but with a more integrated management solution. The SVMi-20i's admin and management interface is now combined with the new Device Manager Tool (DM), allowing for a single management interface for the OfficeServ PBX and the SVMi-20i.

Along with this new admin interface the port structure has been enhanced. Instead of installing hardware based daughter boards to increase the number of voicemail/faxmail/AA ports, the SVMi-20i allows for software based licensing port upgrades. Therefore removing the need to send an engineer to site to perform intrusive, and time consuming hardware installations.

The SVMi-20i also includes an IP interface, which removes the requirement for IP phones to use an MGI resource when connecting to the SVMi-20i.

Feature	Description
Channel Capacity	MAX 20ch (MAX 16ch with sRTP)
Interface	TDM and IP Interface
Message Storage	240 hours
FAX port	4
WEB Management	YES
CPU	Mindspeed M82318
OS	Linux
Main memory	DDR2, 256MB
Storage	SSD 8GB
Ethernet	1port, GbE
Format	G.711 (WAV format for uploading prompts)
EmailG/W encryption	SSL / TLS

New SVMi-20i Voice Messaging Solution

INSTALLATION

The physical size and slot positioning within the OfficeServ chassis has not changed with the development of the SVMi-20i. It should be treated in the same manner as the SVMi-20E in regards of slot and positioning.

The key physical difference from the SVMi-20E is that the SVMi-20i does not have any daughter board positions on the module as ports are added via a software license key.

New SVMi-20i Voice Messaging Solution

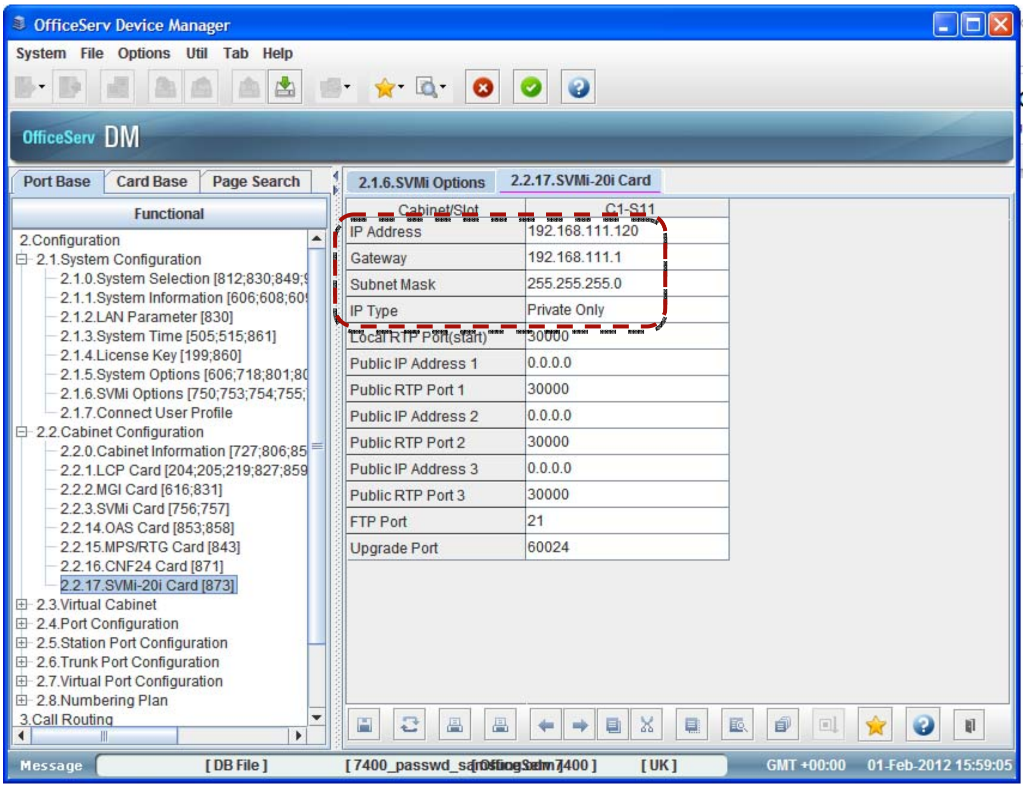
PROGRAMMING

The SVMi-20i delivers all of the same functionality and feature set as the SVMi-20E.

The main programming difference is the access method, which is now Web based access on the SVMi-20i as opposed to Telnet on the SVMi-20E.

The menu structure and layout is much in line with the SVMi-20E.

Admin and programming access to the SVMi-20i is now via the new DM Tool (Device Manager), which is a centralised main system and VM/AA management tool.


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
2.1.System Configuration
2.1.0.System Selection [812;830;849;
2.1.1.System Information [606;608;60
2.1.2.LAN Parameter [830]
2.1.3.System Time [505;515;861]
2.1.4.License Key [199;860]
2.1.5.System Options [606;718;801;80
2.1.6.SVMi Options [750;753;754;755;
2.1.7.Connect User Profile
2.2.Cabinet Configuration
2.2.0.Cabinet Information [727;806;85
2.2.1.LCP Card [204;205;219;827;859
2.2.2.MGI Card [616;831]
2.2.3.SVMi Card [756;757]
2.2.14.OAS Card [853;858]
2.2.15.MPS/RTG Card [843]
2.2.16.CNF24 Card [871]
2.2.17.SVMi-20i Card [873]
2.3.Virtual Cabinet
2.4.Port Configuration
2.5.Station Port Configuration
2.6.Trunk Port Configuration
2.7.Virtual Port Configuration
2.8.Numbering Plan
3.Call Routing
2.1.6.SVMi Options
2.2.17.SVMi-20i Card
Message
[DB File]
[7400_passwd_sa[OfficeServ 7400]
[UK]
GMT +00:00
01-Feb-2012 15:59:05

Cabinet/Slot	C1-S11
IP Address	192.168.111.120
Gateway	192.168.111.1
Subnet Mask	255.255.255.0
IP Type	Private Only
Local RTP Port(start)	30000
Public IP Address 1	0.0.0.0
Public RTP Port 1	30000
Public IP Address 2	0.0.0.0
Public RTP Port 2	30000
Public IP Address 3	0.0.0.0
Public RTP Port 3	30000
FTP Port	21
Upgrade Port	60024

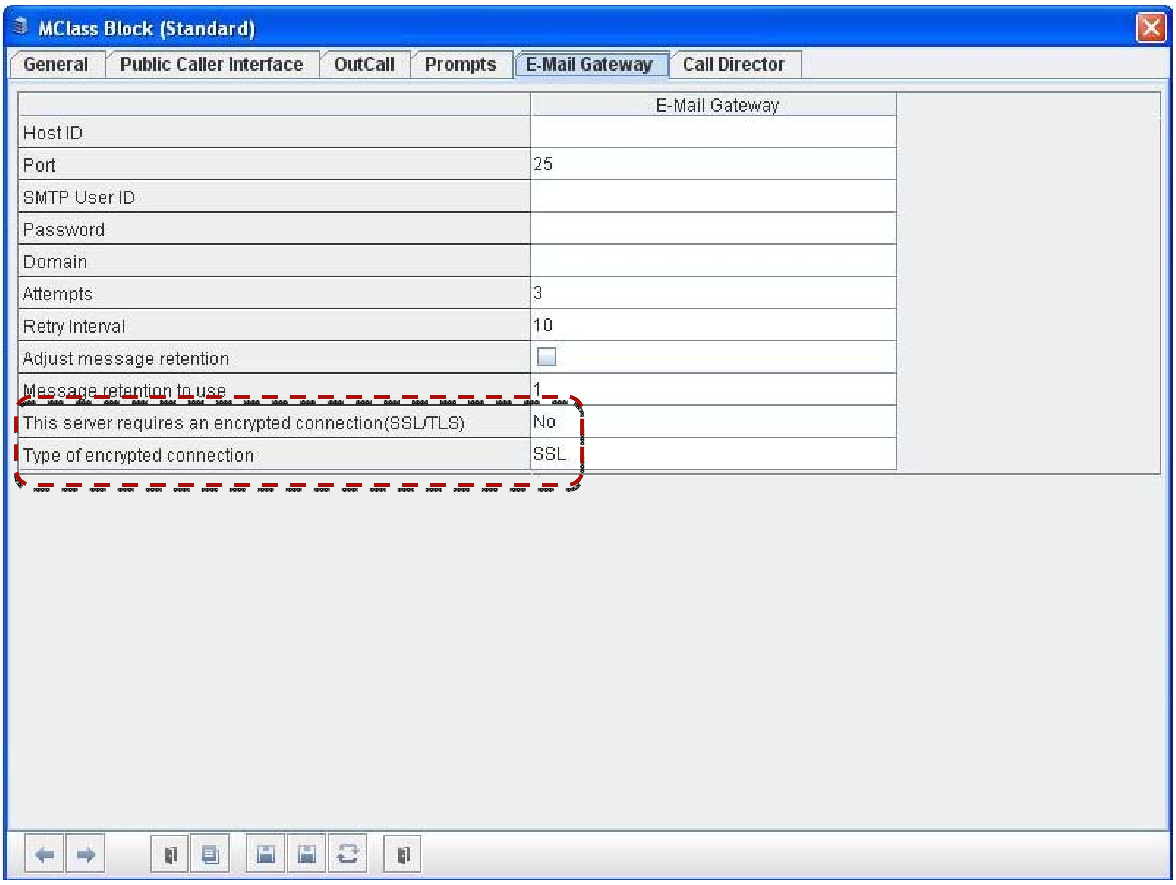
The SVMi-20i should be assigned an IP address via **DM Menu 2.1.6**

The SVMi-20i has been enhanced to include both SSL and TLS encryption for secured communications between the Email Gateway application and the local/remote mail server(s). With the growing amount of threats to business data security, VoIP communications are exposed to data security threats such as hacking and network virus attacks. To minimiseor eliminate the risk, both SSL (secure socket layer) and TLS (transport layer security) options have been added to the OfficeServ SVMi-20i.

Using DM, access the VM/AA function and go to menu 8.1.12, and build the MClass block. Then go to the E-mail Gateway tab and create mail server table with the Host ID, Port, User ID, and Domain, enable encryption, and set the encryption type.

FIELD	PURPOSE
This server requires an encrypted connection (SSL/TLS)	Set this option if the mail server requires encrypted connection (SSL/TLS). This option should be set to yes.
Type of encrypted connection	SSL: SVM first send “STARTTLS” command to the mail server before it begins encrypted connection. TLS: SVM starts encrypted connection with the mail server directly.

In **DM menu 8.1.12** enter the required encryption for each Mclass Block and set encrypted to **YES**



	E-Mail Gateway
Host ID	
Port	25
SMTP User ID	
Password	
Domain	
Attempts	3
Retry Interval	10
Adjust message retention	□
Message retention to use	1
This server requires an encrypted connection(SSL/TLS)	No
Type of encrypted connection	SSL

Multiple SIP Service Provider Support

GENERAL DESCRIPTION

As SIP trunks have become more advanced in their delivery and stability, more and more customers are using SIP as either a direct replacement for, or supplimentary service to traditional analogue and ISDN services.

OfficeServ V4.60 delivers the ability to register to, and simultaneously use up to four SIP providers on one OfficeServ system.

The system can then be programmed to route outbound calls via each SIP provider based on the usual auto route selection criteria per call – traditionally based on cost, distance or end user extension number account details.

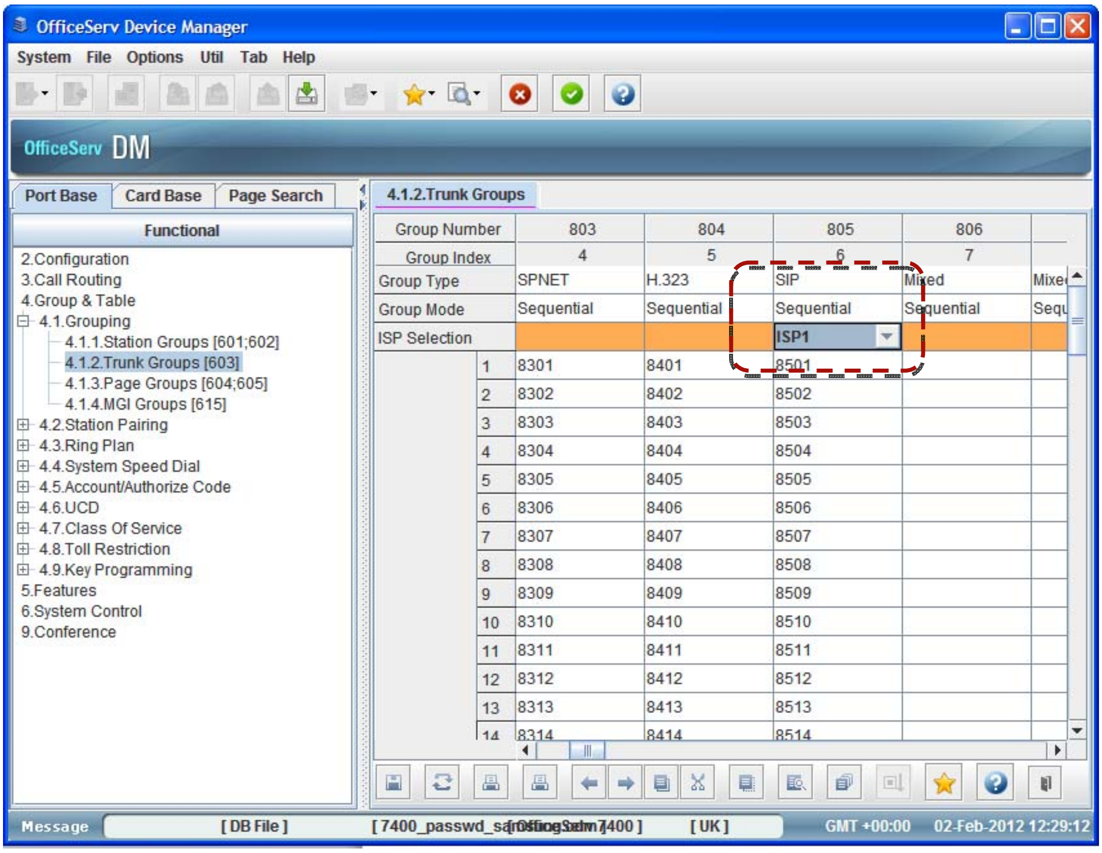
The system can even be programmed to use alternative SIP providers as fail-over or backup routes for other providers whether they are ISDN, analogue or SIP.

Multiple SIP Service Provider Support

PROGRAMMING

Two Menus have been enhanced to enable the programming of Multiple SIP providers.

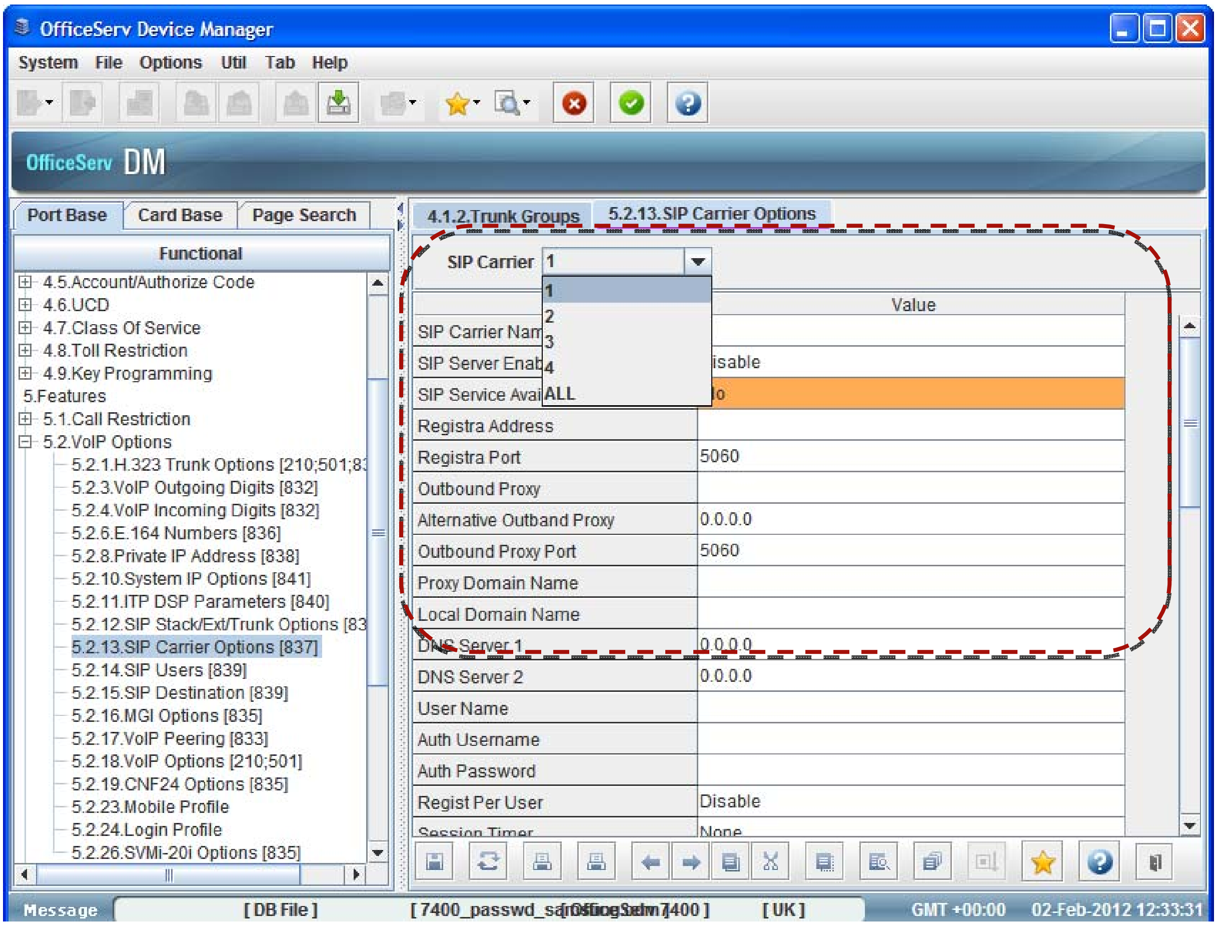
- Firstly, **DM Menu 4.1.2 Trunk Groups**



Group Number		803	804	805	806	
Group Index		4	5	6	7	
Group Type		SPNET	H.323	SIP	Mixed	Mixe
Group Mode		Sequential	Sequential	Sequential	Sequential	Sequ
ISP Selection				ISP1		
	1	8301	8401	8501		
	2	8302	8402	8502		
	3	8303	8403	8503		
	4	8304	8404	8504		
	5	8305	8405	8505		
	6	8306	8406	8506		
	7	8307	8407	8507		
	8	8308	8408	8508		
	9	8309	8409	8509		
	10	8310	8410	8510		
	11	8311	8411	8511		
	12	8312	8412	8512		
	13	8313	8413	8513		
	14	8314	8414	8514		

Where a particular trunk group is assigned as **SIP**, the relative **ISP** or SIP provider should be selected (or SIP peering).

- Secondly, **DM Menu 5.2.13 SIP Carrier Options**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base Card Base Page Search
Functional
4.5.Account/Authorize Code
4.6.UCD
4.7.Class Of Service
4.8.Toll Restriction
4.9.Key Programming
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;83
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.26.SVMi-20i Options [835]
4.1.2.Trunk Groups
5.2.13.SIP Carrier Options
1
2
3
4
ALL
Message

SIP Carrier 1

	Value
SIP Carrier Nam	
SIP Server Enab	isable
SIP Service Avai	lo
Registra Address	
Registra Port	5060
Outbound Proxy	
Alternative Outband Proxy	0.0.0.0
Outbound Proxy Port	5060
Proxy Domain Name	
Local Domain Name	
DNS Server 1	0.0.0.0
DNS Server 2	0.0.0.0
User Name	
Auth Username	
Auth Password	
Regist Per User	Disable
Session Timer	None

[DB File] [7400_passwd_sa[OfficeServ 7400] [UK] GMT +00:00 02-Feb-2012 12:33:31

This menu is used to set up each SIP provider's (ISP) SIP trunk services, including ISP details and account information.

Enhanced MGI Resource Management

GENERAL DESCRIPTION

When the OfficeServ 7000 IP PBX series was launched, any VoIP media was controlled by the MGI (Media Gateway Interface) module and its associated channels. The MGI allows for IP devices to communicate to non-IP devices, such as TMD trunks or handsets.

V4.40 OfficeServ software delivered a new service called MPS (Media Proxy Server), which allowed IP devices to talk to IP devices without the need for an MGI channel to be used. MGI resources are always used toconnect IP to non-IP devices.

An MGI resource was also required to supply RINGBACK Tone even during IP to IP communications. MGI channels were also required to deliver music-on-hold during an IP to IP call.

Version 4.60 changes this MGI allocation by allowing specialized MPS channels called Ring Tone Generation (RTG) channels to provide ringback tone, hold tone, and music on hold. This eliminates the need to overstock MGI channels and in many situations can reduce system cost by reducing the number of OAS or MGI64 cards or MGI licenses needed. There is 1 RTG channel in the system for every (1 or 2 MPS channels).

⚠

1. The OfficeServ 7200 and 7400 require OAS cards in order to provide MPS channel resources

2. RTG channels are only available when the MPS Service is enabled in the system

3. You need to make sure that any RTG ports are allowed through any Firewall

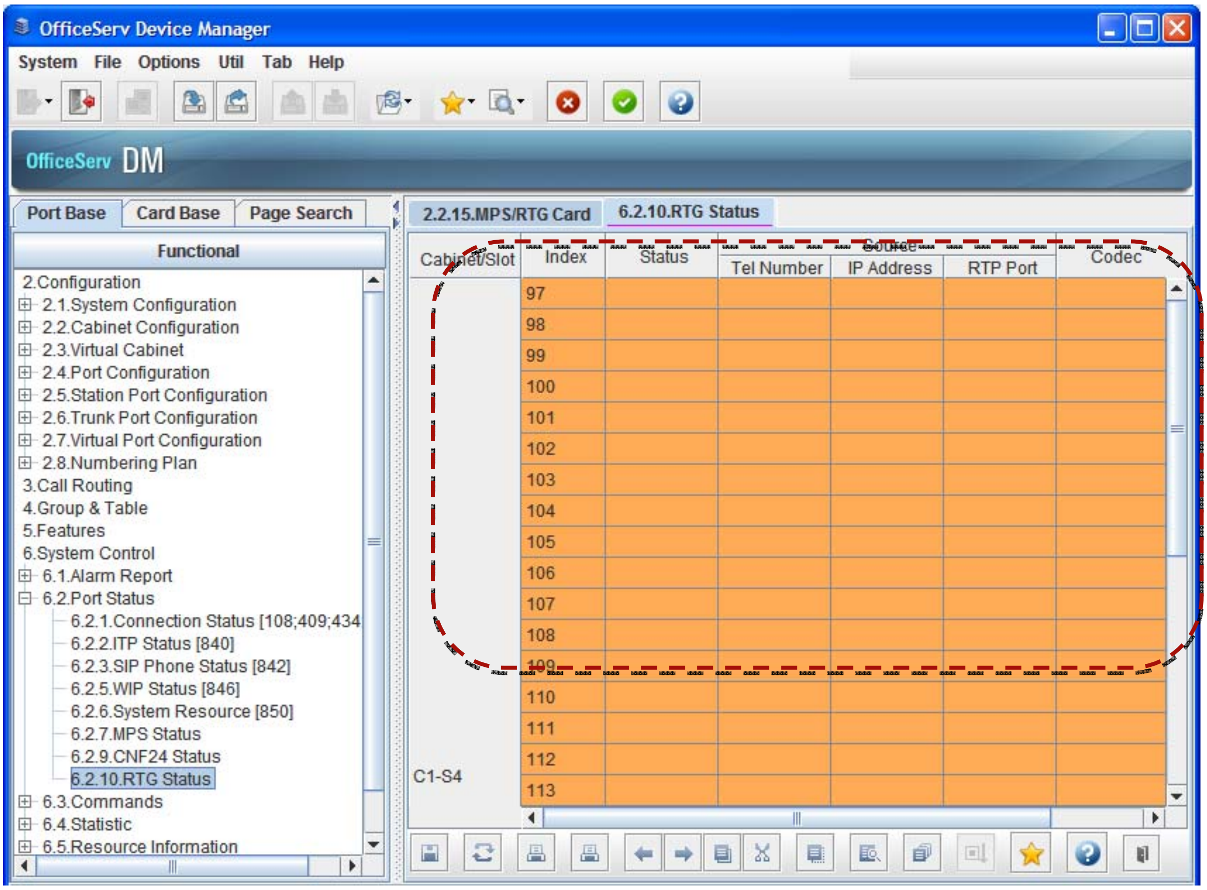
4. One RTG call is equivalent to 1 MPS call (or 2 MPS channels). If a system has 8 MPS calls (or 16 MPS channels) capacity and 1 RTG is in use, there will be 7 MPS calls (or 7 RTG) available for use.

Enhanced MGI Resource Management

PROGRAMMING

One DM Menu has been added and one has been modified to facilitate this new model of MGI resource management structure.

- NEW DM **Menu 6.2.10 RTG Status**

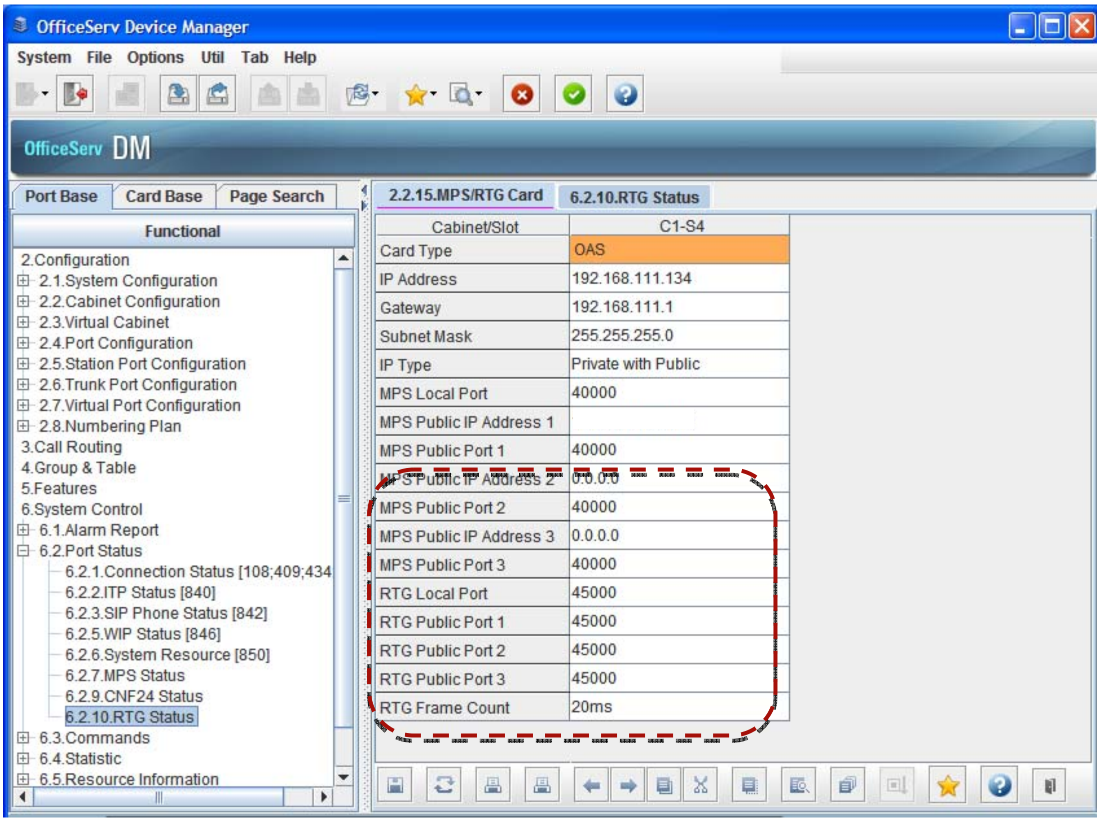


Cabinet/Slot	Index	Status	Source			Codec
			Tel Number	IP Address	RTP Port	
C1-S4	97					
	98					
	99					
	100					
	101					
	102					
	103					
	104					
	105					
	106					
	107					
	108					
	109					
	110					
	111					
	112					
	113					

Here you will see any activity on the MPS channels relating to the RTG port usage.

NEW FIELD	PURPOSE
RTG Local Port	Sets the starting port the RTG channels will listen on for local network traffic. The ending port will be (RTG Local Port) + (number of RTG Calls). The default port is **45000**. ***For example, a starting port of 45000 with 16 RTG calls yields an end port of 45015.***
RTG Public Port 1 ~ 3	Sets the starting port the RTG channels will listen on for public internet traffic. The default port is **45000**. ***This setting is only for use in NAT environments***
RTG Frame Count	Sets the codec latency for RTG channels. ***The default setting of 20ms normally doesn't need to be changed***

- Modified DM **Menu 2.2.15 MPS/RTG Card**



Cabinet/Slot	C1-S4
Card Type	OAS
IP Address	192.168.111.134
Gateway	192.168.111.1
Subnet Mask	255.255.255.0
IP Type	Private with Public
MPS Local Port	40000
MPS Public IP Address 1	
MPS Public Port 1	40000
MPS Public IP Address 2	0.0.0.0
MPS Public Port 2	40000
MPS Public IP Address 3	0.0.0.0
MPS Public Port 3	40000
RTG Local Port	45000
RTG Public Port 1	45000
RTG Public Port 2	45000
RTG Public Port 3	45000
RTG Frame Count	20ms

NEW FIELD	PURPOSE
RTG Local Port	Sets the starting port the RTG channels will listen on for local network traffic. The ending port will be (RTG Local Port) + (number of RTG Calls). The default port is **45000**. ***For example, a starting port of 45000 with 16 RTG calls will result in an end port of 45015.***
RTG Public Port 1 ~ 3	Sets the starting port the RTG channels will listen on for public internet traffic. The default port is **45000**. ***This setting is only for use in NAT environments***
RTG Frame Count	Sets the codec latency for RTG channels. ***The default setting of 20ms normally doesn't need to be changed***

Enhanced VoIP Security – TLS/sRTP

GENERAL DESCRIPTION

As VoIP telephony becomes more and more accepted in the business sector as an alternative to TDM trunks, so the requirements to keep these VoIP communications secure becomes even greater.

By the very nature of VoIP it puts a company's voice telephony onto well know data networks and largely uses the same protocols to deliver the telephony services. This leads to the possibility of opening it up to being at threat from a hacker or network attacks, which are common in the data network world.

V4.60 OfficeServ delivers SIP trunks and SIP extensions that are connected to the OS7200 and S7400 to be secured by a data network industry - standard protocol called TLS. Transport Layer Security is a cryptography standard developed to secure company data networks from attacks.

Note: When TLS is in use, the MP requires more resources to handle the additional load.

- For SIP trunking and SIP peering, the impact is **1:3.5**. That means one TLS connection will use 3.5 SIP channels. For example, if 4 TLS connection are required, you will need to license for 14 (= 4 x 3.5) SIP channels. Each SIP account can be set to TLS individually.

- For 3rd party SIP extensions, the impact is **1:3**. That means one TLS connection will use the equivalent of 3 SIP extns. For example, if 4 TLS connection are required for 3rd party SIP extensions, you will need to license for 12 (= 4 x 3) 3rd party SIP extensions.

Encrypting a data channel with TLS goes a long way toward securing a VoIP communications.
But the media i.e. the speech is still in an open readable format.

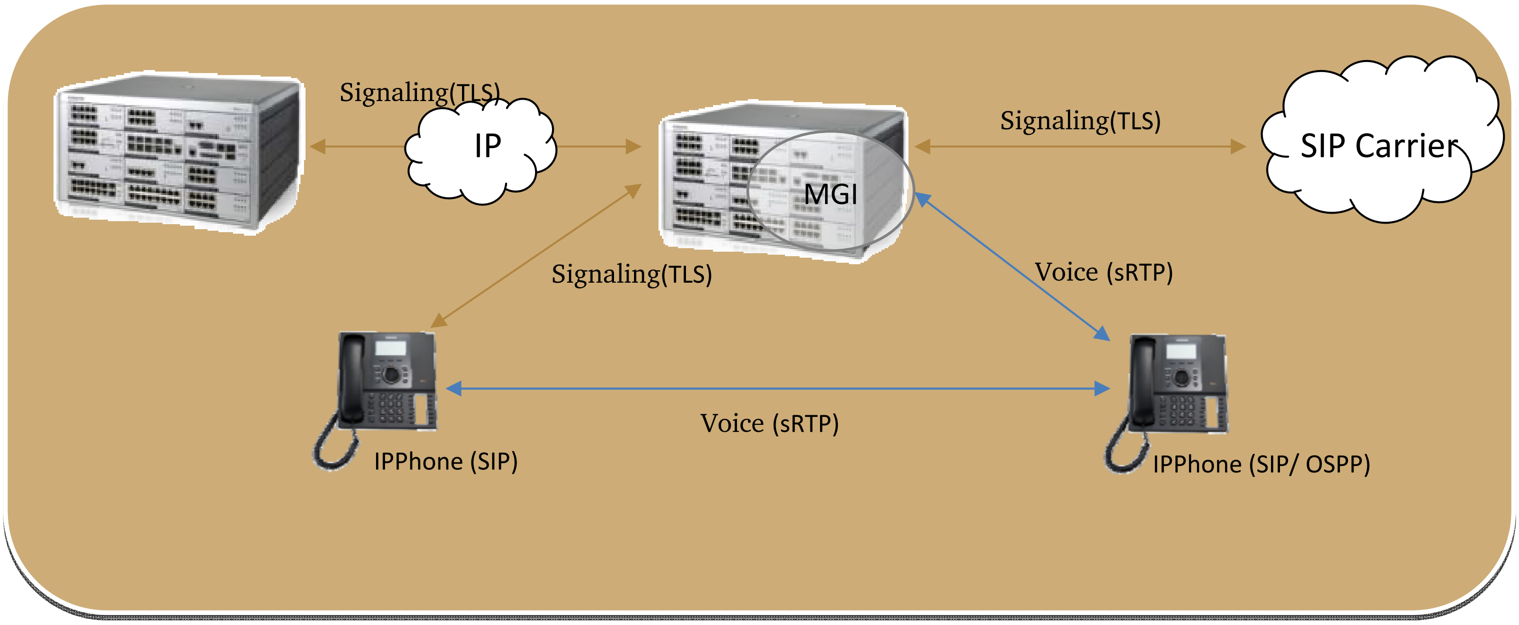
Version 4.60 delivers support for Secure RTP (sRTP) audio streams. sRTPis an encryption protocol developed specifically for VoIP audio streams and prevents hackers from reconstructing audio even where the hacker has gained access to the network and captured the speech packets.

- Version 4.60 allows sRTP to be enabled for any or all of the following:
- MGIs (including MGI64 cardsOAS cards, and embedded MGI channels)
- SMT-i Series IP Phones
- SPNet channels
- SMT-W5120E WiFi handsets.

⚠

When sRTP is in use, the MP requires more resources to handle the additional load. The overall MGI channel capacity is reduced. sRTP is a system wide selection. Once set, all MGI channels are set. That means all OAS cards in the system will use the sRTP setting.
Example capacity table can be seen here:

Module Type	VoIP using (RTP)	VoIP using (sRTP)
OAS Module - MPS/RTG (no impact)	32	32
MGI16	16	10
MGI 64	64	40

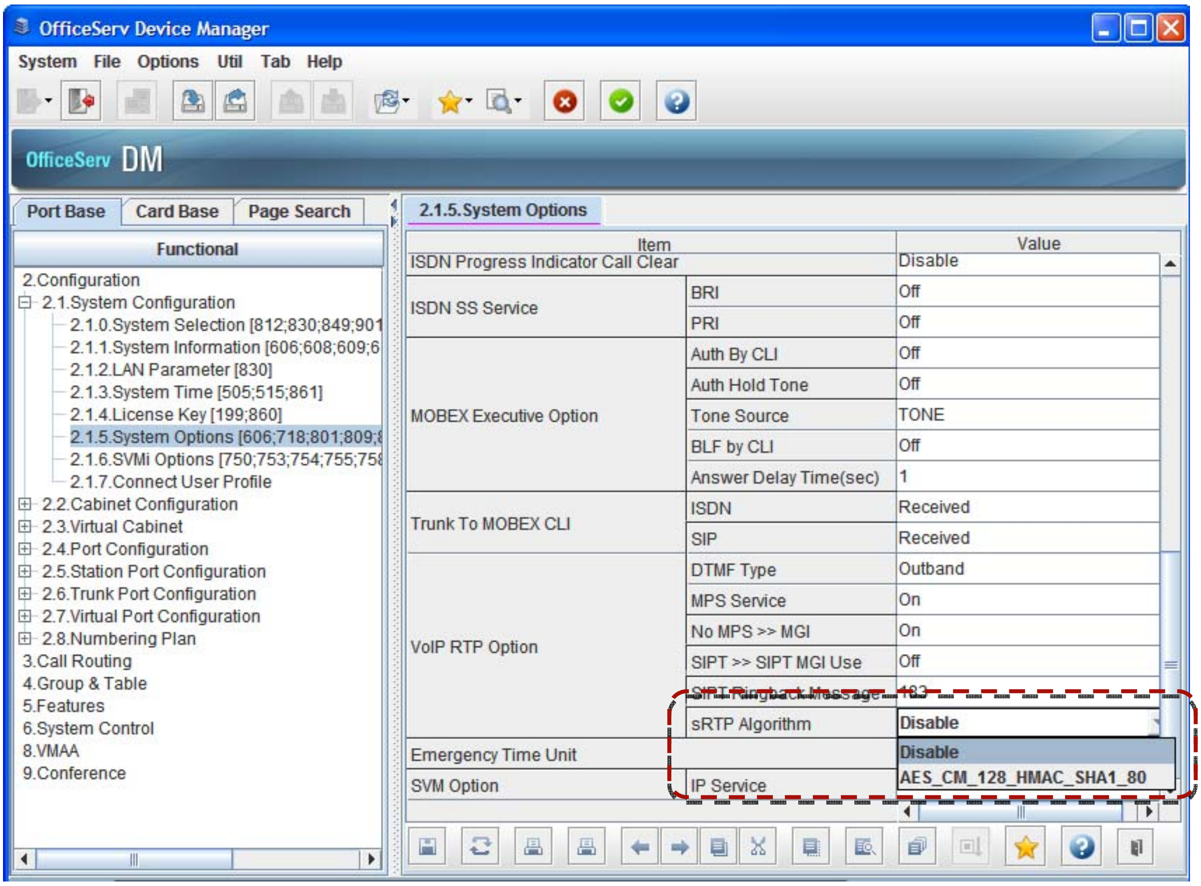


Enhanced VoIP Security – TLS/sRTP

PROGRAMMING

Five DM Menus have been modified and one has been added to support sRTP.

- DM **Menu 2.1.5 System Options**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base Card Base Page Search
Functional
2.1.5.System Options

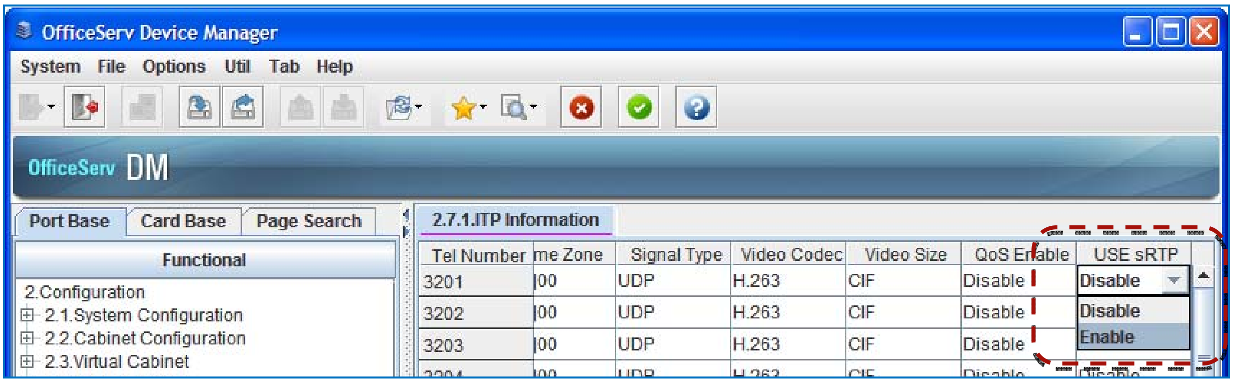
- 2.Configuration
  - 2.1.System Configuration
    - 2.1.0.System Selection [812;830;849;901
    - 2.1.1.System Information [606;608;609;6
    - 2.1.2.LAN Parameter [830]
    - 2.1.3.System Time [505;515;861]
    - 2.1.4.License Key [199;860]
    - 2.1.5.System Options [606;718;801;809;8
    - 2.1.6.SVMi Options [750;753;754;755;758
    - 2.1.7.Connect User Profile
  - 2.2.Cabinet Configuration
  - 2.3.Virtual Cabinet
  - 2.4.Port Configuration
  - 2.5.Station Port Configuration
  - 2.6.Trunk Port Configuration
  - 2.7.Virtual Port Configuration
  - 2.8.Numbering Plan
- 3.Call Routing
- 4.Group & Table
- 5.Features
- 6.System Control
- 8.VMAA
- 9.Conference

Item		Value
ISDN Progress Indicator Call Clear		Disable
ISDN SS Service	BRI	Off
	PRI	Off
MOBEX Executive Option	Auth By CLI	Off
	Auth Hold Tone	Off
	Tone Source	TONE
	BLF by CLI	Off
	Answer Delay Time(sec)	1
Trunk To MOBEX CLI	ISDN	Received
	SIP	Received
VoIP RTP Option	DTMF Type	Outband
	MPS Service	On
	No MPS >> MGI	On
	SIPT >> SIPT MGI Use	Off
	SIPT Ringback Message	183
	sRTP Algorithm	Disable
Emergency Time Unit		
SVM Option	IP Service	

sRTP Algorithm options: Disable, AES_CM_128_HMAC_SHA1_80

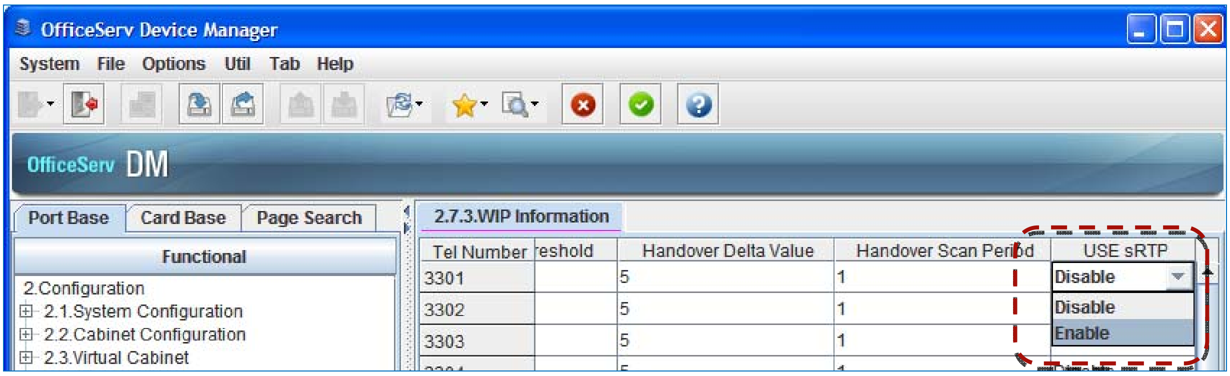
Here you can enable or disable sRTP system wide using AES encryption.

- DM **Menu 2.7.1 ITP Information -** Here you can enable or disable sRTP per IP device.



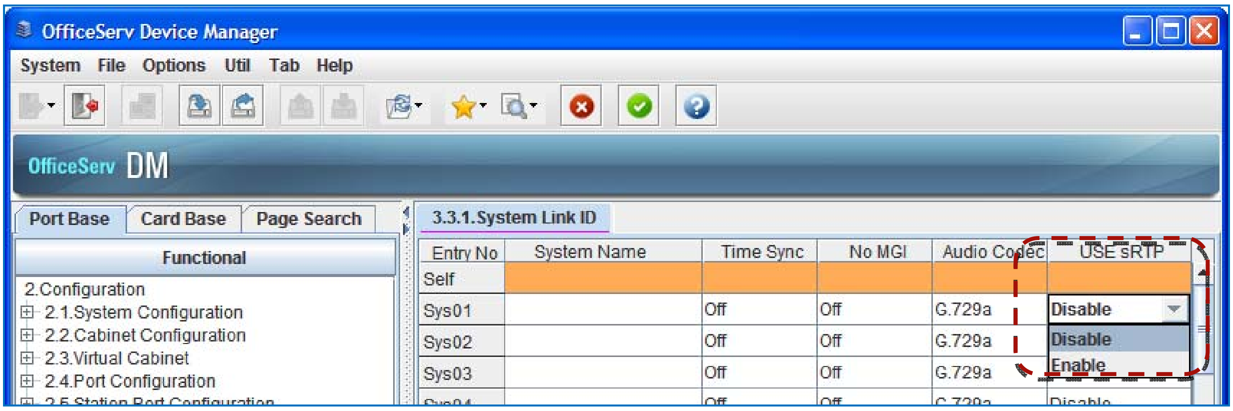
Tel Number	me Zone	Signal Type	Video Codec	Video Size	QoS Enable	USE sRTP
3201	00	UDP	H.263	CIF	Disable	Disable
3202	00	UDP	H.263	CIF	Disable	
3203	00	UDP	H.263	CIF	Disable	

- DM **Menu 2.7.3 WIP Phone Information -** Here you can enable or disable sRTP per Wi-Fi handset.



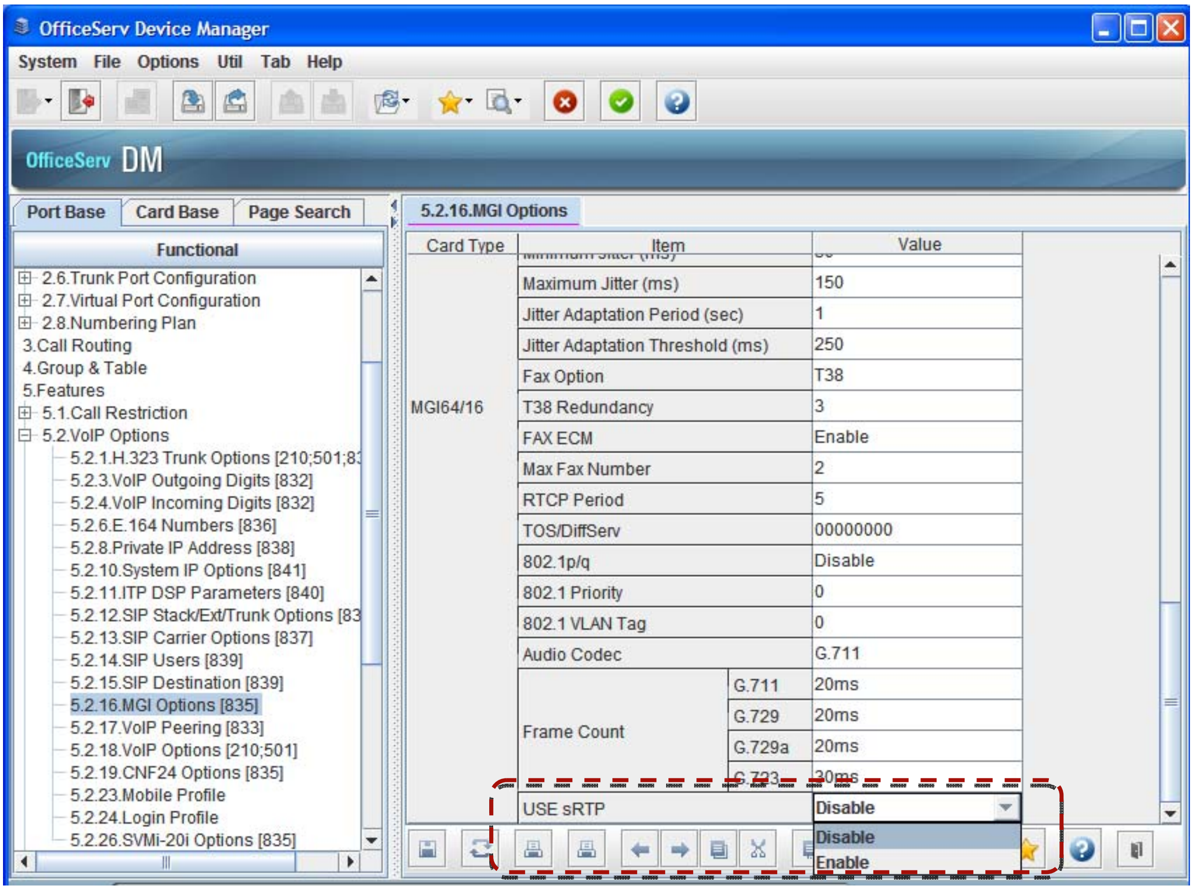
Tel Number	reshold	Handover Delta Value	Handover Scan Period	USE sRTP
3301		5	1	Disable
3302		5	1	
3303		5	1	

- DM **Menu 3.3.1 System Link ID -** Here you can enable or disable sRTP per SPNet site connection.



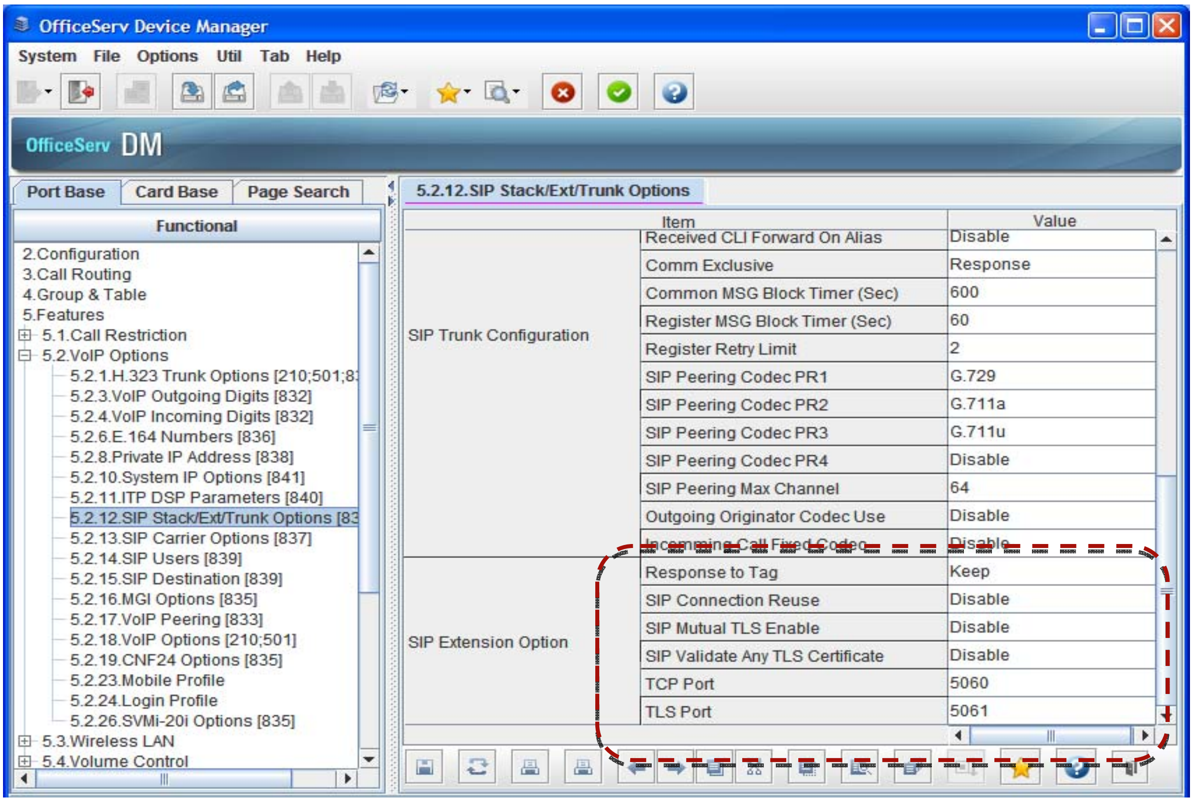
Entry No	System Name	Time Sync	No MGI	Audio Codec	USE sRTP
Self					
Sys01		Off	Off	G.729a	Disable
Sys02		Off	Off	G.729a	
Sys03		Off	Off	G.729a	

- DM **Menu 5.2.16 MGI Options –** Here you can enable or disable sRTP per MGI or OAS or licensed ports on OS7030, OS7100 and OS7200s.


OfficeServ Device Manager
System
File
Options
Util
Tab
Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.6.Trunk Port Configuration
2.7.Virtual Port Configuration
2.8.Numbering Plan
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;83
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.26.SVMi-20i Options [835]
5.2.16.MGI Options

Card Type	Item		Value
MGI64/16	Maximum Jitter (ms)		150
	Jitter Adaptation Period (sec)		1
	Jitter Adaptation Threshold (ms)		250
	Fax Option		T38
	T38 Redundancy		3
	FAX ECM		Enable
	Max Fax Number		2
	RTCP Period		5
	TOS/DiffServ		00000000
	802.1p/q		Disable
	802.1 Priority		0
	802.1 VLAN Tag		0
	Audio Codec		G.711
	Frame Count	G.711	20ms
		G.729	20ms
		G.729a	20ms
		G.723	30ms
	USE sRTP		Disable

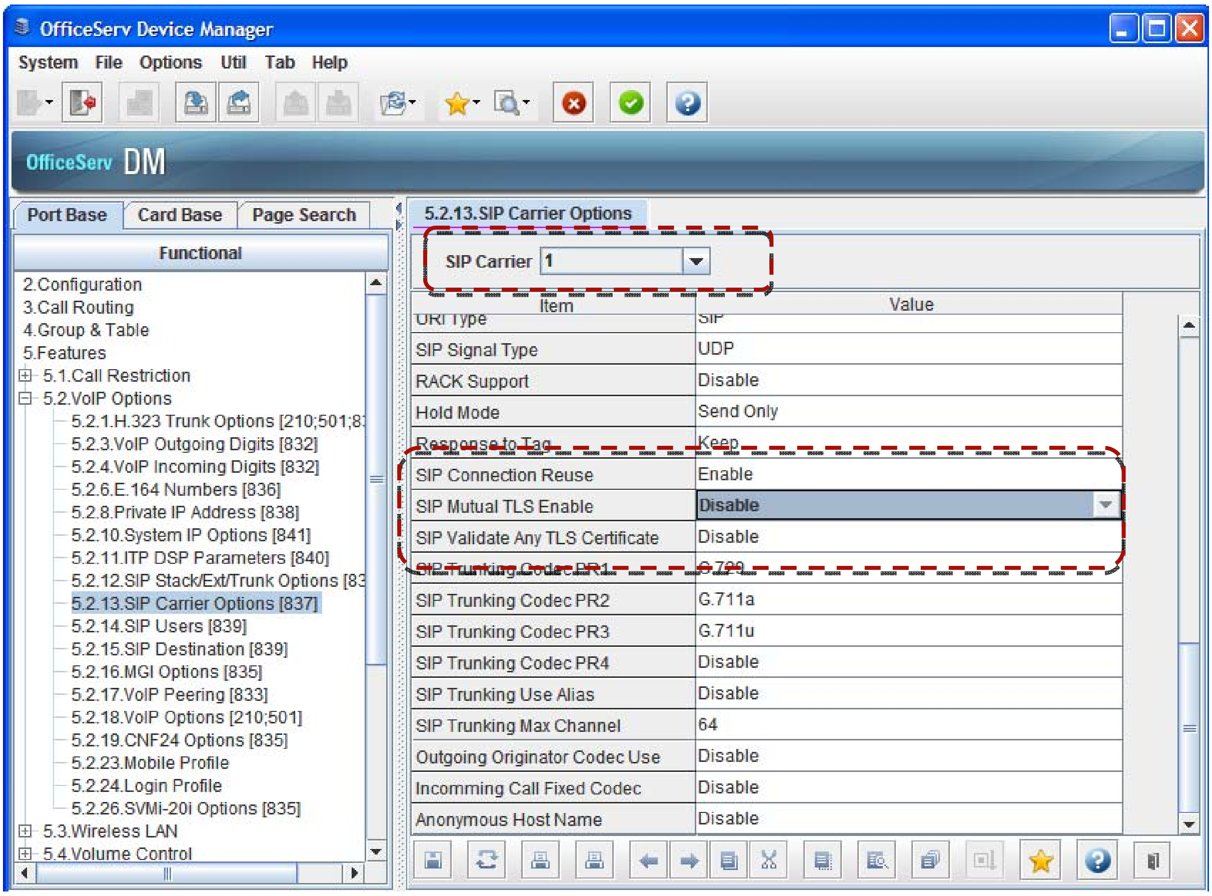
- DM **Menu 5.2.12 SIP Stack/Ext/Trunk Options**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.26.SVMi-20i Options [835]
5.3.Wireless LAN
5.4.Volume Control
5.2.12.SIP Stack/Ext/Trunk Options

	Item	Value
SIP Trunk Configuration	Received CLI Forward On Alias	Disable
	Comm Exclusive	Response
	Common MSG Block Timer (Sec)	600
	Register MSG Block Timer (Sec)	60
	Register Retry Limit	2
	SIP Peering Codec PR1	G.729
	SIP Peering Codec PR2	G.711a
	SIP Peering Codec PR3	G.711u
	SIP Peering Codec PR4	Disable
	SIP Peering Max Channel	64
	Outgoing Originator Codec Use	Disable
	Incomming Call Fixed Codec	Disable
SIP Extension Option	Response to Tag	Keep
	SIP Connection Reuse	Disable
	SIP Mutual TLS Enable	Disable
	SIP Validate Any TLS Certificate	Disable
	TCP Port	5060
	TLS Port	5061

FIELD	PURPOSE
SIP Connection Reuse	Sets whether or not TLS certification must happen on every call or only once during registration
SIP Mutual TLS Enable	Sets whether or not to use TLS encryption for SIP stations
SIP Validate Any TLS Certificate	Sets whether the system will reject (Disable) or accept (enable) unknown certificates during the TLS handshake
TLS Port	Sets the TCP port the TLS engine will listen for connections on. The default value is 5061

- DM **Menu 5.2.13 SIP Carrier Options**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
5.2.13.SIP Carrier Options

2.Configuration
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.26.SVMi-20i Options [835]
5.3.Wireless LAN
5.4.Volume Control

SIP Carrier: 1

Item	Value
URI Type	SIP
SIP Signal Type	UDP
RACK Support	Disable
Hold Mode	Send Only
Response to Tag	Keep
SIP Connection Reuse	Enable
SIP Mutual TLS Enable	Disable
SIP Validate Any TLS Certificate	Disable
SIP Trunking Codec PR1	G.729
SIP Trunking Codec PR2	G.711a
SIP Trunking Codec PR3	G.711u
SIP Trunking Codec PR4	Disable
SIP Trunking Use Alias	Disable
SIP Trunking Max Channel	64
Outgoing Originator Codec Use	Disable
Incomming Call Fixed Codec	Disable
Anonymous Host Name	Disable

FIELD	PURPOSE
Outbound Proxy Port	Sets the TCP or UDP port used to communicate with the SIP Carrier. For TLS this value is typically 5061.
URI Type	Sets the login method for this SIP Carrier. Options are SIP, TEL, and SIPS.
SIP Signal Type	Sets the signalling type for IP packets. Options are UDP, TCP, and TLS.
SIP Connection Reuse	Sets whether or not TLS certification must happen on every call or only once during registration
SIP Mutual TLS Enable	Sets whether or not to use TLS encryption on calls for this SIP Carrier
SIP Validate Any TLS Certificate	Sets whether the system will reject (Disable) or accept (enable) unknown certificates during the TLS handshake

- DM **Menu 5.2.17 VoIP Peering**

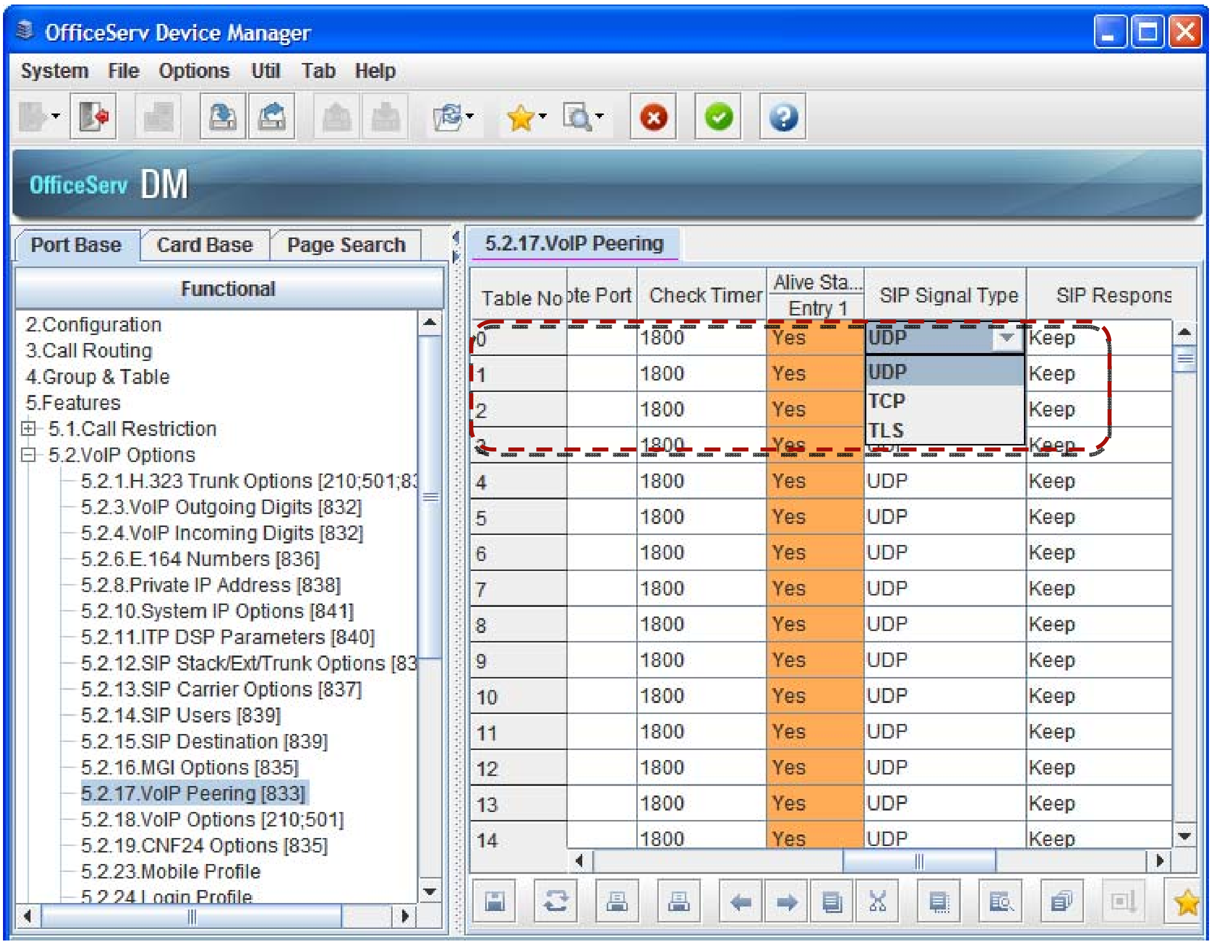

OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.17.VoIP Peering

Table No	ote Port	Check Timer	Alive Sta... Entry 1	SIP Signal Type	SIP Respons
0		1800	Yes	UDP	Keep
1		1800	Yes	UDP	Keep
2		1800	Yes	TCP	Keep
3		1800	Yes	TLS	Keep
4		1800	Yes	UDP	Keep
5		1800	Yes	UDP	Keep
6		1800	Yes	UDP	Keep
7		1800	Yes	UDP	Keep
8		1800	Yes	UDP	Keep
9		1800	Yes	UDP	Keep
10		1800	Yes	UDP	Keep
11		1800	Yes	UDP	Keep
12		1800	Yes	UDP	Keep
13		1800	Yes	UDP	Keep
14		1800	Yes	UDP	Keep

Here you can enable or disable TLS per SIP Peer connection.

General SIP Trunk Use Enhancements

GENERAL DESCRIPTION

Version 4.60 adds several enhancements to SIP trunk usage:

- **Specify which and how many SIP Trunks can be used for which SIP Provider**

In prior versions of software all licensed SIP trunks were seen as one large pool for incoming calls, and it was not possible to determine how many trunks could be reserved for incoming calls. Version 4.60 changes this by adding the ability to specify the maximum number of SIP trunks that can be used for incoming calls for each SIP Carrier and how many can be used for SIP Peering.

- **Segregate SIP Provider trunk calls from SIP Peer trunk calls**

In addition to the segregation of inbound SIP Carrier traffic, version 4.60 also enhances system Trunk Groups by adding a field to SIP Trunk Groups that determines which SIP Carrier can use the Trunk Group or if it is used for SIP Peering. This ensures a greater level of control over SIP trunks for outbound calls and call accounting by assigning which specific trunks are used for which service.

- **Voice Band Data (VBD) support for Fax-over-IP (FoIP)**

Many of the error correction techniques used in VoIP processing are designed to ensure that voice data sounds as good as possible. As VoIP usage is increasing, more and more Fax machines are being connected to SIP lines and becoming subject to these same error correction techniques. This can have a negative effect to fax transmissions. With version 4.60 it is now possible for MGIs to use the Voice Band Data (VBD) protocol. The VBD protocol disables NLP and Jitter Buffer processing to ensure that data transmissions (like fax or modem data) are not distorted.

- **Outgoing Caller ID blocking for SIP Trunks**

With version 4.60 software it is now possible to block outgoing Caller ID on SIP Carrier or SIP Peer trunks. The option is also provided to allow blocking of the OfficeServ 7000 Series system host ID as well.
If Caller ID is disabled the SIP Carrier or SIP Peer will receive a CID packet in the form of <anonymous@*[OfficeServ Public IP Address]*>. If the host ID is hidden as well the CID packet sent will show <anonymous@anonymous.invalid>.

NOTE: Some *SIP Providers do not support hiding the host ID. Check with your SIP Carrier before enabling host ID masking.*

- **Tandem trunking for SIP Peers**

Prior to version 4.60 it was not possible to disable tandem trunking with SIP Peer trunks. Version 4.60 changes this by adding an option to enable or disable tandem trunking, which is the ability for an incoming call on a SIP Peer trunk to be connected to an outgoing SIP Carrier or SIP Peer trunk, on SIP Peer trunks.

- **SIP Trunk Error Alarm**

A new series of alarm indications have been added to version 4.60 relating to SIP Trunks. Any time a SIP trunk registers or loses registration it will now be logged in the system, as will any resource or allocation errors relating to SIP Trunks.

- **Specify how the system should respond to unknown SIP traffic**

Prior to version 4.60 the only way to ignore SIP traffic from unknown sources was to send a reject message. This lets a hacker know that the system exists and can lead to an increase in hacker traffic. In version 4.60 it is now possible to determine exactly how the system should respond to incoming SIP traffic from unknown sources. The new options are **No Response**, meaning that the system simply ignores the traffic as if it had not been detected.**Response**, which means that the system will send a SIP reject message. And **none**, which means that the system will accept the unknown traffic as valid.

- **Specify codec used for SIP Trunks**

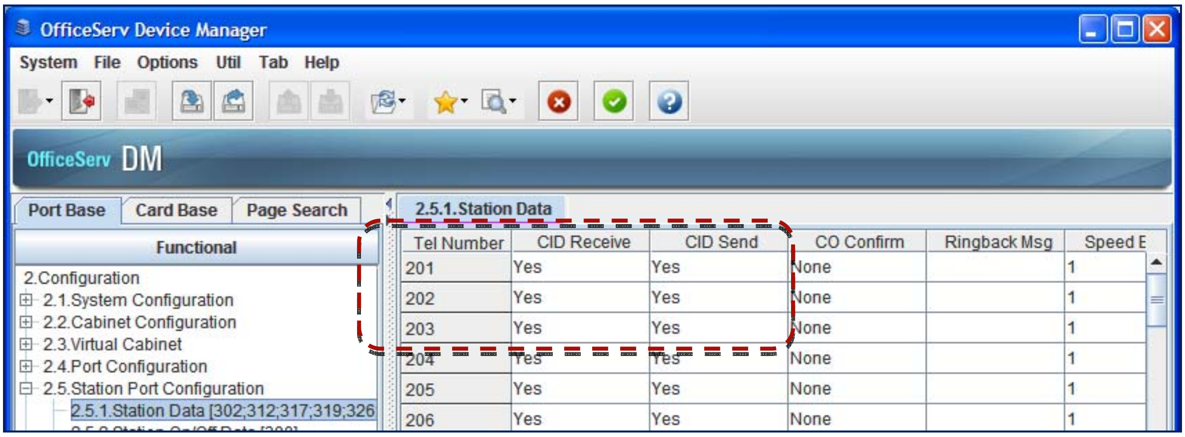
Version 4.60 adds the ability to specify the audio codec used for SIP conversations. Different codecs can be chosen for each SIP Carrier and each SIP Peer. Additionally there are four codec priority levels that can be set so that if the desired codec cannot be used the next lower priority codec will be automatically attempted.

General SIP Trunk Use Enhancements

PROGRAMMING

Six DM Menus have been modified to deliver these new SIP trunk enhancements.

- DM **Menu 2.5.1 Station Data**

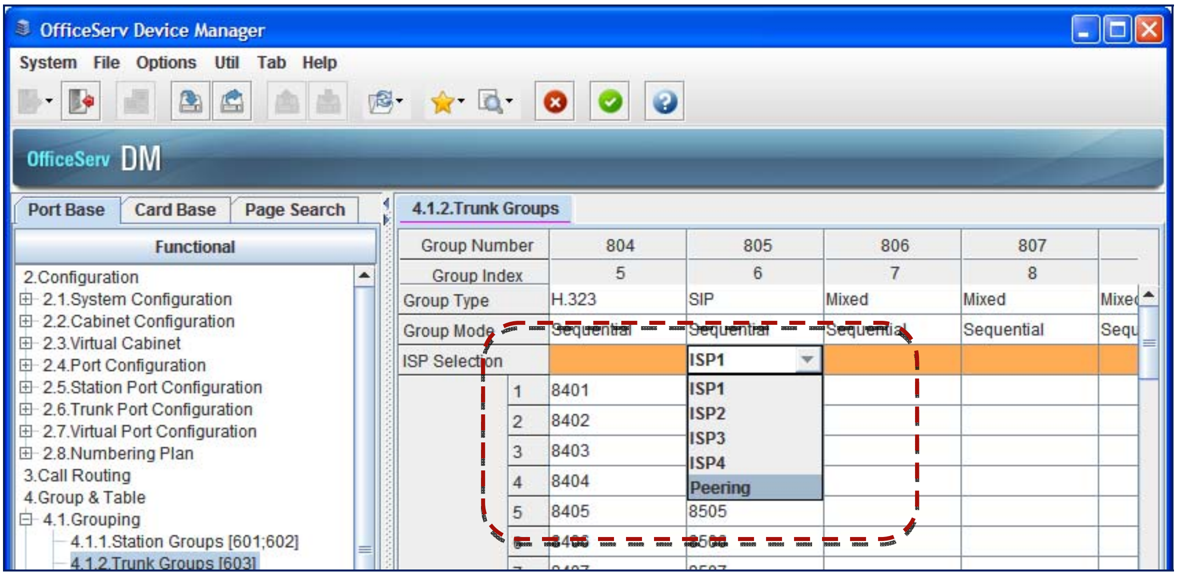

OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
2.1.System Configuration
2.2.Cabinet Configuration
2.3.Virtual Cabinet
2.4.Port Configuration
2.5.Station Port Configuration
2.5.1.Station Data [302;312;317;319;326
2.5.1.Station Data

Tel Number	CID Receive	CID Send	CO Confirm	Ringback Msg	Speed E
201	Yes	Yes	None		1
202	Yes	Yes	None		1
203	Yes	Yes	None		1
204	Yes	Yes	None		1
205	Yes	Yes	None		1
206	Yes	Yes	None		1

Here you can set whether or not this extension will send CLI when making a call.

This option is unchanged, but from v4.60 it will determine the extension's CLI information for SIP calls also.

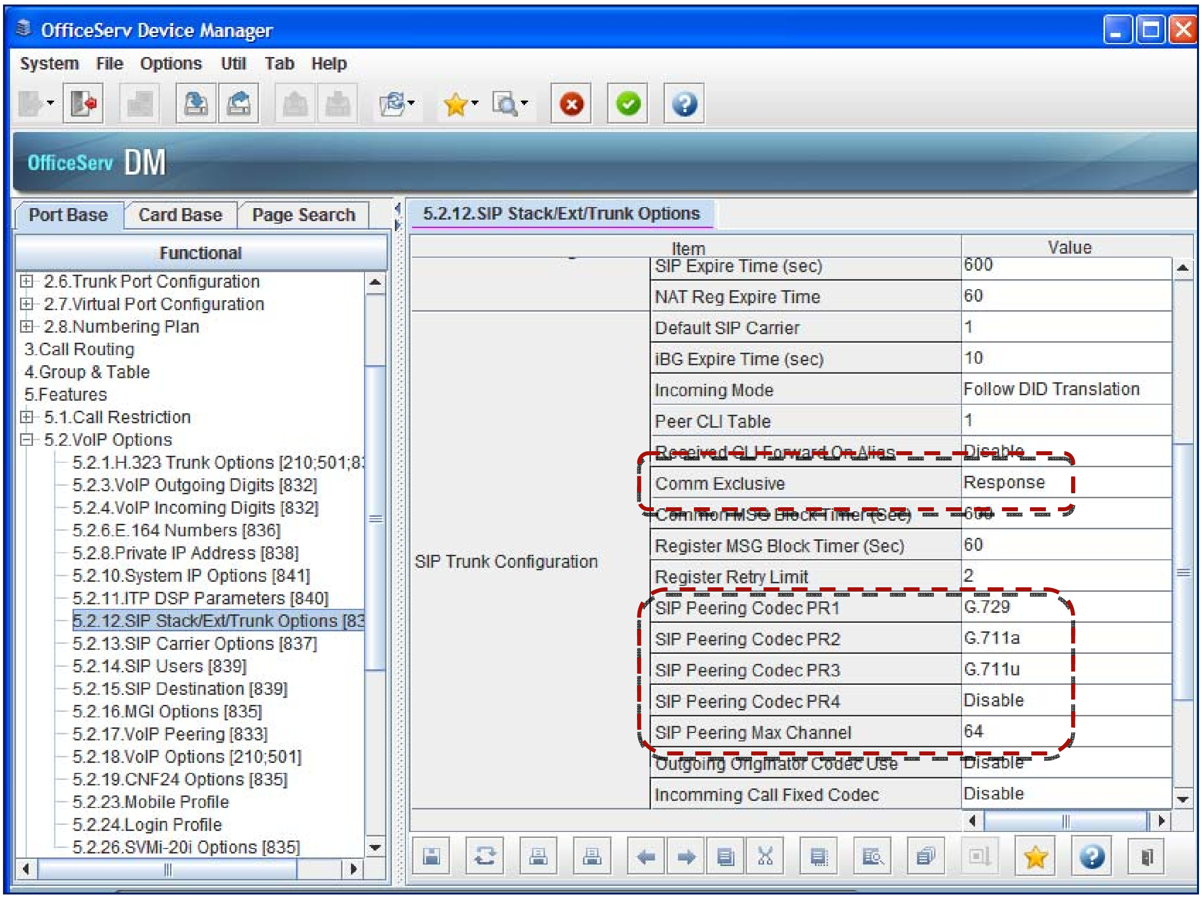
- DM **Menu 4.1.2 Trunk Groups**



	Group Number	804	805	806	807	
	Group Index	5	6	7	8	
Group Type		H.323	SIP	Mixed	Mixed	Mixed
Group Mode		Sequential	Sequential	Sequential	Sequential	Sequ
ISP Selection			ISP1			
	1	8401				
	2	8402				
	3	8403				
	4	8404				
	5	8405	8505			
	6	8406	8506			
	7	8407	8507			

Here you can assign each SIP trunk group to an ISP or to SIP Peering.

- DM **Menu 5.2.12 SIP Stack/Ext/Trunk Options**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.6.Trunk Port Configuration
2.7.Virtual Port Configuration
2.8.Numbering Plan
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.26.SVMi-20i Options [835]
5.2.12.SIP Stack/Ext/Trunk Options

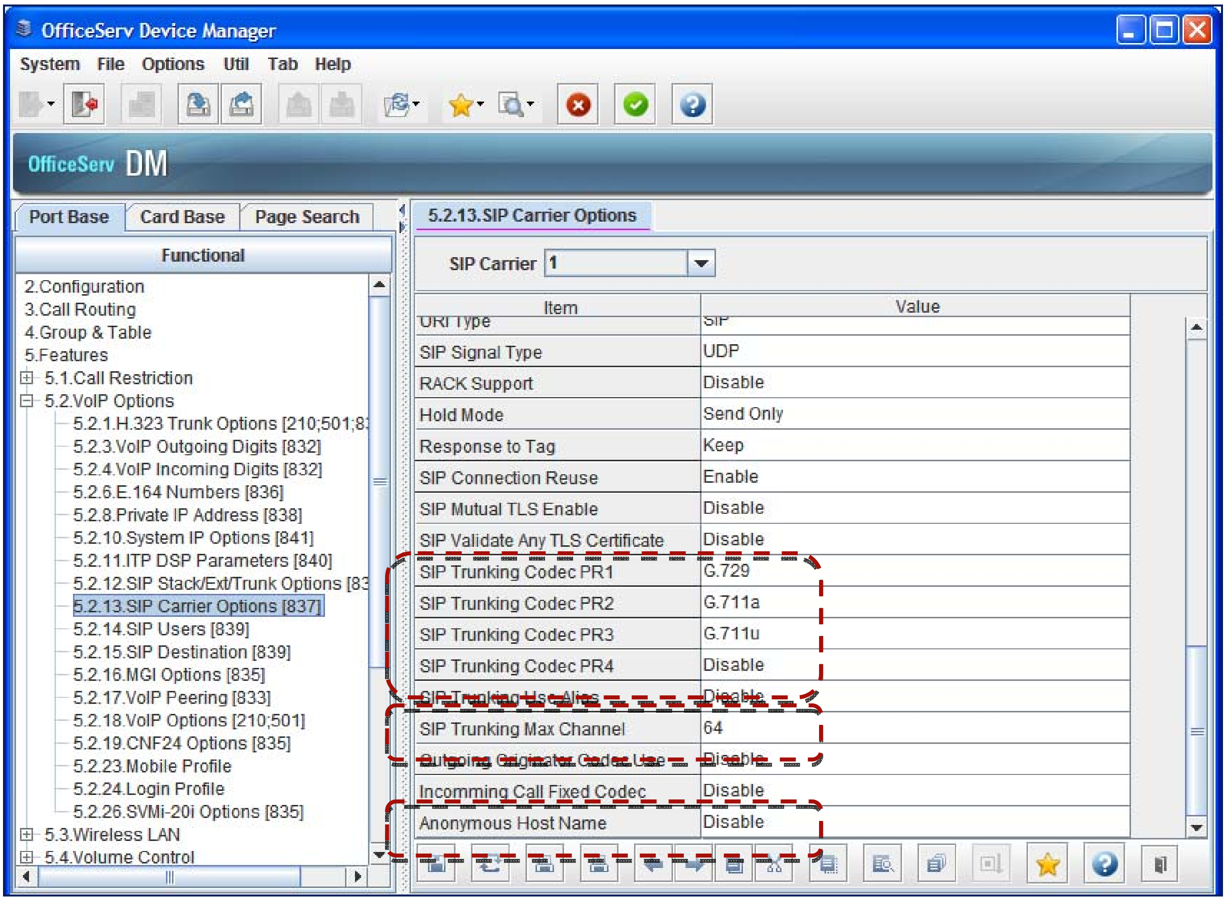
	Item	Value
SIP Trunk Configuration	SIP Expire Time (sec)	600
	NAT Reg Expire Time	60
	Default SIP Carrier	1
	iBG Expire Time (sec)	10
	Incoming Mode	Follow DID Translation
	Peer CLI Table	1
	Received CLI Forward On Alias	Disable
	Comm Exclusive	Response
	Common MSG Block Timer (Sec)	600
	Register MSG Block Timer (Sec)	60
	Register Retry Limit	2
	SIP Peering Codec PR1	G.729
	SIP Peering Codec PR2	G.711a
	SIP Peering Codec PR3	G.711u
	SIP Peering Codec PR4	Disable
	SIP Peering Max Channel	64
	Outgoing Originator Codec Use	Disable
	Incomming Call Fixed Codec	Disable

FIELD	PURPOSE
Comm Exclusive	Sets the method the system will use to respond with error message to SIP traffic from unknown sources.
SIP Peering Codec PR1 ~ 4	Sets the audio codec prioritization to use when establishing a SIP Peering call. PR1 will be attempted first and if that codec cannot be negotiated PR2 will be attempted…
SIP Peering Max Channel	Sets the maximum number of trunks that can be used simultaneously for inbound or outbound SIP Peering calls. Call attempts beyond this limit will receive a busy.

⚠

If the IP address is used (rather than the Domain name) in outbound proxy of the SIP carrier (DM 5.2.13), you will need to set Comm Exclusive to “none” to avoid rejecting the incoming call.

- DM **Menu 5.2.13 SIP Carrier Options**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base Card Base Page Search
Functional
5.2.13.SIP Carrier Options

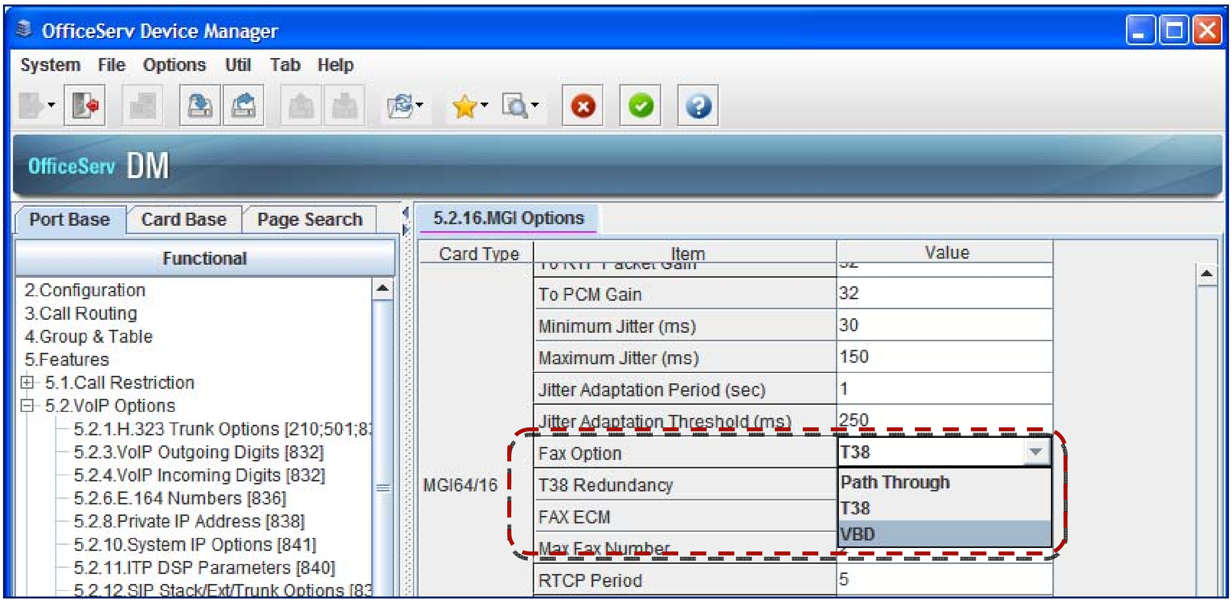
2.Configuration
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.26.SVMi-20i Options [835]
5.3.Wireless LAN
5.4.Volume Control

SIP Carrier 1

Item	Value
URI Type	SIP
SIP Signal Type	UDP
RACK Support	Disable
Hold Mode	Send Only
Response to Tag	Keep
SIP Connection Reuse	Enable
SIP Mutual TLS Enable	Disable
SIP Validate Any TLS Certificate	Disable
SIP Trunking Codec PR1	G.729
SIP Trunking Codec PR2	G.711a
SIP Trunking Codec PR3	G.711u
SIP Trunking Codec PR4	Disable
SIP Trunking Use Alias	Disable
SIP Trunking Max Channel	64
Outgoing Originator Codec Use	Disable
Incomming Call Fixed Codec	Disable
Anonymous Host Name	Disable

FIELD	PURPOSE
SIP Trunking Codec PR1 ~ 4	Sets the audio codec prioritization to use when establishing a call for this SIP Carrier. PR1 will be attempted first and if that codec cannot be negotiated PR2 will be attempted, etc.
SIP Trunking Max Channel	Sets the maximum number of trunks that can be used simultaneously for inbound or outbound calls using this SIP Carrier. Call attempts beyond this limit will receive a busy signal.
Anonymous Host Name	When Enabled, outbound calls for this SIP Carrier will have an anonymous host name, so the Caller ID information sent will be in the form <[stationID]@anonymous.invalid>

- DM **Menu 5.2.16 MGI Options**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [83
5.2.16.MGI Options
Path Through
T38
VBD

Card Type	Item	Value
MGI64/16	To PCM Gain	32
	Minimum Jitter (ms)	30
	Maximum Jitter (ms)	150
	Jitter Adaptation Period (sec)	1
	Jitter Adaptation Threshold (ms)	250
	Fax Option	T38
	T38 Redundancy	
	FAX ECM	
	Max Fax Number	
	RTCP Period	5

Here you can determine what type of service is used for Fax over IP calls:

1. T.38
2. Pass Through
3. Or the new VBD option

- DM **Menu 5.2.17 VoIP Peering Options**

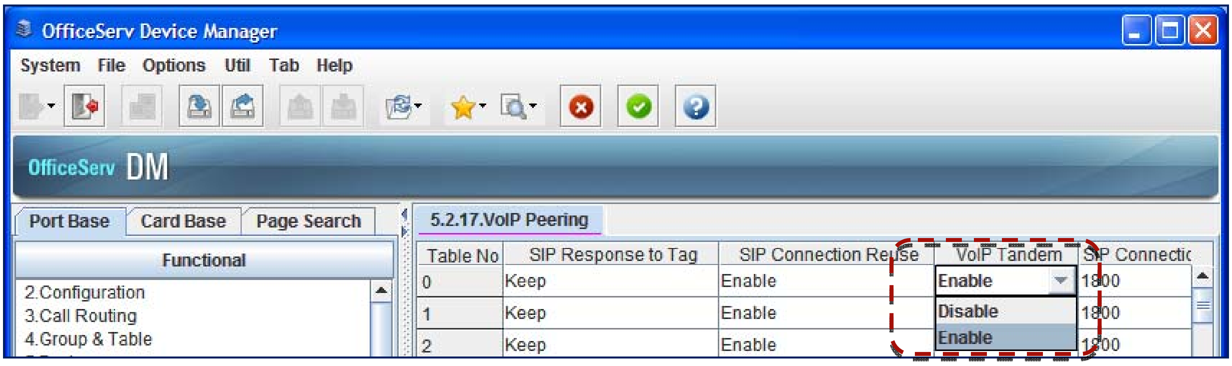


Table No	SIP Response to Tag	SIP Connection Reuse	VoIP Tandem	SIP Connectic
0	Keep	Enable	Enable	1800
1	Keep	Enable		1800
2	Keep	Enable		1800

Here you can enable or disable the system’s ability route incoming SIP Peering calls out over other trunk circuits – SIP, ISDN etc.

1. VoIP Tandem

Advanced Plug and Play Options

GENERAL DESCRIPTION

Businesses that deploy a large number of IP telephones can often be frustrated by the amount of time it takes to set up, configure and connect each IP terminal.

As these larger businesses often have in-house IT departments that will manage the IP telephony deployment on-going, it is becoming more apparent that simple Plug and Play technology is paramount to these types of customers.

V4.60 takes the already substantial PnP functionality on the OfficeServ IP phones and enhances it to make it even more of a “zero touch” deployment for high numbers of IP phones.

This feature, enabled by version 4.60 and the latest IP phone software, allows SMT-i Series IP phones to find the OfficeServ system automatically and register with minimal pre-setup.

Version 4.60 also adds the ability to set the OfficeServ system as a DHCP server (*for OfficeServ 7030, 7100, and 7200S only*) and to specify how to register IP phones.

Version 4.60 allows SMT-i Series IP phones to register in one of three ways:

- **ID/Password Registration (Normal Login)**

This is the normal registration method used by OfficeServ systems prior to version 4.60 and for ITP Series IP Phones, OfficeServ Softphones, and OfficeServ Communicator Softphones

- **MAC Address Registration (Pre-MAC Address)**

This mode allows the technician to set which extension number corresponds to which IP Phone MAC Address. When connecting to the system it can be assigned the correct station registration

- **Auto Registration (Auto PNP)**

This mode, which is the system default, allows phones to register without any user or technician action at all. When an IP phone connects to the system the MAC address will automatically be assigned to the next available IP extension number in sequence.

Both the MAC Address and Auto Registration modes require custom DHCP flags to be sent to the SMT-i Series IP phones when it is assigned an IP address. These DHCP settings are automatically configured when an OfficeServ 7030, 7100, or 7200S is set to operate as a DHCP server, but the same settings can be configured for sites with an OfficeServ 7200 or 7400 where a customer-provided DHCP server isalready installed.

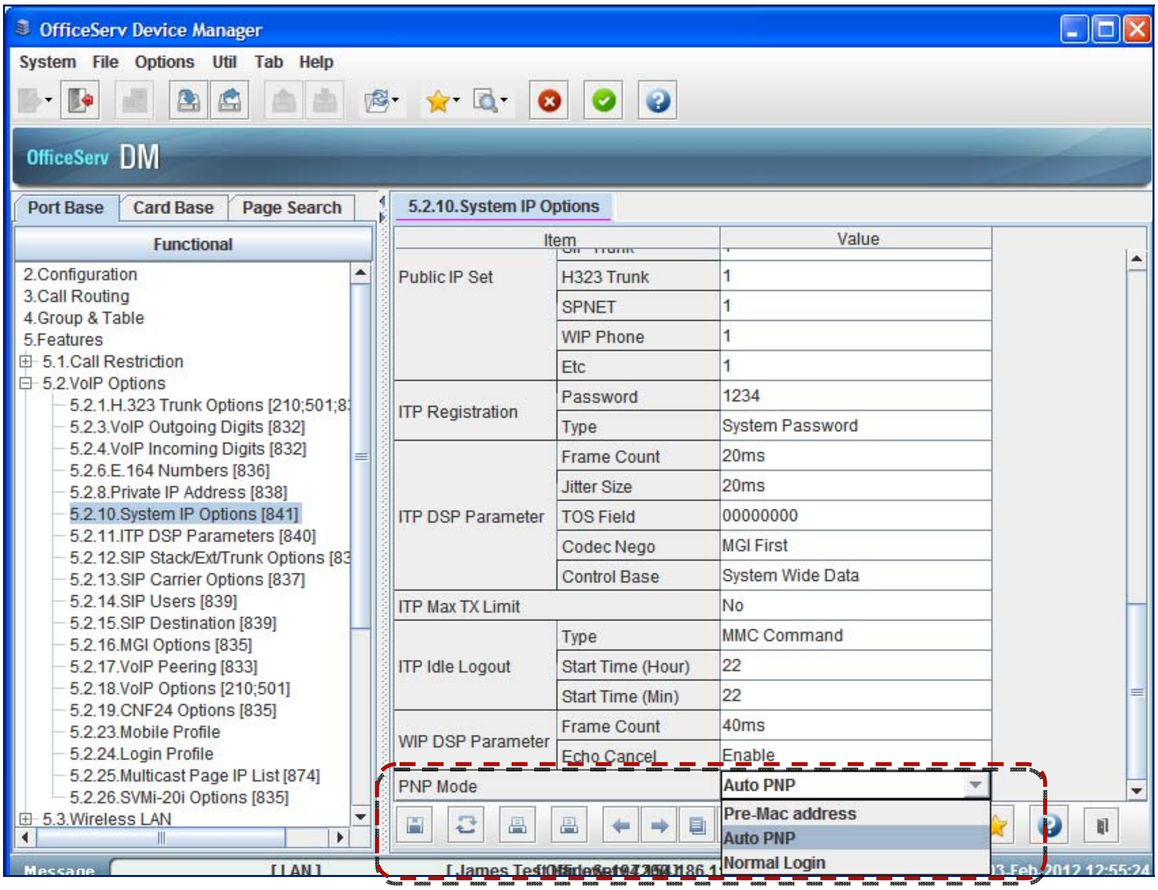
Advanced Plug and Play Options

PROGRAMMING

Just one DM Menu is used to manage the PnP settings for the OfficeServ. **Menu 5.2.10** is an existing Menu used to manage various IP phone settings.

The SMT IP phone range can also use standard based DHCP server settings: Option 66 and 128.

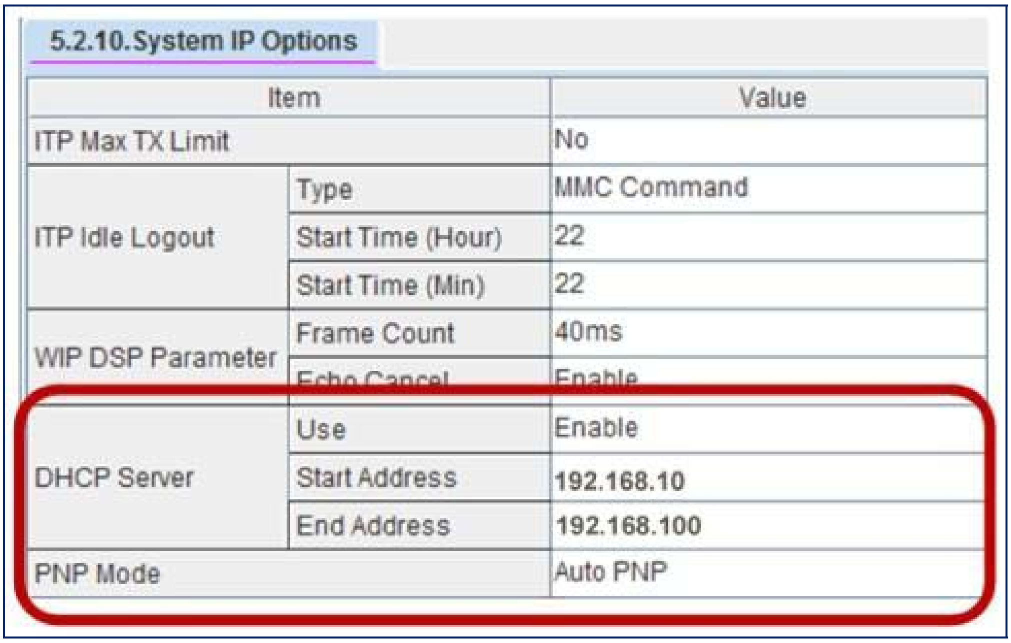
- DM **Menu 5.2.10 System IP Options (OS7200 / OS7400)**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.8.Private IP Address [838]
5.2.10.System IP Options [841]
5.2.11.ITP DSP Parameters [840]
5.2.12.SIP Stack/Ext/Trunk Options [8
5.2.13.SIP Carrier Options [837]
5.2.14.SIP Users [839]
5.2.15.SIP Destination [839]
5.2.16.MGI Options [835]
5.2.17.VoIP Peering [833]
5.2.18.VoIP Options [210;501]
5.2.19.CNF24 Options [835]
5.2.23.Mobile Profile
5.2.24.Login Profile
5.2.25.Multicast Page IP List [874]
5.2.26.SVMi-20i Options [835]
5.3.Wireless LAN
Message
[LAN]
5.2.10.System IP Options

Item		Value
Public IP Set	H323 Trunk	1
	SPNET	1
	WIP Phone	1
	Etc	1
ITP Registration	Password	1234
	Type	System Password
ITP DSP Parameter	Frame Count	20ms
	Jitter Size	20ms
	TOS Field	00000000
	Codec Nego	MGI First
	Control Base	System Wide Data
ITP Max TX Limit		No
ITP Idle Logout	Type	MMC Command
	Start Time (Hour)	22
	Start Time (Min)	22
WIP DSP Parameter	Frame Count	40ms
	Echo Cancel	Enable
PNP Mode		Auto PNP

FIELD	PURPOSE
PNP Mode	Sets the Plug-N-Play registration mode Auto PNP, pre-MAC address, or normal login

- DM **Menu 5.2.10 System IP Options (OS7030/OS7100/OS7200S with DHCP Options)**



5.2.10.System IP Options

Item		Value
ITP Max TX Limit		No
ITP Idle Logout	Type	MMC Command
	Start Time (Hour)	22
	Start Time (Min)	22
WIP DSP Parameter	Frame Count	40ms
	Echo Cancel	Enable
DHCP Server	Use	Enable
	Start Address	192.168.10
	End Address	192.168.100
PNP Mode		Auto PNP

DHCP Server Use	Sets whether or not the OfficeServ will be used as a DHCP Server *Available only on OfficeServ 7030 / 7100 / 7200S*
Start Address	Sets the start IP address of the DHCP pool Must be the same as the OfficeServ system subnet range
End Address	Sets the final IP address of the DHCP pool

Configuring a Customer-Provided DHCP Server

In order to configure a customer-provided DHCP Server there are two options that must be configured. It is not possible to give specific instructions on how to implement these two options as every DHCP Server’s configuration is different, but the DHCP option numbers are industry-standard, which should aid in finding the specifics for the server in use.

Option 66 – TFTP Server Name

This option tells the DHCP server to respond to requests sent from specific host names. In the case of the SMT-i Series phones this value should be set to “SEC_ITP”.

Option 128 – TFTP Server IP

After receiving an option 66 request the DHCP server will use option 128 to send out the IP address of the server the requesting host should connect to. This value should be set to the IP address of the OfficeServ.

Multicast Paging for IP Phones

GENERAL DESCRIPTION

As VoIP technology is accepted more and more as the preferred solution for telephony for local users connected to a company LAN, as well as remote users over a WAN, it has become vital to reduce the amount traffic on the LAN.

V4.60 delivers the Multicast service for paging to IP telephones. Prior to V4.60 if a user establishes a page call to a number of, or all IP phones on the network, the system would send a separate media stream to each and every IP phone that is receiving the page call. The system would also need to assign an MGI resource for each IP phone, which is not only extra load on the LAN, but also uses a high number of MGI channels for just one call.

By using Multicast just a single media stream will be used, and just one MGI channel will be allocated for the page call.

⚠

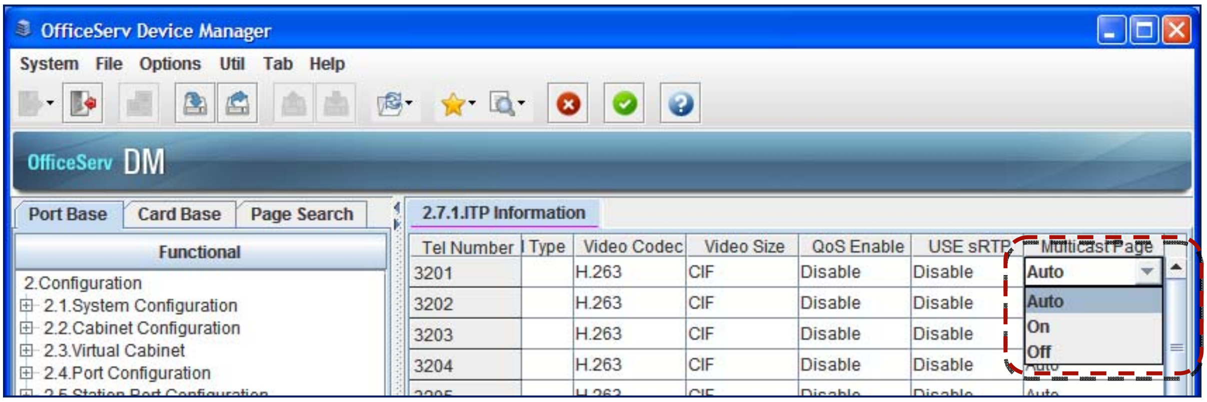
Only IP phones on the local LAN can use the Multicast feature. IP Phones across a WAN network may still require an individual MGI resource.
Where the Routers that support the WAN are Multicast compliant, the Multicast functions of the OfficeServ can be used.

Multicast Paging for IP Phones

PROGRAMMING

Two DM Menus have been modified and one has been added to support multicasting. The new menu is 5.2.25 Multicast Page IP List and the modified menus are 2.7.1 ITP Information and 4.1.3 Page Groups.

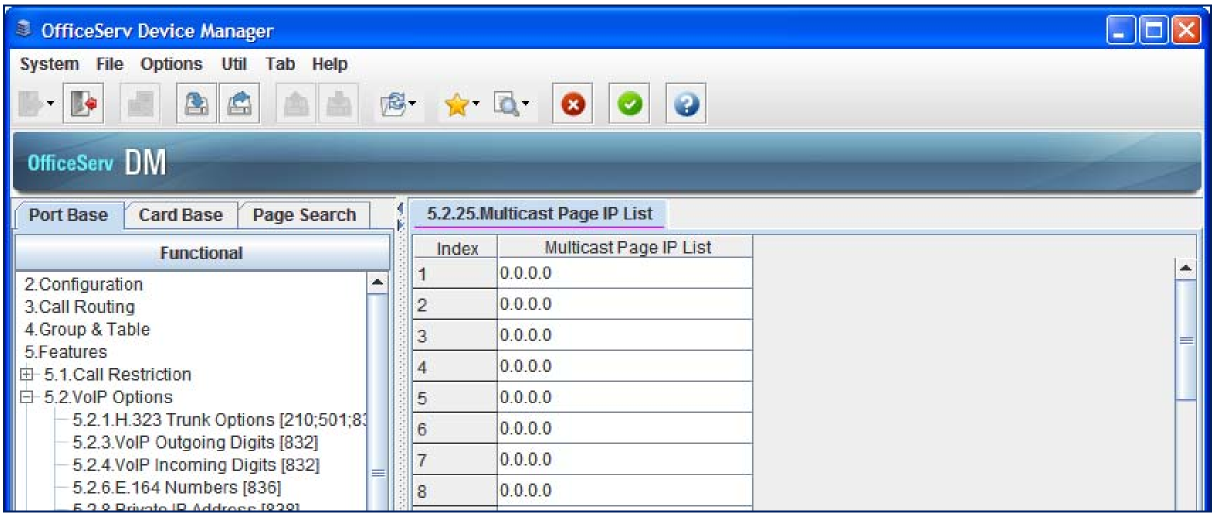
- DM **Menu 2.7.1 ITP Information**



Tel Number	Type	Video Codec	Video Size	QoS Enable	USE sRTP	Multicast Page
3201		H.263	CIF	Disable	Disable	Auto
3202		H.263	CIF	Disable	Disable	
3203		H.263	CIF	Disable	Disable	
3204		H.263	CIF	Disable	Disable	
3205		H.263	CIF	Disable	Disable	Auto

Here you can enable Multicast per IP extension.

- DM **Menu 5.2.25 Multicast IP List**

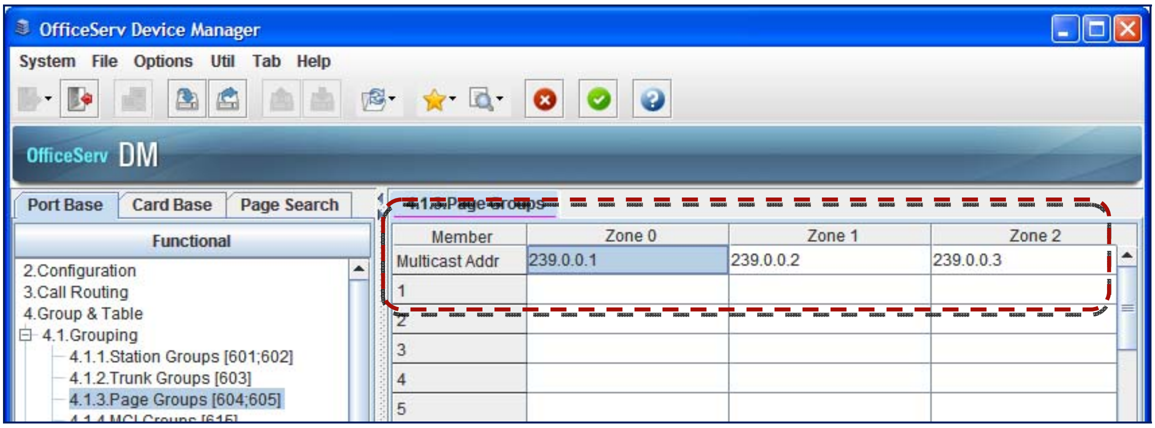

OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
5.1.Call Restriction
5.2.VoIP Options
5.2.1.H.323 Trunk Options [210;501;8
5.2.3.VoIP Outgoing Digits [832]
5.2.4.VoIP Incoming Digits [832]
5.2.6.E.164 Numbers [836]
5.2.25.Multicast Page IP List

Index	Multicast Page IP List
1	0.0.0.0
2	0.0.0.0
3	0.0.0.0
4	0.0.0.0
5	0.0.0.0
6	0.0.0.0
7	0.0.0.0
8	0.0.0.0

Here you can assign IP address data for up to 80 remote subnets that can receive Multicast packets.

If no remote IP phones are in use, or the Routers supporting the remote IP phones cannot support Multicast, then this table can be left in its default state.

- DM **Menu 4.1.3 Page Groups**



Member	Zone 0	Zone 1	Zone 2
Multicast Addr	239.0.0.1	239.0.0.2	239.0.0.3
1			
2			
3			
4			
5			

Here you can assign Page Zones to be Multicast or Unicast. Multicast uses well-known IP addresses and any data network equipment should recognise these address ranges as Multicast – but please check the network equipment's capabilities with Multicast first.

FIELD	PURPOSE
Multicast Page IP List	Sets the Multicast IP address for each Zone. A default value of 255.255.255.255 means that Multicast will not be used. Valid Multicast addresses are: 224.0.0.1 ~ 239.255.255.254.

OfficeServ Connect Enhancements - Mobex

GENERAL DESCRIPTION

OfficeServ Connect, which is Samsung's Mobex solution, has been a very successful solution to businesses wishing to better organise and deliver calls to their mobile or remote workforce.

V4.60 enhances the solution to even greater heights and delivers even more business benefits by adding the following set of new functionality:

- **MOBEX Scheduling**

Allows a user to set the hours during which MOBEX is active. Up to three periods can be set per day of the week. As an example, a user can ensure that they do not receive MOBEX calls during lunch, when driving home, on weekends, or between the weekday hours of 9pm and 7am.

- **MOBEX Targeting**

Allows a user to set which types of calls will make it to their mobile phone. Users can specify whether internalcallers, externalcallers, or SPNet callers will reach their mobile phone. They can also determine whether or not calls to Station Groups they are a member of will ring to their mobile phone.

- **Executive MOBEX Callback**

When an Executive MOBEX user wants to make a call through the system, it can often lead to higher call charges if for example they are out of the country. Version 4.60 allows an Executive MOBEX user to be set so that when they call in to the system it immediately hangs up that call and then calls them back. When they answer they will hear system dial tone and are then able to dial out as normal. This ensures that any toll charges for using Executive MOBEX call go to the system trunk lines instead of the cell phone. Also added isa timer to set how long the system should wait after disconnecting to call back to the Executive MOBEX phone and a counter to determine how many times the callback should be attempted before aborting.

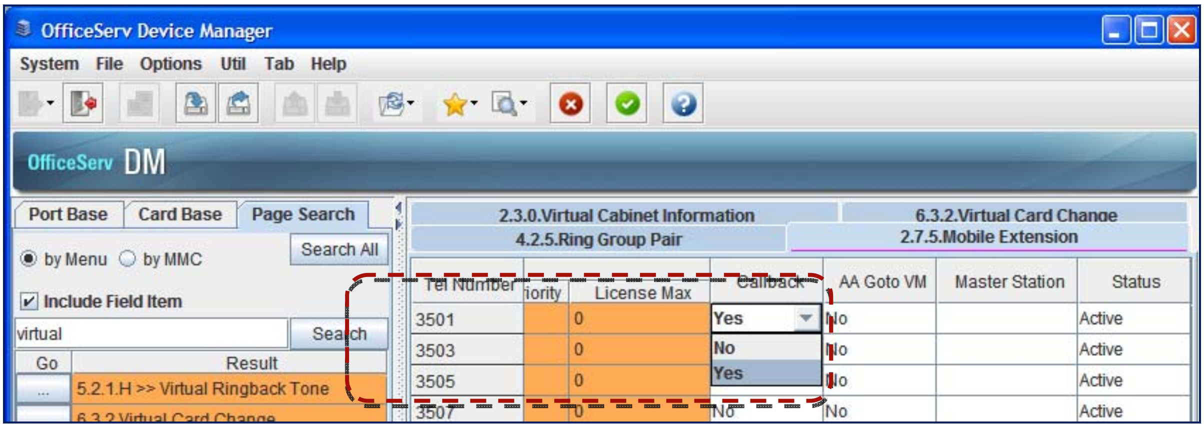
- **MOBEX Busy**

For heavy MOBEX users it is common that while speaking on their mobile phone at their desk a second call rings in to their desk phone. In prior versions of software this was unavoidable, but version 4.60 adds the option for the system to see both the MOBEX extension and the paired desk phone as busy when either device is in use, much the way that Station Pairing operates.

OfficeServ Connect Enhancements - Mobex

PROGRAMMING

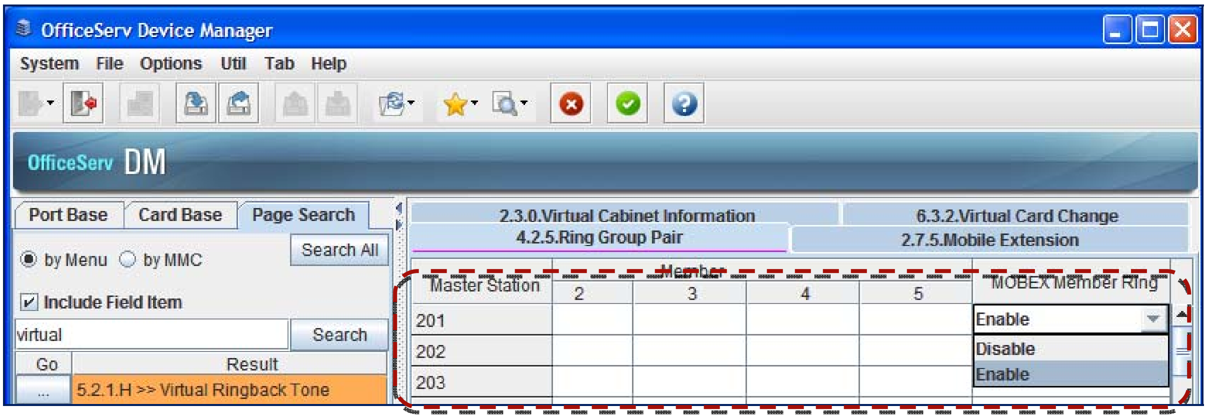
- DM **Menu 2.7.5 Mobile Extension**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Search All
● by Menu ○ by MMC
☑ Include Field Item
virtual
Search
Go
Result
5.2.1.H >> Virtual Ringback Tone
6.3.2 Virtual Card Change
2.3.0.Virtual Cabinet Information
6.3.2.Virtual Card Change
4.2.5.Ring Group Pair
2.7.5.Mobile Extension

Tel Number	iority	License Max	Callback	AA Goto VM	Master Station	Status
3501		0	Yes	No		Active
3503		0	No	No		Active
3505		0	Yes	No		Active
3507		0	No	No		Active

Here you can assign whether the Mobex user can have the Mobex CALLBACK feature or not.

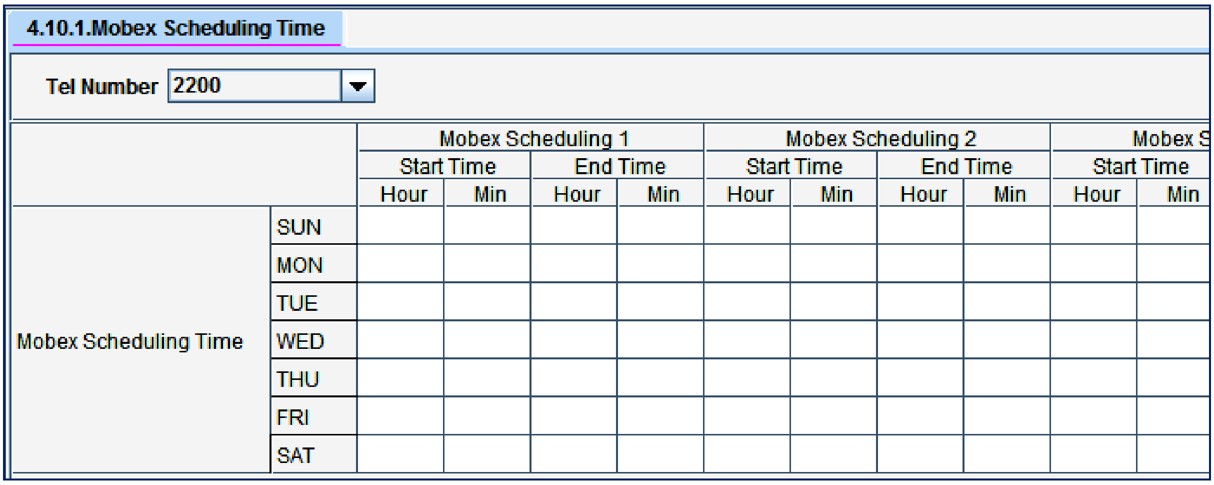
- DM **Menu 4.2.5 Ring Group Pair**



Master Station	Member				MOBEX Member Ring
	2	3	4	5	
201					Enable
202					Disable
203					Enable

Here you can enable or disable that ALL Mobex member devices are considered busy when any device in busy.

- DM **Menu 4.10.1 Mobex Schedule Time**



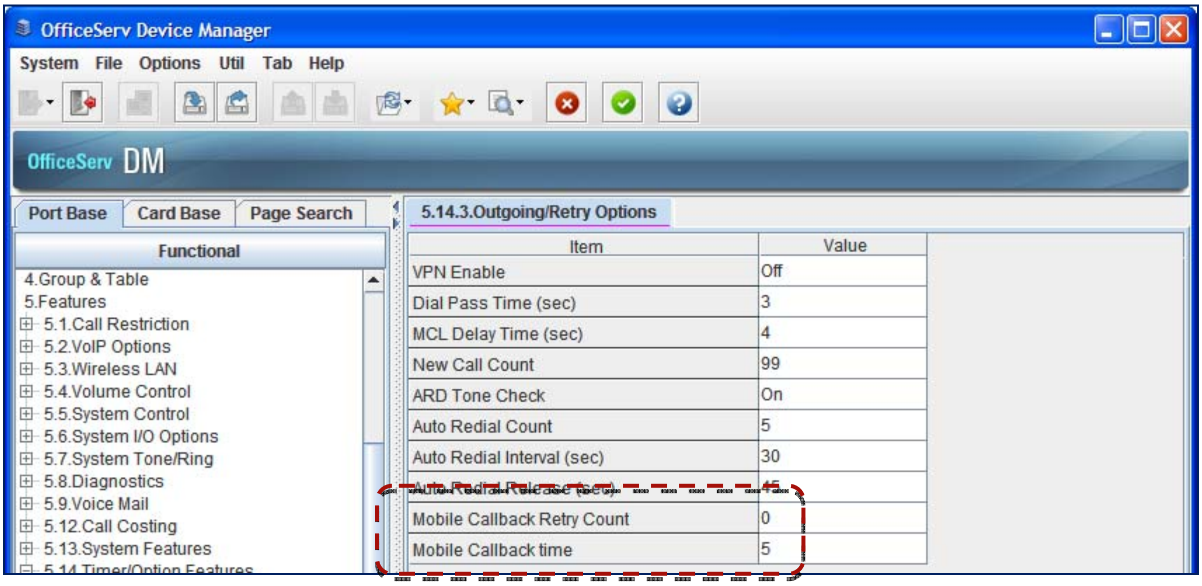
4.10.1.Mobex Scheduling Time

Tel Number 2200

		Mobex Scheduling 1				Mobex Scheduling 2				Mobex S	
		Start Time		End Time		Start Time		End Time		Start Time	
		Hour	Min	Hour	Min	Hour	Min	Hour	Min	Hour	Min
Mobex Scheduling Time	SUN										
	MON										
	TUE										
	WED										
	THU										
	FRI										
	SAT										

Here you can assign various schedules for Mobex calls to be delivered or not.

- DM **Menu 5.14.3 Outgoing Retry Options**

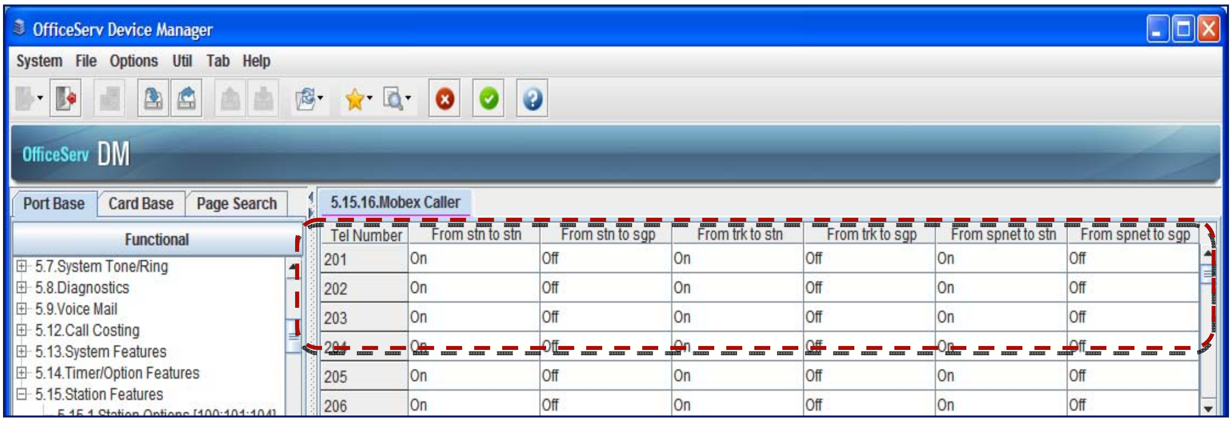


5.14.3.Outgoing/Retry Options

Item	Value
VPN Enable	Off
Dial Pass Time (sec)	3
MCL Delay Time (sec)	4
New Call Count	99
ARD Tone Check	On
Auto Redial Count	5
Auto Redial Interval (sec)	30
Auto Redial Release (sec)	15
Mobile Callback Retry Count	0
Mobile Callback time	5

FIELD	PURPOSE
Mobile Callback Retry Count	Sets the number of times the Executive MOBEX Callback feature will attempt to call the user back
Mobile Callback Time (sec)	Sets the amount of time the system will wait before making the initial Executive MOBEX Callback as well as the time made between callback attempts

- DM **Menu 5.15.16 Mobex Caller**



Tel Number	From stn to stn	From stn to sgp	From trk to stn	From trk to sgp	From spnet to stn	From spnet to sgp
201	On	Off	On	Off	On	Off
202	On	Off	On	Off	On	Off
203	On	Off	On	Off	On	Off
204	On	Off	On	Off	On	Off
205	On	Off	On	Off	On	Off
206	On	Off	On	Off	On	Off

Here you can enable or disable the type of calls that will be delivered to the Mobex user.

OfficeServ Connect Enhancements - Mobex

END-USER INSTRUCTIONS

How to setup Mobex Schedules from a handset:

1. Press **TRANSFER**and then dial **129**
2. Press **VOLUME + or –**to select the appropriate day of the week
3. Press the **RIGHT HAND SOFT KEY**twice
4. Dial the required time of day to enable Mobex calls: e.g. **0830**
5. Dial the required time of day to disable Mobex calls: e.g. **1730**
6. Press **TRANSFER**to exit and save the changes

Network Time Protocol Support (NTP Server Support)

GENERAL DESCRIPTION

The correct time and date on a PBX is such a simple and most basic feature. Yet it is also a vital component to the successful and professional operation of any business that operates specific working hours.

Simple daylight saving hour changes cause companies a constant headache when the clocks go back or forward each year, and leads to a peak in workload for a reseller's support desk.

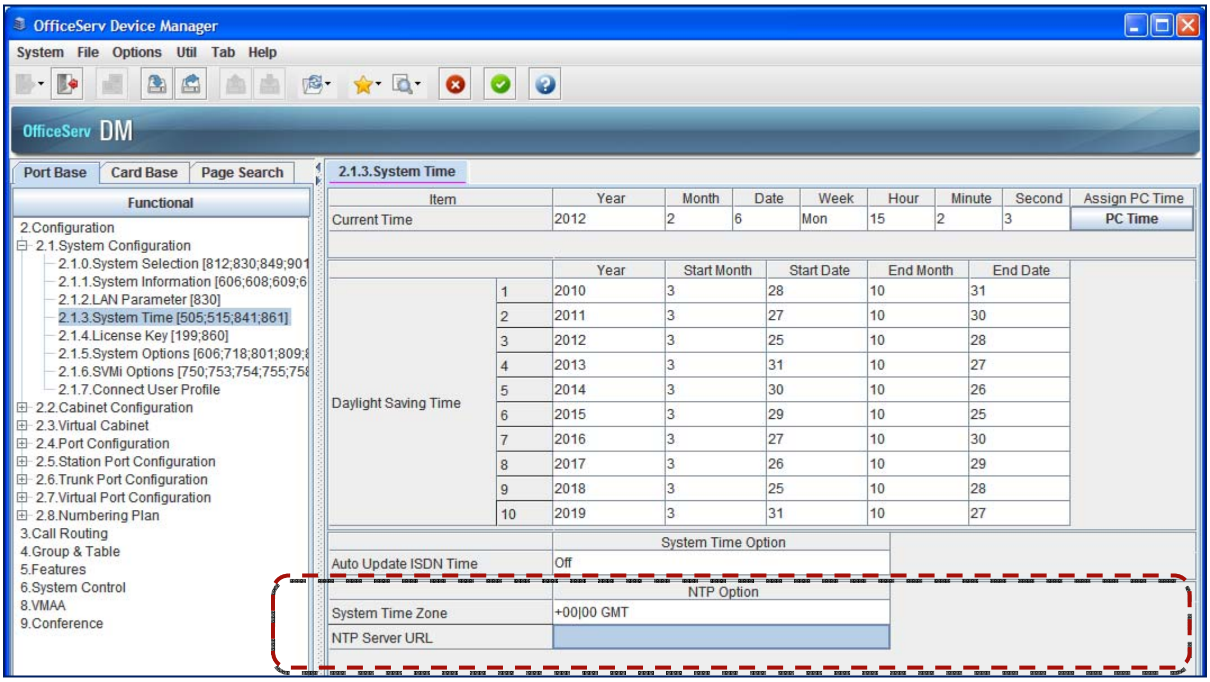
To overcome this, V4.60 delivers the latest method of system time and date information being automatically updated by an NTP Server.

NTP also negates the common misconception of system clocks that lose or gain time or where a system has suffered a power outage and therefore lost the correct time.

Network Time Protocol Support (NTP Server Support)

PROGRAMMING

- DM **Menu 2.1.3 System Time**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
2.1.System Configuration
2.1.0.System Selection [812;830;849;901
2.1.1.System Information [606;608;609;6
2.1.2.LAN Parameter [830]
2.1.3.System Time [505;515;841;861]
2.1.4.License Key [199;860]
2.1.5.System Options [606;718;801;809;8
2.1.6.SVMi Options [750;753;754;755;758
2.1.7.Connect User Profile
2.2.Cabinet Configuration
2.3.Virtual Cabinet
2.4.Port Configuration
2.5.Station Port Configuration
2.6.Trunk Port Configuration
2.7.Virtual Port Configuration
2.8.Numbering Plan
3.Call Routing
4.Group & Table
5.Features
6.System Control
8.VMAA
9.Conference
2.1.3.System Time
PC Time

Item	Year	Month	Date	Week	Hour	Minute	Second	Assign PC Time
Current Time	2012	2	6	Mon	15	2	3	PC Time

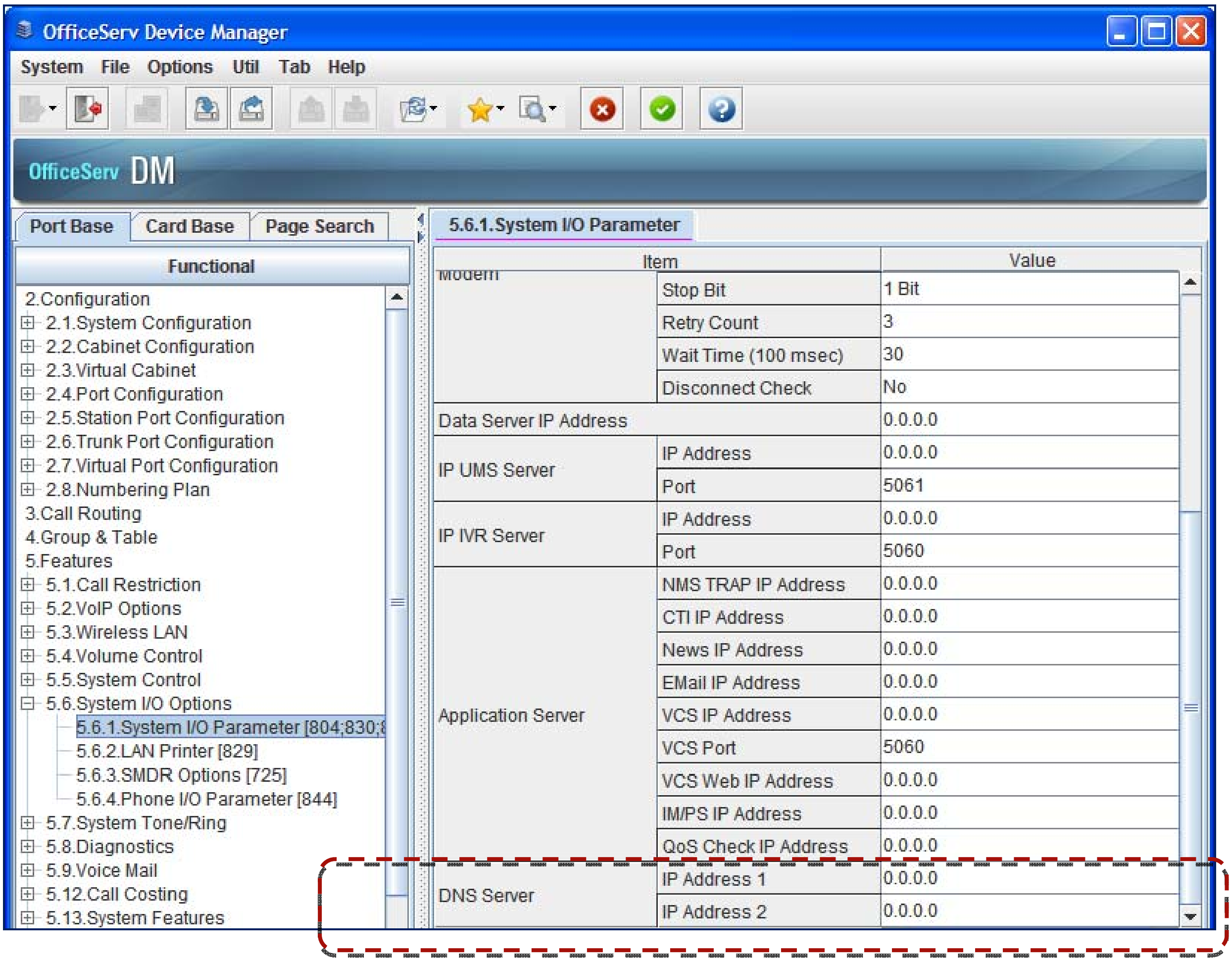
		Year	Start Month	Start Date	End Month	End Date
Daylight Saving Time	1	2010	3	28	10	31
	2	2011	3	27	10	30
	3	2012	3	25	10	28
	4	2013	3	31	10	27
	5	2014	3	30	10	26
	6	2015	3	29	10	25
	7	2016	3	27	10	30
	8	2017	3	26	10	29
	9	2018	3	25	10	28
	10	2019	3	31	10	27

	System Time Option
Auto Update ISDN Time	Off

	NTP Option
System Time Zone	+00|00 GMT
NTP Server URL	

Here you can assign the time zone & NTP Server URL.

- DM **Menu 5.6.1 System I/O Parameters**



Item		Value
Modem	Stop Bit	1 Bit
	Retry Count	3
	Wait Time (100 msec)	30
	Disconnect Check	No
Data Server IP Address		0.0.0.0
IP UMS Server	IP Address	0.0.0.0
	Port	5061
IP IVR Server	IP Address	0.0.0.0
	Port	5060
Application Server	NMS TRAP IP Address	0.0.0.0
	CTI IP Address	0.0.0.0
	News IP Address	0.0.0.0
	EMail IP Address	0.0.0.0
	VCS IP Address	0.0.0.0
	VCS Port	5060
	VCS Web IP Address	0.0.0.0
	IM/PS IP Address	0.0.0.0
	QoS Check IP Address	0.0.0.0
DNS Server	IP Address 1	0.0.0.0
	IP Address 2	0.0.0.0

Here you can assign the DNS IP address for the system. This address will be used by the OfficeServ to deliver such features as NTP Server support. This allows the system to resolve Domain names to IP addresses.

CNF24 Module Enhancements (Conference 24 Module)

GENERAL DESCRIPTION

The CNF24 module has been enhanced to include several new features and functions:

- **Add-to-Calendar With ICS Attachment**

When the Conference Card sends invite emails to attendees they now contain an iCalendar (.ics) file attachment, which is an industry standard calendar file that can be added to most personal or business calendar applications.

- **Retry on Invalid Conference ID or Password**

When an attendee accidentally enters an invalid conference ID or password they will now be prompted up to 3 times to retry before being disconnected.

- **Conference Email Login Instructions Support**

Prior to V4.60 the login instructions sent in the conference email had to be re-entered each time a conference was created, meaning that users had to maintain their own set of instructions to copy and paste during every conference creation. V4.60 has added the ability to save a system-wide instructions template that will be used for every conference.

NOTE: *Users may still set their own instructions if desired while creating their conference; the saved instructions are only populated for convenience.*

- **New Prompt Languages**

In addition to US English the following prompt languages have been added: *Korean, UK English, Australian English, German, Greek, Italian, Russian, Castilian Spanish, Turkish, Finnish, French, Dutch, Danish, Portuguese, Swedish, and Norwegian*. When the prompt language is changed the Conference Invite Email template language is also changed.

- **Set Conference Time Zone**

To avoid confusion when inviting conference attendees from different or multiple time zones, Phase 2 allows the user to set the local time zone for the conference. This ensures that when attendees add the conference to their calendar they are saving the correct time.

- **Enhanced Member Kick**

In Phase 1 if a user was kicked out of the conference they were unable to re-join. Phase 2 now allows two options when kicking a member: Keep and Clear. Keep means that the member kicked out cannot log back in to the conference, and is the default option. Clear means that when a member is kicked out they are able to call back in and log in to the conference. This is a system-wide option that affects all conferences and cannot be changed for individual conferences or during a conference.

- **Station Search During Conference Creation**

When creating a conference through the web interface users can now search for and add any station in the system without the technician first having to program the list of valid members.

- **Conference Email With Sender Address**

Phase 2 has added the ability to specify a user's "from" address in the conference invitation email. This ensures that attendees can reply to the invitation with any comments or questions without having to write a new email.

- **View Conference Card Port Status**

Technicians may now view the status of Conference Card ports through the Device Manager.

- **Daylight Savings Time Support**

The system will now automatically adjust the time on conference invitation emails to account for Daylight Savings Time based on the current time zone and Daylight Savings date list.

- **Schedule Recurring Conference Reservations**

When creating a conference, users may now set their conference to recur daily or weekly for up to 3 months.

- **Extension Email Address Support**

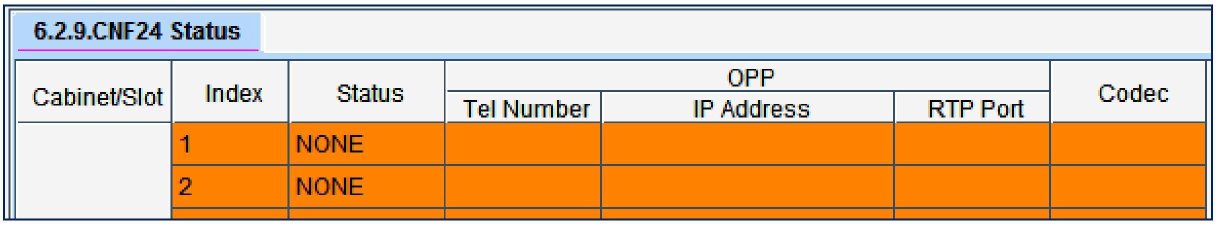
Version 4.60 now allows users to enter their own email address to be used when they are invited to attend a conference. Technicians and system administrators may still enter the list of addresses, but it is now possible for users to add or edit their own information.

CNF24 Module Enhancements (Conference 24 Module)

PROGRAMMING

Two new DM menus have been added and three have been modified to deliver the new set of features with v4.60.

- DM **Menu 6.2.9 Conf Status**

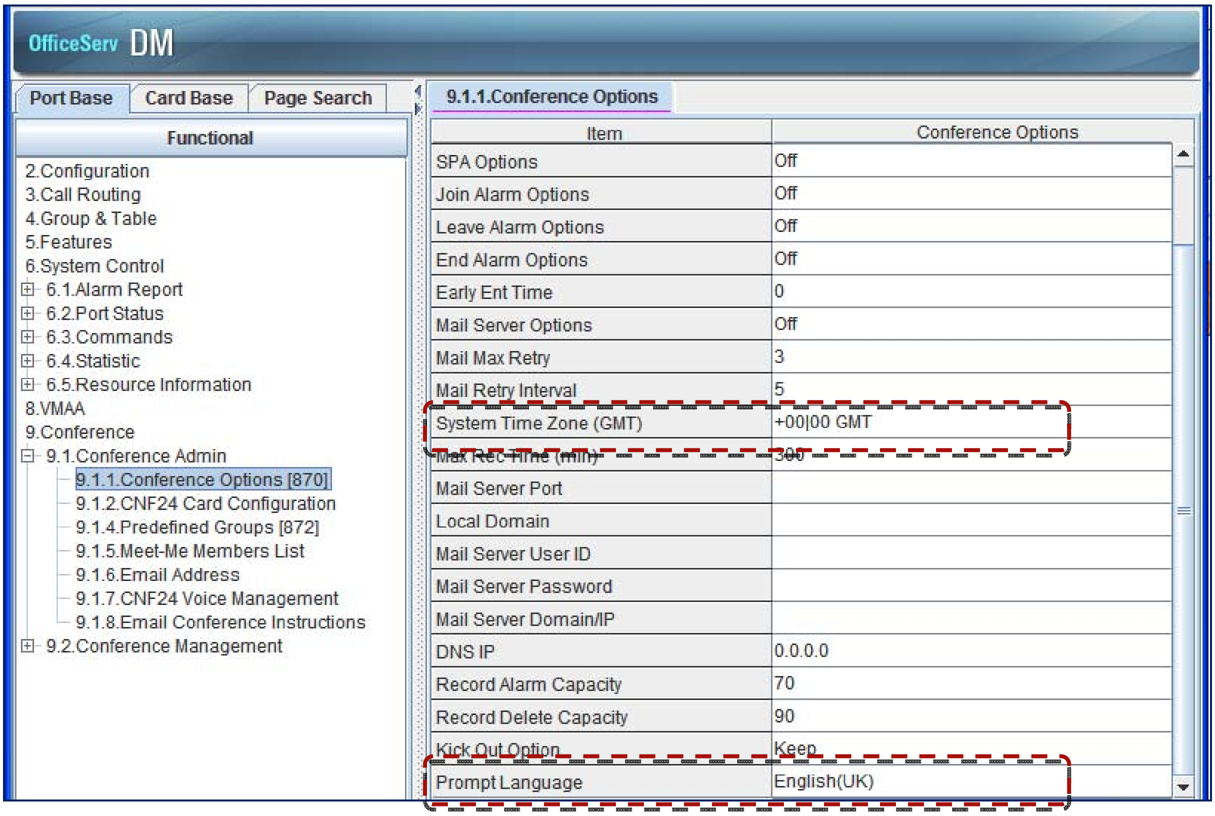


6.2.9.CNF24 Status

Cabinet/Slot	Index	Status	OPP			Codec
			Tel Number	IP Address	RTP Port	
	1	NONE				
	2	NONE				

Here you can view the status of each CNF24 port.

- DM **Menu 9.1.1 Conf Options**

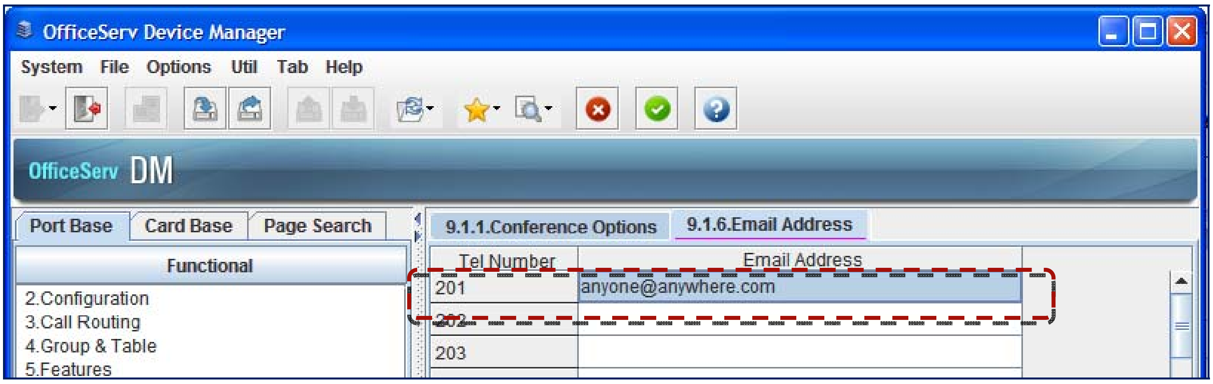


9.1.1.Conference Options

Item	Conference Options
SPA Options	Off
Join Alarm Options	Off
Leave Alarm Options	Off
End Alarm Options	Off
Early Ent Time	0
Mail Server Options	Off
Mail Max Retry	3
Mail Retry Interval	5
System Time Zone (GMT)	+00|00 GMT
Max Rec Time (min)	300
Mail Server Port	
Local Domain	
Mail Server User ID	
Mail Server Password	
Mail Server Domain/IP	
DNS IP	0.0.0.0
Record Alarm Capacity	70
Record Delete Capacity	90
Kick Out Option	Keep
Prompt Language	English(UK)

Here you can set the time zone and prompt language for the CNF24 module.

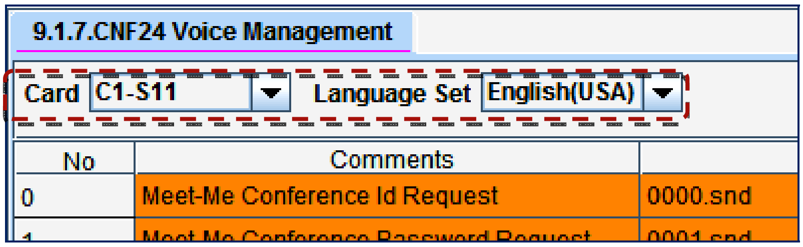
- DM **Menu 9.1.6 Email Address**



Tel Number	Email Address
201	anyone@anywhere.com
202	
203	

Here you can set each CNF24 user's email address. This address is the default recipient's address used to receive conference invites.

- DM **Menu 9.1.7 CNF24 Voice Management**

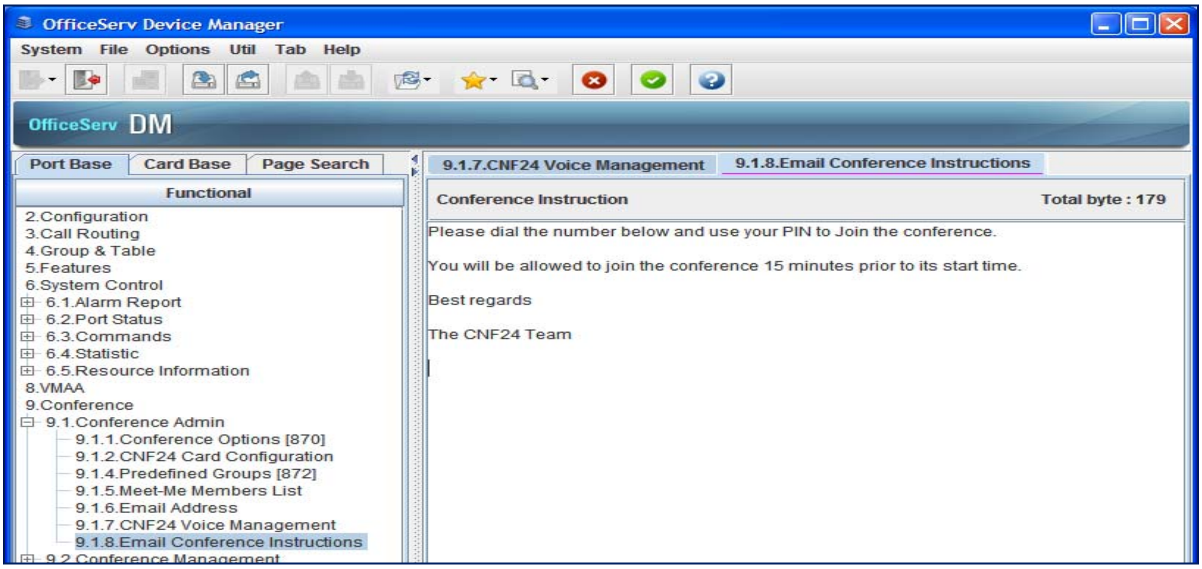


Card C1-S11 Language Set English(USA)

No	Comments	
0	Meet-Me Conference Id Request	0000.snd
1	Meet-Me Conference Password Request	0001.snd

Here you can set the default language used for voice prompts on each CNF24 module.

- DM **Menu 9.1.8 Email Conf Instructions**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
6.System Control
6.1.Alarm Report
6.2.Port Status
6.3.Commands
6.4.Statistic
6.5.Resource Information
8.VMAA
9.Conference
9.1.Conference Admin
9.1.1.Conference Options [870]
9.1.2.CNF24 Card Configuration
9.1.4.Predefined Groups [872]
9.1.5.Meet-Me Members List
9.1.6.Email Address
9.1.7.CNF24 Voice Management
9.1.8.Email Conference Instructions
9.2.Conference Management
9.1.7.CNF24 Voice Management
9.1.8.Email Conference Instructions

Conference Instruction Total byte : 179

Please dial the number below and use your PIN to Join the conference.

You will be allowed to join the conference 15 minutes prior to its start time.

Best regards

The CNF24 Team

Here you can enter some free text, which will be sent with every invite.

SIP Extension DTMF & H.264 Support

GENERAL DESCRIPTION

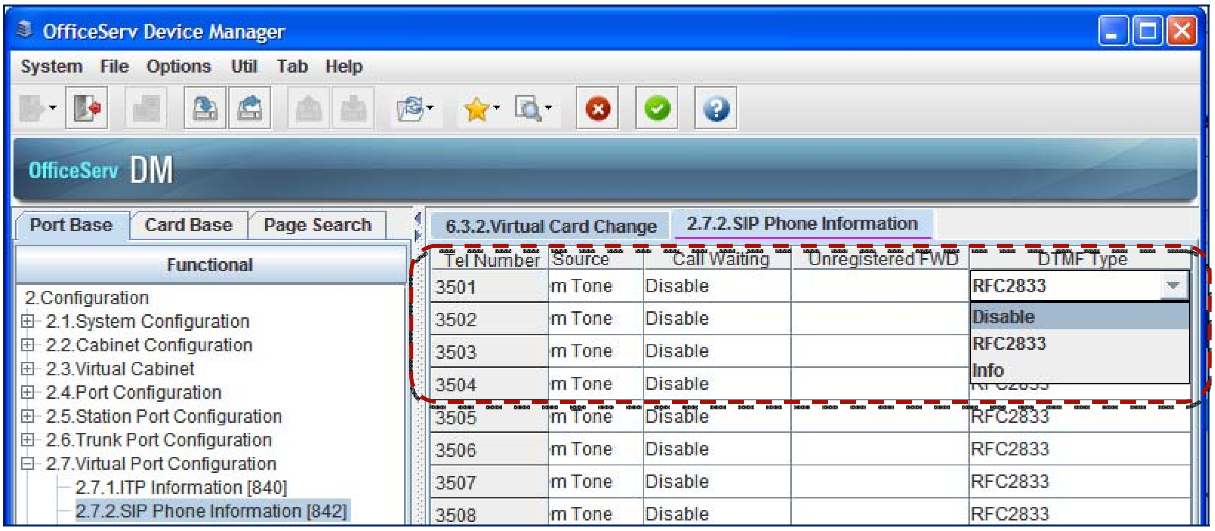
As SIP extensions and services are a growing part of IP PBX connectivity, V4.60 delivers two new features for 3rd party SIP extension devices.

1. **DTMF** support during calls – this allows DTMF to be sent to a SIP device during a call, which is particularly useful where a SIP door phone for example is connected to the system.
    - V4.60 can support both DTMF protocols in SIP: **RFC2833** or the **INFO** method
2. **H.264** Video Codec support – this codec is a video codec and allows 3rd party SIP devices that support this codec to establish video calls when connected as a SIP extension to the OfficeServ.

SIP Extension DTMF & H.264 Support

PROGRAMMING

- DM **Menu 2.7.2 SIP Phone Info**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
2.1.System Configuration
2.2.Cabinet Configuration
2.3.Virtual Cabinet
2.4.Port Configuration
2.5.Station Port Configuration
2.6.Trunk Port Configuration
2.7.Virtual Port Configuration
2.7.1.ITP Information [840]
2.7.2.SIP Phone Information [842]
6.3.2.Virtual Card Change
2.7.2.SIP Phone Information
Disable
RFC2833
Info

Tel Number	Source	Call Waiting	Unregistered FWD	DTMF Type
3501	m Tone	Disable		RFC2833
3502	m Tone	Disable		
3503	m Tone	Disable		
3504	m Tone	Disable		
3505	m Tone	Disable		RFC2833
3506	m Tone	Disable		RFC2833
3507	m Tone	Disable		RFC2833
3508	m Tone	Disable		RFC2833

Here you can assign the type of DTMF protocol used per SIP device.

There are no programming changes to make for the video codec H.264.

DDI Max Call per Ring Plan

GENERAL DESCRIPTION

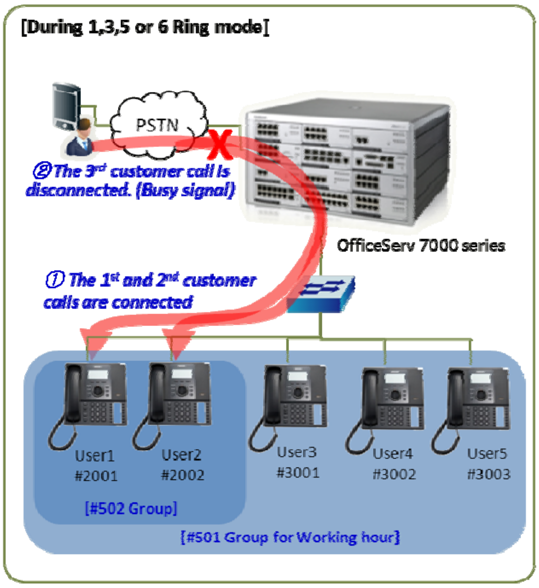
The OfficeServ's DDI and Ring Plan management has been advanced greatly by allowing the ability to assign maximum call counts per DDI per Ring Plan.

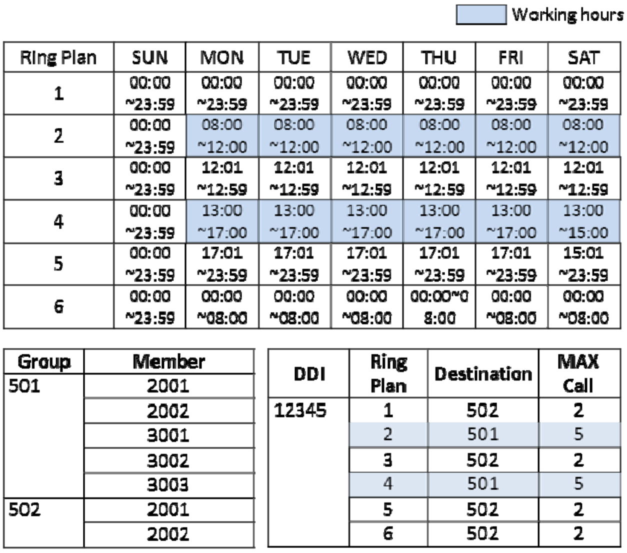
This is particularly important where a customer needs to restrict the volume of incoming traffic on a particular DDI during certain working hours – *for example during lunch time there may be a reduced number of staff available to answer calls at sales or order desks.*

The above scenario is a much requested function by doctorssurgeriesand health centres.

So for example, a Doctors surgery appointment line that has five staff members during the morning and only three during lunch time can have a Ring Plan for lunch time that restricts the volume of allowed calls on that DDI to three calls only. Calls four, five, six and so on will either receive busy tone.

1 - SAMPLE DDI MAX COUNT SCENARIO


[During 1,3,5 or 6 Ring mode]
PSTN
② The 3rd customer call is disconnected. (Busy signal)
OfficeServ 7000 series
① The 1st and 2nd customer calls are connected
User1 #2001
User2 #2002
User3 #3001
User4 #3002
User5 #3003
[#502 Group]
[#501 Group for Working hour]



▨ Working hours

Ring Plan	SUN	MON	TUE	WED	THU	FRI	SAT
1	00:00 ~23:59	00:00 ~23:59	00:00 ~23:59	00:00 ~23:59	00:00 ~23:59	00:00 ~23:59	00:00 ~23:59
2	00:00 ~23:59	08:00 ~12:00	08:00 ~12:00	08:00 ~12:00	08:00 ~12:00	08:00 ~12:00	08:00 ~12:00
3	00:00 ~23:59	12:01 ~12:59	12:01 ~12:59	12:01 ~12:59	12:01 ~12:59	12:01 ~12:59	12:01 ~12:59
4	00:00 ~23:59	13:00 ~17:00	13:00 ~17:00	13:00 ~17:00	13:00 ~17:00	13:00 ~17:00	13:00 ~15:00
5	00:00 ~23:59	17:01 ~23:59	17:01 ~23:59	17:01 ~23:59	17:01 ~23:59	17:01 ~23:59	15:01 ~23:59
6	00:00 ~23:59	00:00 ~08:00	00:00 ~08:00	00:00 ~08:00	00:00~0 8:00	00:00 ~08:00	00:00 ~08:00

Group	Member
501	2001
	2002
	3001
	3002
	3003
502	2001
	2002

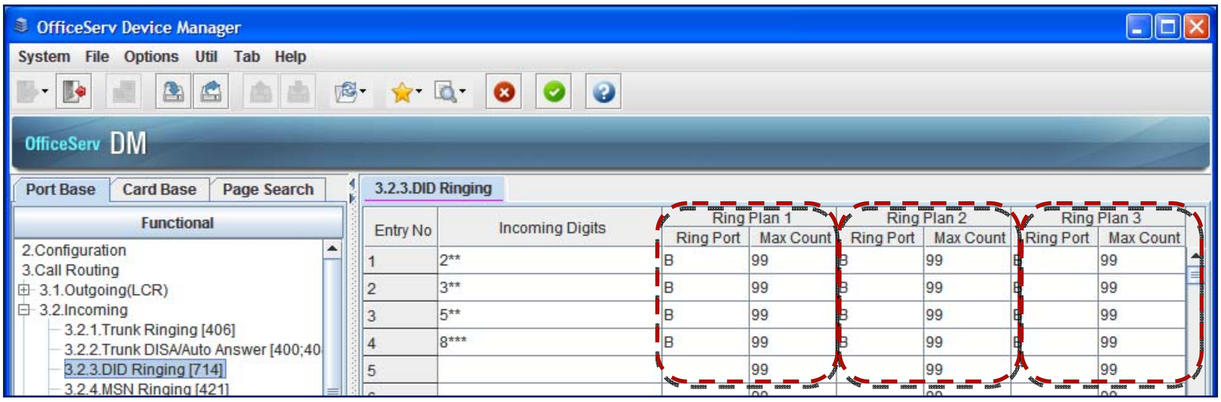
DDI	Ring Plan	Destination	MAX Call
12345	1	502	2
	2	501	5
	3	502	2
	4	501	5
	5	502	2
	6	502	2

DDI Max Call per Ring Plan

PROGRAMMING

DM menu 3.2.3 DDI Ringing has been modified to deliver the new Max Call Per DDI per Ring Plan feature.

- DM **Menu 3.2.3 DDI Ringing**



Entry No	Incoming Digits	Ring Plan 1		Ring Plan 2		Ring Plan 3	
		Ring Port	Max Count	Ring Port	Max Count	Ring Port	Max Count
1	2**	B	99	B	99	B	99
2	3**	B	99	B	99	B	99
3	5**	B	99	B	99	B	99
4	8***	B	99	B	99	B	99
5			99		99		99

Here you can set the Max Count of calls per DDI per Ring Plan.

The default value is 99 for each DDI/RP.

Max Call in Queue Feature (enhanced UCD feature)

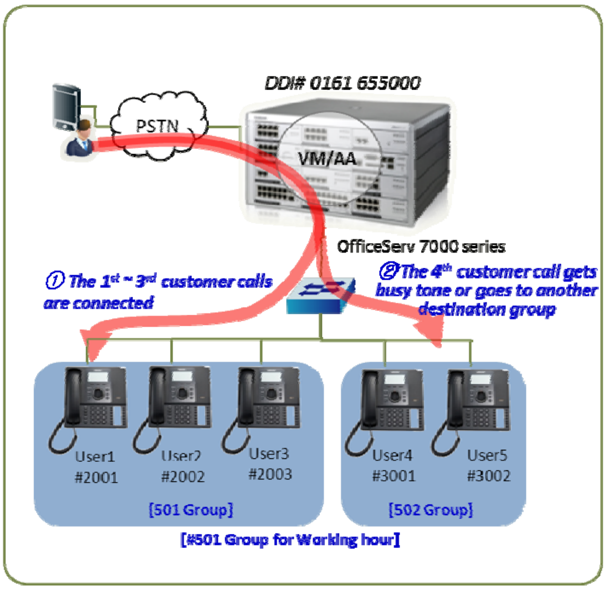
GENERAL DESCRIPTION

Another incoming call volume restriction that is required in the doctor surgery and health centre environment is the ability to restrict the amount of calls that can be queued at a UCD group.

This feature differs from the Max DDI count feature because it is instigated after the call has been answered by the system (either by Auto Attendant or a user).

This can also be useful in small contact centres where a maximum of calls that can queue to a particular group can be set. Once this maximum is met, any subsequent calls to that UCD group can be rerouted to another department, staff member or AA/VM menu or mailbox.

2 - MAX CALLS IN QUEUE FEATURE SAMPLE SCENARIO


DDI# 0161 655000
PSTN
VM/AA
OfficeServ 7000 series
① The 1st ~ 3rd customer calls are connected
② The 4th customer call gets busy tone or goes to another destination group
User1 #2001
User2 #2002
User3 #2003
User4 #3001
User5 #3002
[501 Group]
[502 Group]
[#501 Group for Working hour]

Group	Member
501	2001
	2002
	2003
502	3001
	3002

UCD Group	501
MAX call Count	3
MAX call destination	502

↑
Max call in queue function (MMC 607 UCD Options)

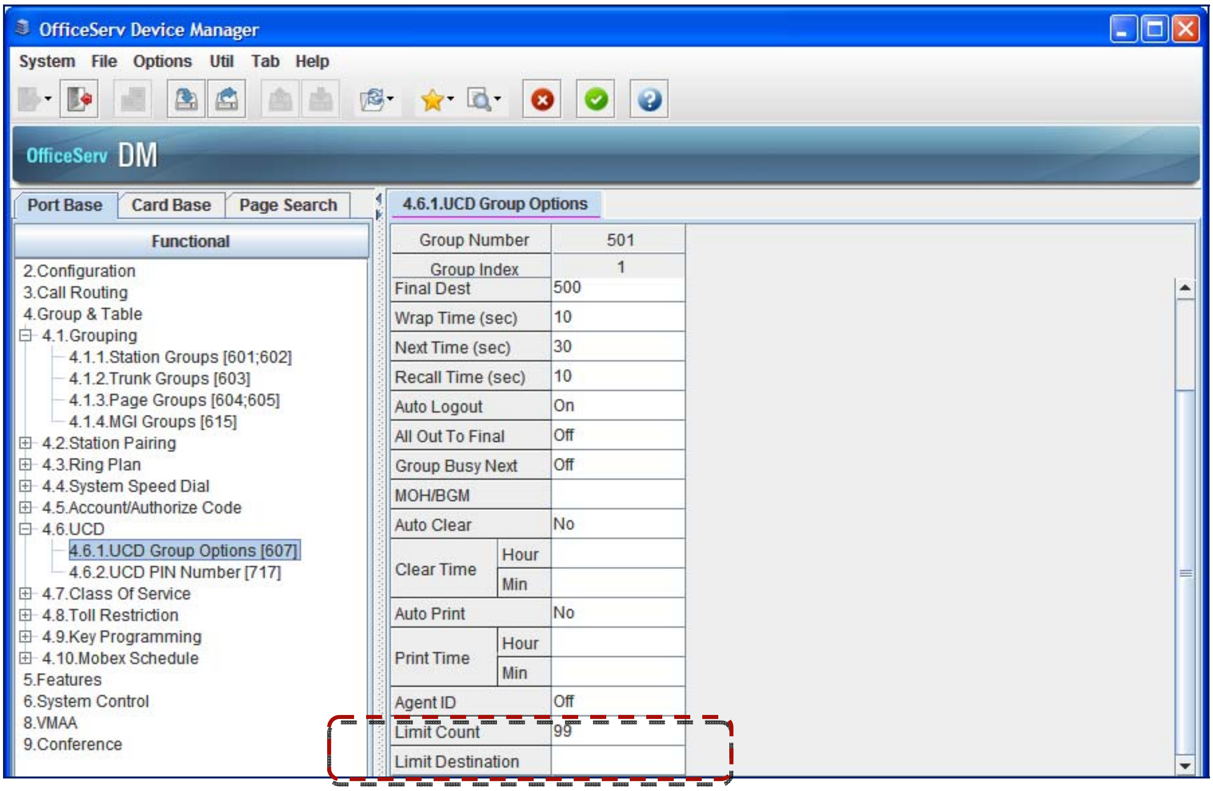
SCENARIO

1. Customer has just one main DDI number (e.g. 0161 655000)
2. This DDI is answered by the VM/AA and the caller has options to press - (1) to book an appointment
3. When (1) is selected, they are transferred to a UCD group with 3 members (group 501)
4. If "Max Call" is set to "3", only 3 calls will be transferred to group 501, the 4th, 5th ~ calls will get busy tone, or go to another group 502.

Max Call in Queue Feature (enhanced UCD feature)

PROGRAMMING

- DM **Menu 4.6.1 UCD Options**



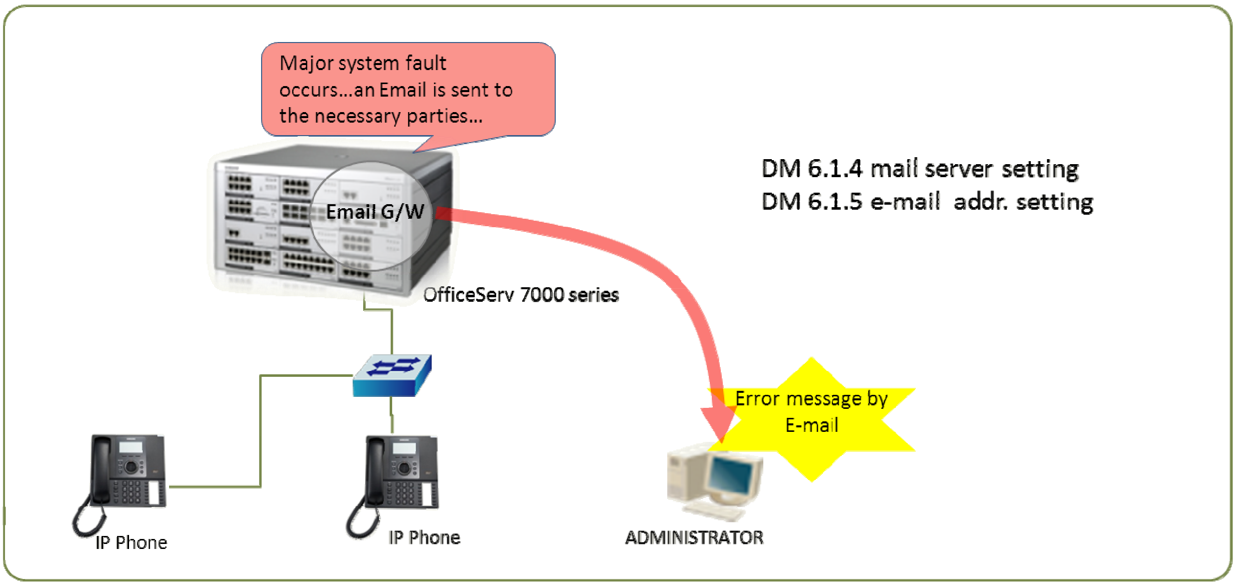
Group Number		501
Group Index		1
Final Dest		500
Wrap Time (sec)		10
Next Time (sec)		30
Recall Time (sec)		10
Auto Logout		On
All Out To Final		Off
Group Busy Next		Off
MOH/BGM		
Auto Clear		No
Clear Time	Hour	
	Min	
Auto Print		No
Print Time	Hour	
	Min	
Agent ID		Off
Limit Count		99
Limit Destination		

Here you can assign the maximum limit count of calls allowed to queue and the destination of for calls over the limit to be rerouted to – per UCD group.

Major System Alarm and Fault Reporting by Email

GENERAL DESCRIPTION

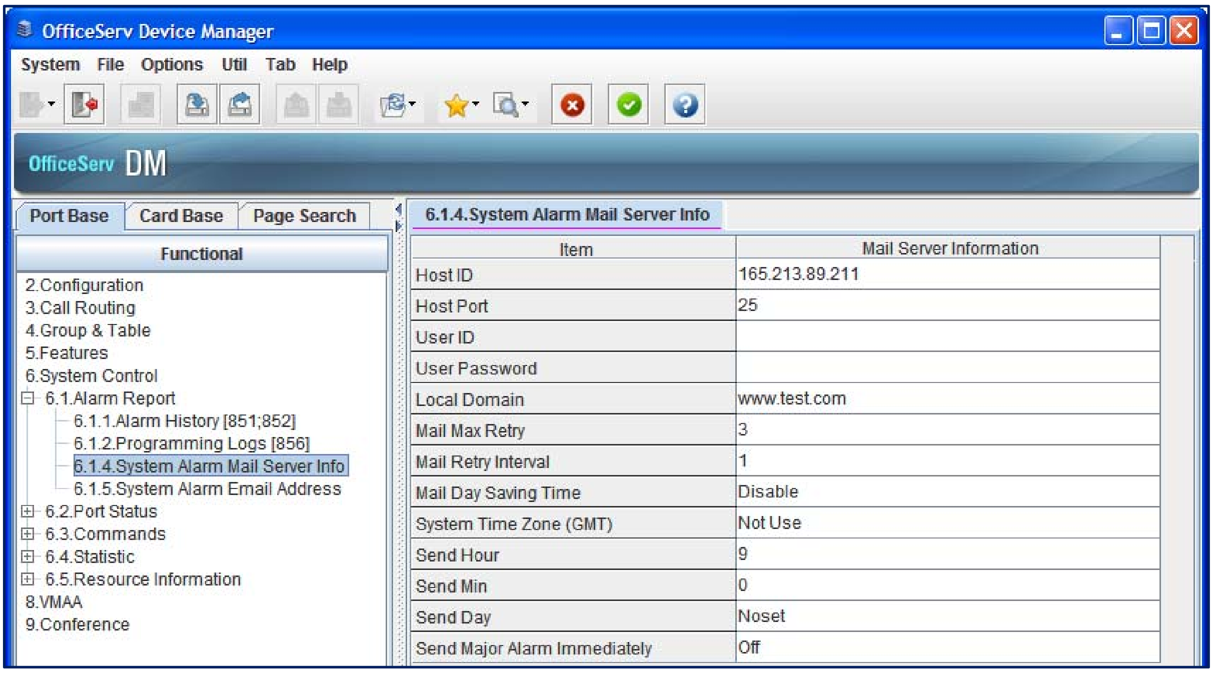
To further enhance the fault and alarm management on the OfficeServ, V4.60 enables system administrators and maintenance staff to receive Emails when a major system fault or alarm occurs. Up to four Email addresses can be registered to receive the alarm notifications.


Major system fault occurs...an Email is sent to the necessary parties...
Email G/W
OfficeServ 7000 series
DM 6.1.4 mail server setting
DM 6.1.5 e-mail addr. setting
Error message by E-mail
IP Phone
IP Phone
ADMINISTRATOR

Major System Alarm and Fault Reporting by Email

PROGRAMMING

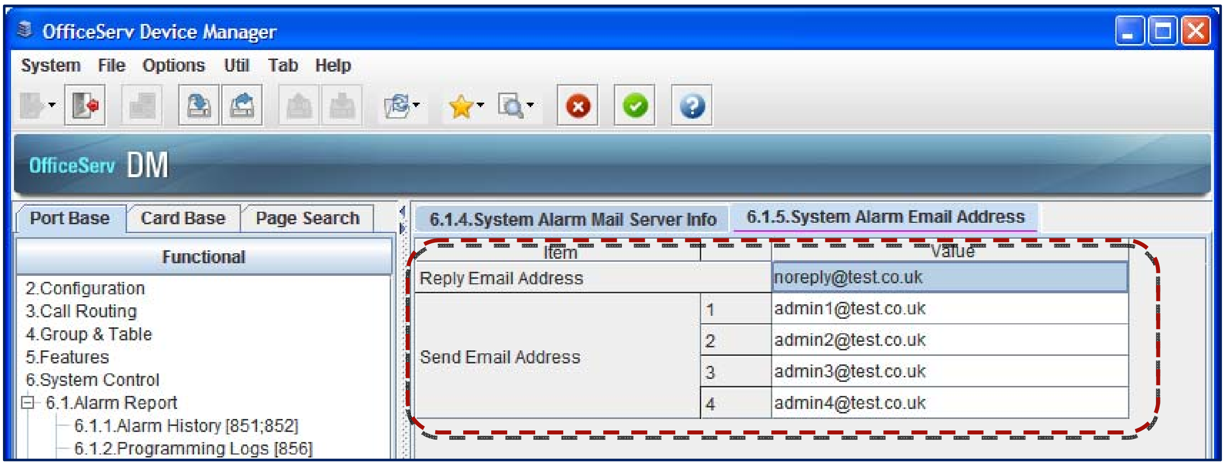
- DM **Menu 6.1.4 System Alarm Mail Server Info**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base Card Base Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
6.System Control
6.1.Alarm Report
6.1.1.Alarm History [851;852]
6.1.2.Programming Logs [856]
6.1.4.System Alarm Mail Server Info
6.1.5.System Alarm Email Address
6.2.Port Status
6.3.Commands
6.4.Statistic
6.5.Resource Information
8.VMAA
9.Conference
6.1.4.System Alarm Mail Server Info

Item	Mail Server Information
Host ID	165.213.89.211
Host Port	25
User ID	
User Password	
Local Domain	www.test.com
Mail Max Retry	3
Mail Retry Interval	1
Mail Day Saving Time	Disable
System Time Zone (GMT)	Not Use
Send Hour	9
Send Min	0
Send Day	Noset
Send Major Alarm Immediately	Off

FIELD	PURPOSE
Host ID	Sets the **IP address** or **DNS name** of the mail server
Host Port	Sets the **TCP port** to use to talk to the mail server (typically port **25**)
User ID	Sets the **login ID**, if any, used to log in to the mail server
User Password	Sets the **password** for the above **User ID**
Local Domain	Sets the **domain name** to use when logging in to the mail server, if necessary
Mail Max Retry	Set the **number of times** the system will attempt to resend the message upon failure
Mail Retry Interval	Sets the **time to wait** between retry attempts
Mail Day Saving Time	Determine if the system will adjust the email time stamp for **Daylight Savings Time** or not
System Time Zone (GMT)	Sets the **time zone** of the system based on the offset from **Greenwich Mean Time** (**GMT**)
Send Hour / Send Min	Sets the **time of day** alarm emails should be sent
Send Day	Sets whether emails should send **daily** or only **on demand**
Send Major Alarm Immediately	Determine if major alarms will generate an email **immediately** or if they will be sent along with the **normally scheduled report**

- DM **Menu 6.1.5 System Alarm Email Address**


OfficeServ Device Manager
System File Options Util Tab Help
OfficeServ DM
Port Base
Card Base
Page Search
Functional
2.Configuration
3.Call Routing
4.Group & Table
5.Features
6.System Control
6.1.Alarm Report
6.1.1.Alarm History [851;852]
6.1.2.Programming Logs [856]
6.1.4.System Alarm Mail Server Info
6.1.5.System Alarm Email Address

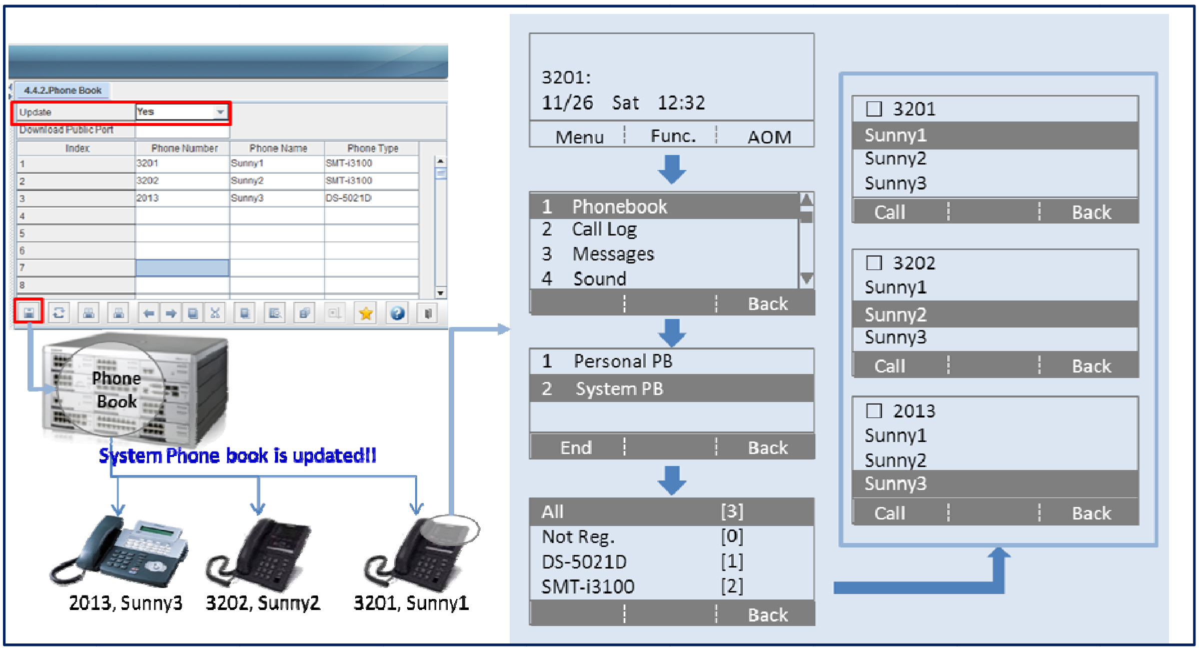
Item		Value
Reply Email Address		noreply@test.co.uk
Send Email Address	1	admin1@test.co.uk
	2	admin2@test.co.uk
	3	admin3@test.co.uk
	4	admin4@test.co.uk

FIELD	PURPOSE
Reply Email Address	Sets the “**from**” address of the alarm email
Send Email Address 1~ 4	Sets up to **four email addresses** the alarm email will be sent to

IP Phone Phonebook Download

GENERAL DESCRIPTION

A central Phonebook can now be held on the system, updated centrally and then pushed to any SMT IP phones on the network. Upto 100 phonebook entries can be stored.



4.4.2.Phone Book

Update: Yes

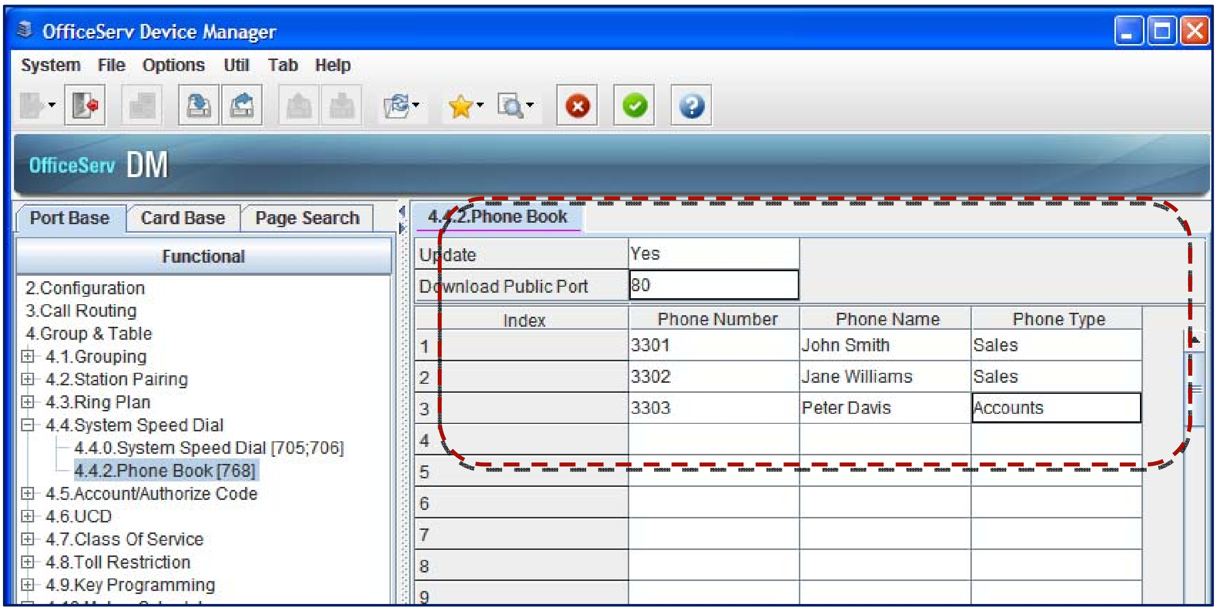
Download Public Port

Index	Phone Number	Phone Name	Phone Type
1	3201	Sunny1	SMT-i3100
2	3202	Sunny2	SMT-i3100
3	2013	Sunny3	DS-5021D
4			
5			
6			
7			
8			

IP Phone Phonebook Download

PROGRAMMING

- DM **Menu 4.4.2 Phonebook**



Update	Yes
Download Public Port	80

	Index	Phone Number	Phone Name	Phone Type
1		3301	John Smith	Sales
2		3302	Jane Williams	Sales
3		3303	Peter Davis	Accounts
4				
5				
6				
7				
8				
9				

FIELD	PURPOSE
Update	Set to Yes to push the updated phonebook to all connected SMT-I phones.
Download Public Port	Sets the HTTP port the system will use to download the phonebook to the remote location on the public network. System use HTTP port 80 for the local SMT-I phones.
Phone Number	Sets the phonebook entry's phone number
Phone Name	Sets the name to associate with the phonebook entry's phone number
Phone Type	Sets the phone book category to associate with the phonebook entry's phone number (such as "Sales" or "Marketing")

SVMi-20i WAV File Prompt Support

GENERAL DESCRIPTION

To enable quick and professional Auto Attendant and Voicemail prompts to be uploaded, V4.60 and the new SVMi20-i voicemail solution now supports the uploading of standard WAV file.

The SVMi-20i has been enhanced to automatically convert the format of uploaded audio WAV files to the voicemail system. Where an administrator uploads an existing WAV file using theSVMi-20i's VoiceStudio, the SVMi-20i will automatically convert the WAV file to the format required for the SVMi-20i.

⚠

1. *Wav file prompt conversion is supported on the OS7030, 7100 & 7200S with built-in SVM & v4.60 software.*

2. *This enhancement is not supported on the SVMi-20E installed with v4.60 software.*

3. *The SVi-20i only supports one wav file format (8kHz, mono, 16 bit signed, 128kps).*

New System Management Tool – Device Manager (DM)

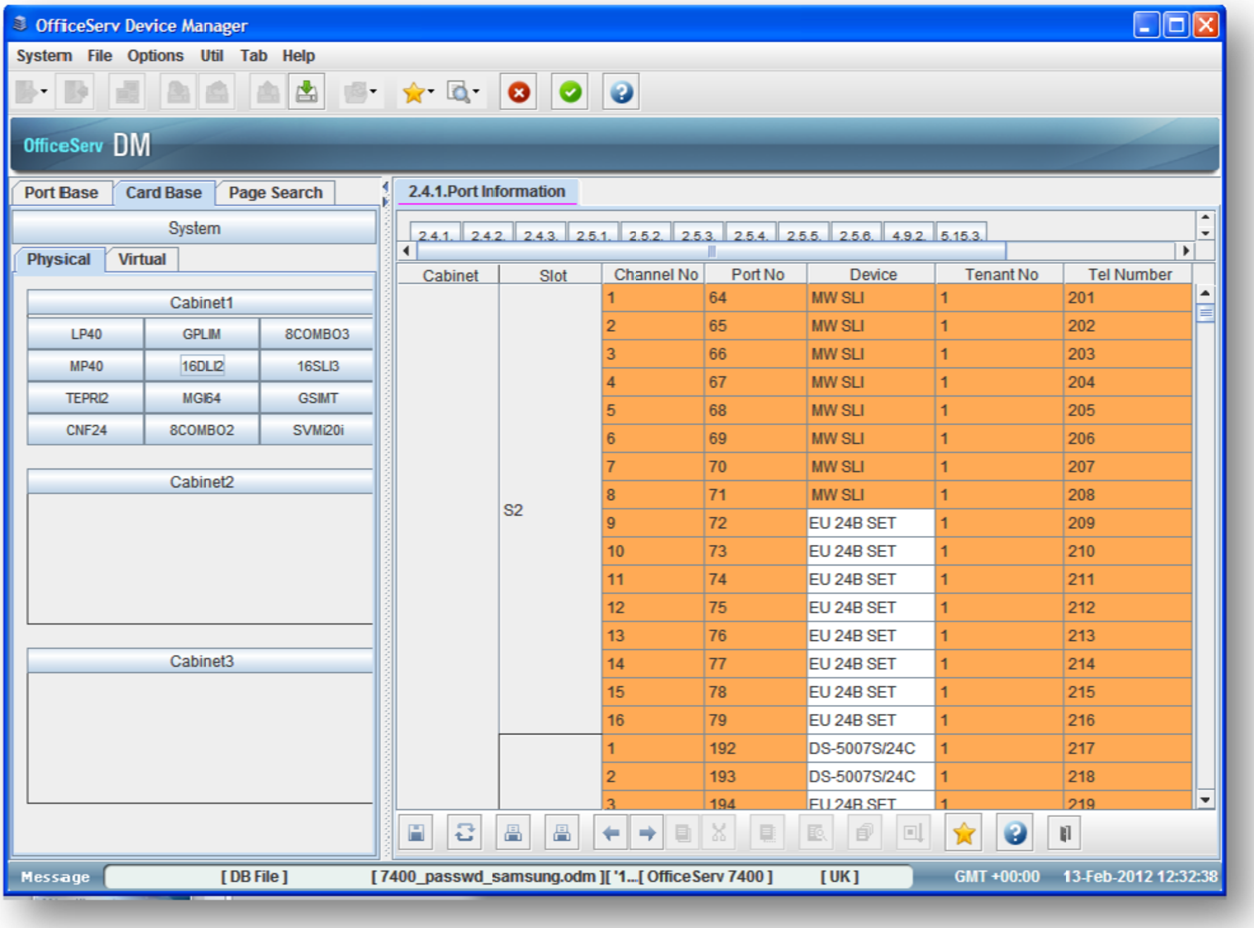
GENERAL DESCRIPTION

The need to be able to administer, program and manage the OfficeServ from any Windows device via a Web Browser is now even more of a necessity.

Prior to V4.60, IT Tool was required to be installed on the PC that you wanted to access the system from. Version 4.60 brings a new tool that is browser based – Device Manager or DM as its known is a new way of accessing and programming the OfficeServ series of IP PBXs.

DM can be used to program the main system, the SVMi-20i and the CNF24 conference module.

Also, DM delivers the latest in security for Web access. Every OfficeServ system with V4.60 now contains an embedded Web Server to allow DM to connect. The very latest versions of Apache Web Server and PHP engines have been included in V4.60.



Cabinet	Slot	Channel No	Port No	Device	Tenant No	Tel Number
	S2	1	64	MW SLI	1	201
		2	65	MW SLI	1	202
		3	66	MW SLI	1	203
		4	67	MW SLI	1	204
		5	68	MW SLI	1	205
		6	69	MW SLI	1	206
		7	70	MW SLI	1	207
		8	71	MW SLI	1	208
		9	72	EU 24B SET	1	209
		10	73	EU 24B SET	1	210
		11	74	EU 24B SET	1	211
		12	75	EU 24B SET	1	212
		13	76	EU 24B SET	1	213
		14	77	EU 24B SET	1	214
		15	78	EU 24B SET	1	215
		16	79	EU 24B SET	1	216
		1	192	DS-5007S/24C	1	217
		2	193	DS-5007S/24C	1	218
		3	194	EU 24B SET	1	219

[DB File] [7400_passwd_samsung.odm]['1...[OfficeServ 7400] [UK] GMT +00:00 13-Feb-2012 12:32:38

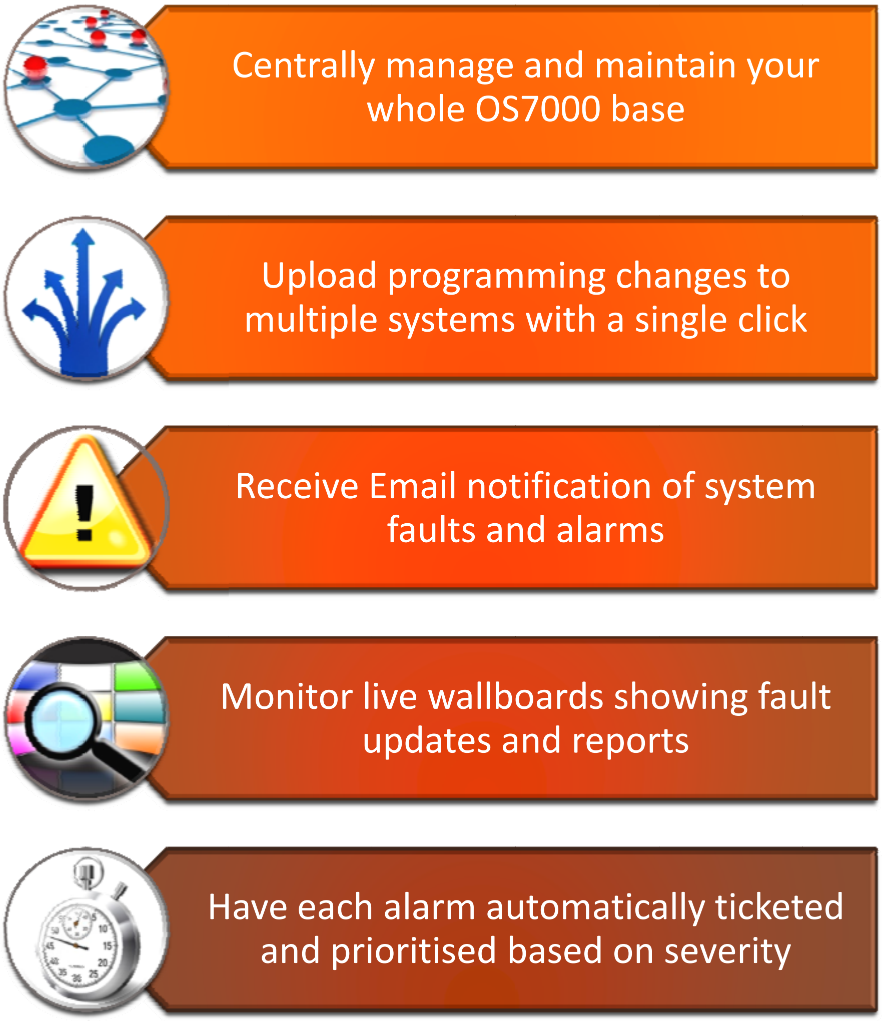
NMS V1.6 (Network Management System)

GENERAL DESCRIPTION

The ability to manage and affect moves and changes to your OfficeServ customer base effectively and efficiently has never been more important.

NMS delivers a multitude of services and benefits to your customers and importantly, your own business by allowing a host of network management tools for the OS7000 series.

V4.60 and NMS V1.6 can create a centralised management and administration centre for upto 10,000 OfficeServ 7000 systems and some of its features and benefits include:



Centrally manage and maintain your whole OS7000 base

Upload programming changes to multiple systems with a single click

Receive Email notification of system faults and alarms

Monitor live wallboards showing fault updates and reports

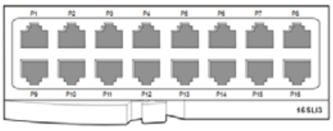
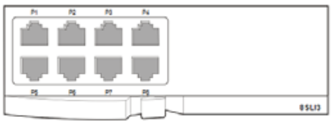
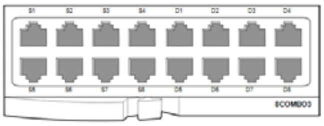
Have each alarm automatically ticketed and prioritised based on severity

New Series of SLI Modules

GENERAL DESCRIPTION

Version 4.60 enables the support of three new station modules, which include some functionssthat were previously only available by using extra daughter modules.

These three new modules are:

Items	16SLI3	8SLI3	8COMBO3
Image			
Description	SLI 16Port	SLI 8Port	SLI 8port + DLI 8port
Features	• Built-in DTMF Receivers • Built-in CID Tx/port • Support for Message Waiting		

The new SLI3 modules deliver functions such as CID that were previously only available via other modules such as the CRM and IRM boards.

Version 4.60 Upgrade Procedures

This section explains all necessary methods and processes you need, when considering an upgrade path for an existing customer that does not have v4.60 installed.

It is important to read and understand the following section, as there are many parts to consider when upgrading to V4.60 from a lower version. It may be a requirement to upgrade several pieces of software including the LCP, LP40 and not just the main processor.

The Customer Database

Upgrading any OfficeServ 7000 to v4.60 will default the database. Therefore it is essential that prior to any upgrade work the current system's database must be backed-up and saved.

Databases built on software versions lower than V4.60 cannot be just uploaded straight into a V4.60 system.

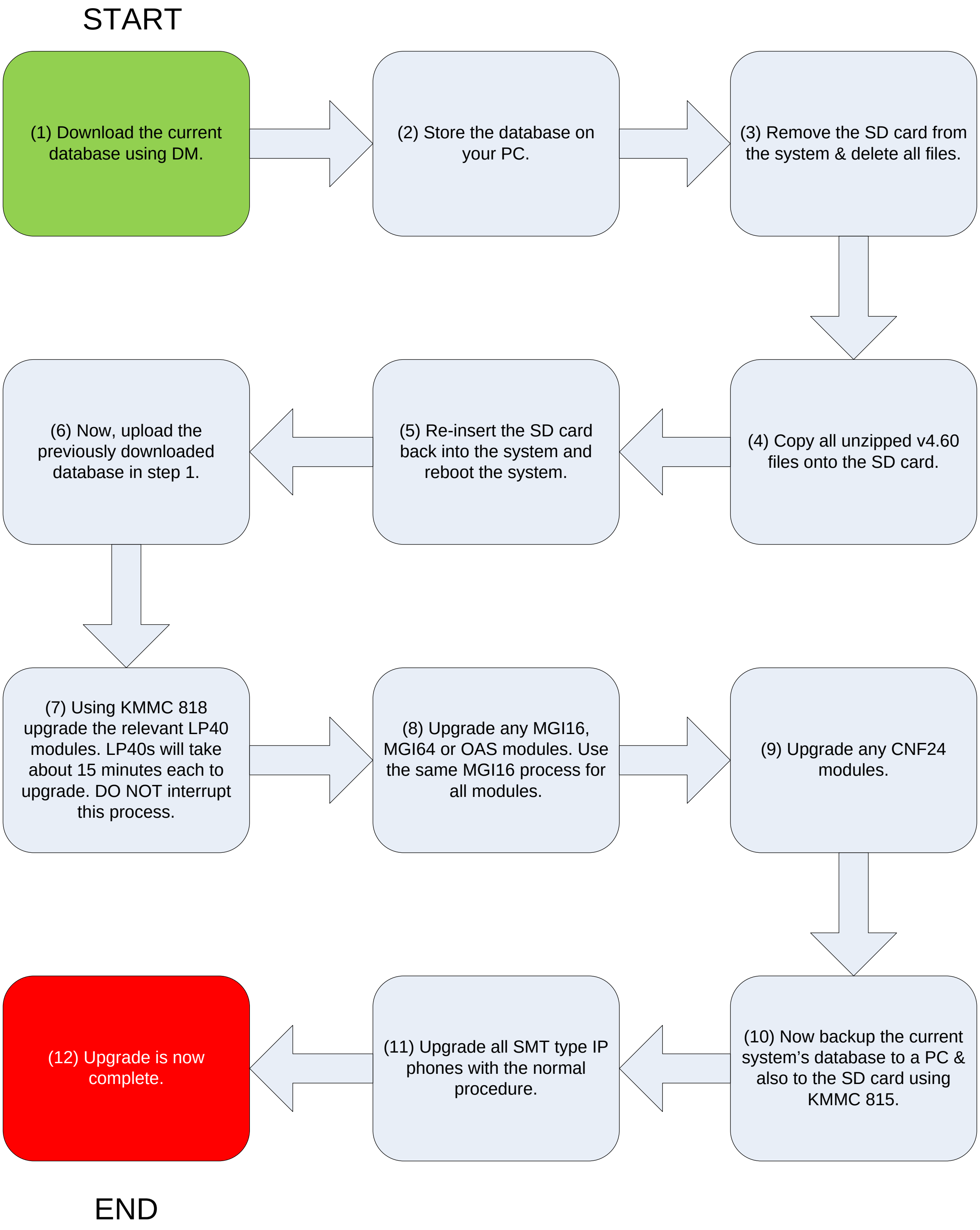
The key difference that you will find with V4.60, when upgrading a 7200 or 7400 system, is the need to upgrade via the SD or storage card, by removing all of the existing files, and replacing with the new unzipped V4.60 files.

Remember, if you've backed up the current database correctly, you can always revert back to the old versions if your upgrade procedure goes wrong or if errors are made during the process.

The following pages will take you through the correct upgrade procedure for each OfficeServ 7000 system. There are some crossover process for each system but please follow the procedure relative to the system that you are working on.

Version 4.60 Upgrade Procedures

UPGRADING THE OFFICESERV7400 (MP40)



START

(1) Download the current database using DM.

(2) Store the database on your PC.

(3) Remove the SD card from the system & delete all files.

(4) Copy all unzipped v4.60 files onto the SD card.

(5) Re-insert the SD card back into the system and reboot the system.

(6) Now, upload the previously downloaded database in step 1.

(7) Using KMMC 818 upgrade the relevant LP40 modules. LP40s will take about 15 minutes each to upgrade. DO NOT interrupt this process.

(8) Upgrade any MGI16, MGI64 or OAS modules. Use the same MGI16 process for all modules.

(9) Upgrade any CNF24 modules.

(10) Now backup the current system's database to a PC & also to the SD card using KMMC 815.

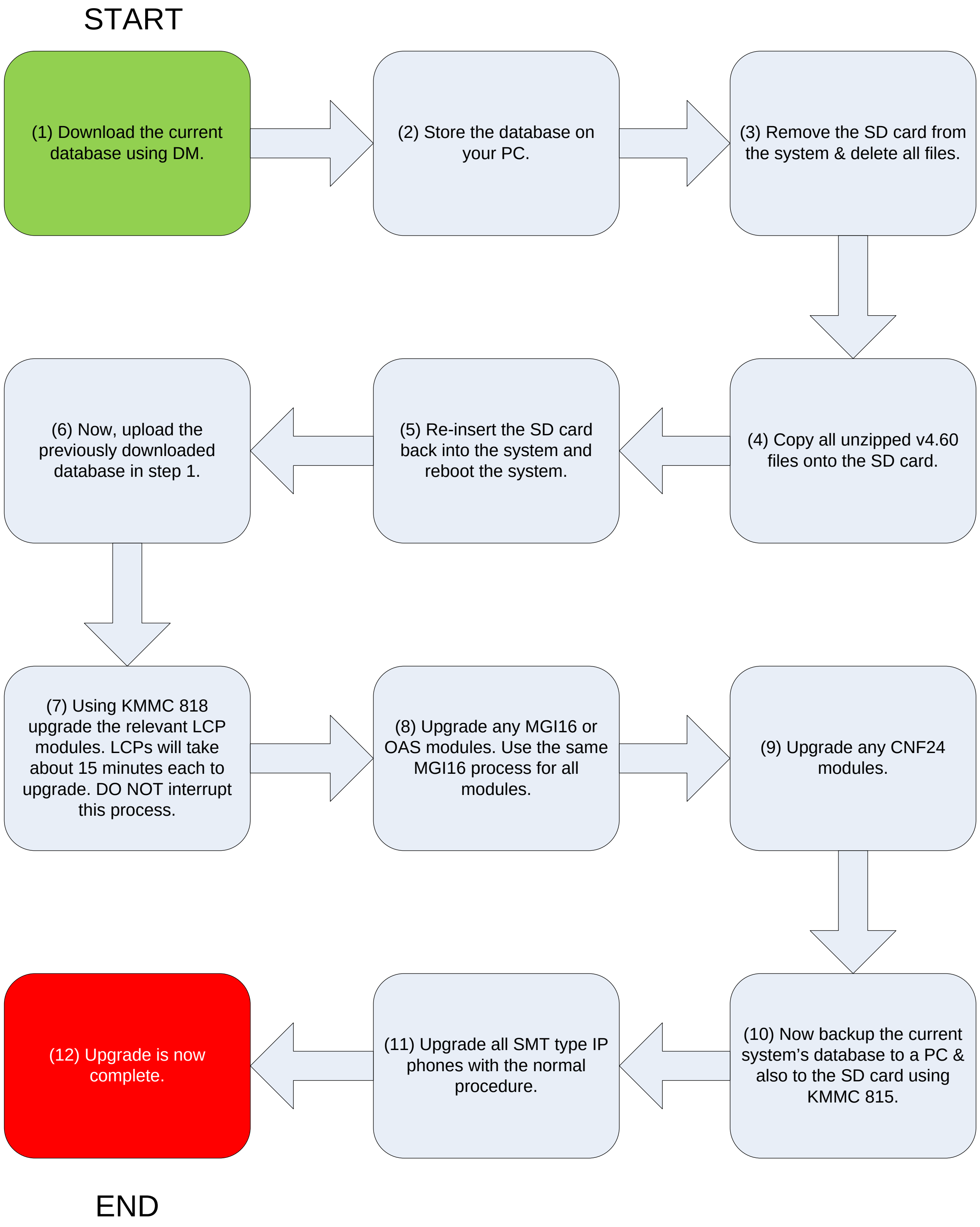
(11) Upgrade all SMT type IP phones with the normal procedure.

(12) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

UPGRADING THE OFFICESERV 7200 (MP20)



START

(1) Download the current database using DM.

(2) Store the database on your PC.

(3) Remove the SD card from the system & delete all files.

(4) Copy all unzipped v4.60 files onto the SD card.

(5) Re-insert the SD card back into the system and reboot the system.

(6) Now, upload the previously downloaded database in step 1.

(7) Using KMMC 818 upgrade the relevant LCP modules. LCPs will take about 15 minutes each to upgrade. DO NOT interrupt this process.

(8) Upgrade any MGI16 or OAS modules. Use the same MGI16 process for all modules.

(9) Upgrade any CNF24 modules.

(10) Now backup the current system's database to a PC & also to the SD card using KMMC 815.

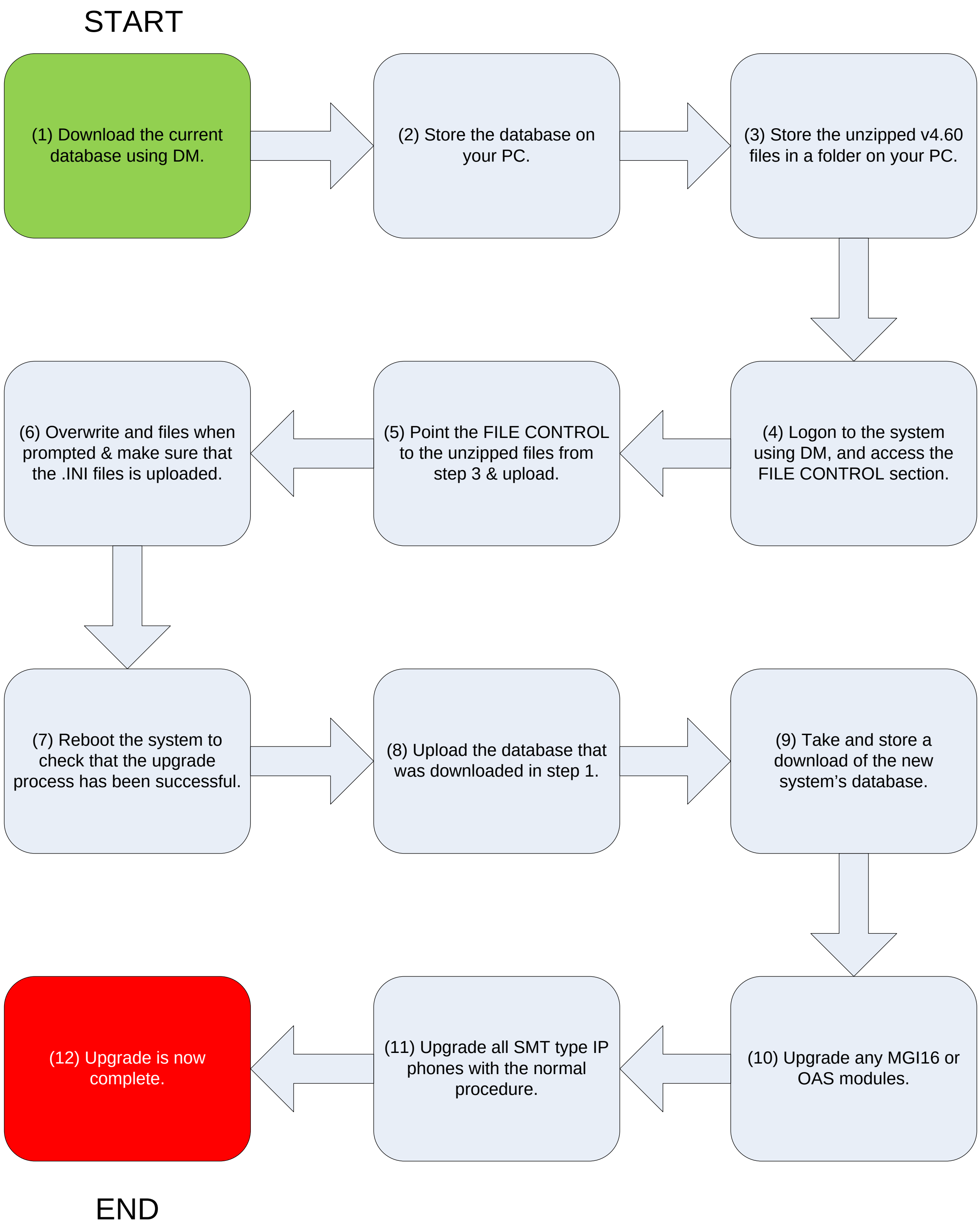
(11) Upgrade all SMT type IP phones with the normal procedure.

(12) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

UPGRADING THE OFFICESERV 7200S (MP20S)



START

(1) Download the current database using DM.

(2) Store the database on your PC.

(3) Store the unzipped v4.60 files in a folder on your PC.

(4) Logon to the system using DM, and access the FILE CONTROL section.

(5) Point the FILE CONTROL to the unzipped files from step 3 & upload.

(6) Overwrite and files when prompted & make sure that the .INI files is uploaded.

(7) Reboot the system to check that the upgrade process has been successful.

(8) Upload the database that was downloaded in step 1.

(9) Take and store a download of the new system’s database.

(10) Upgrade any MGI16 or OAS modules.

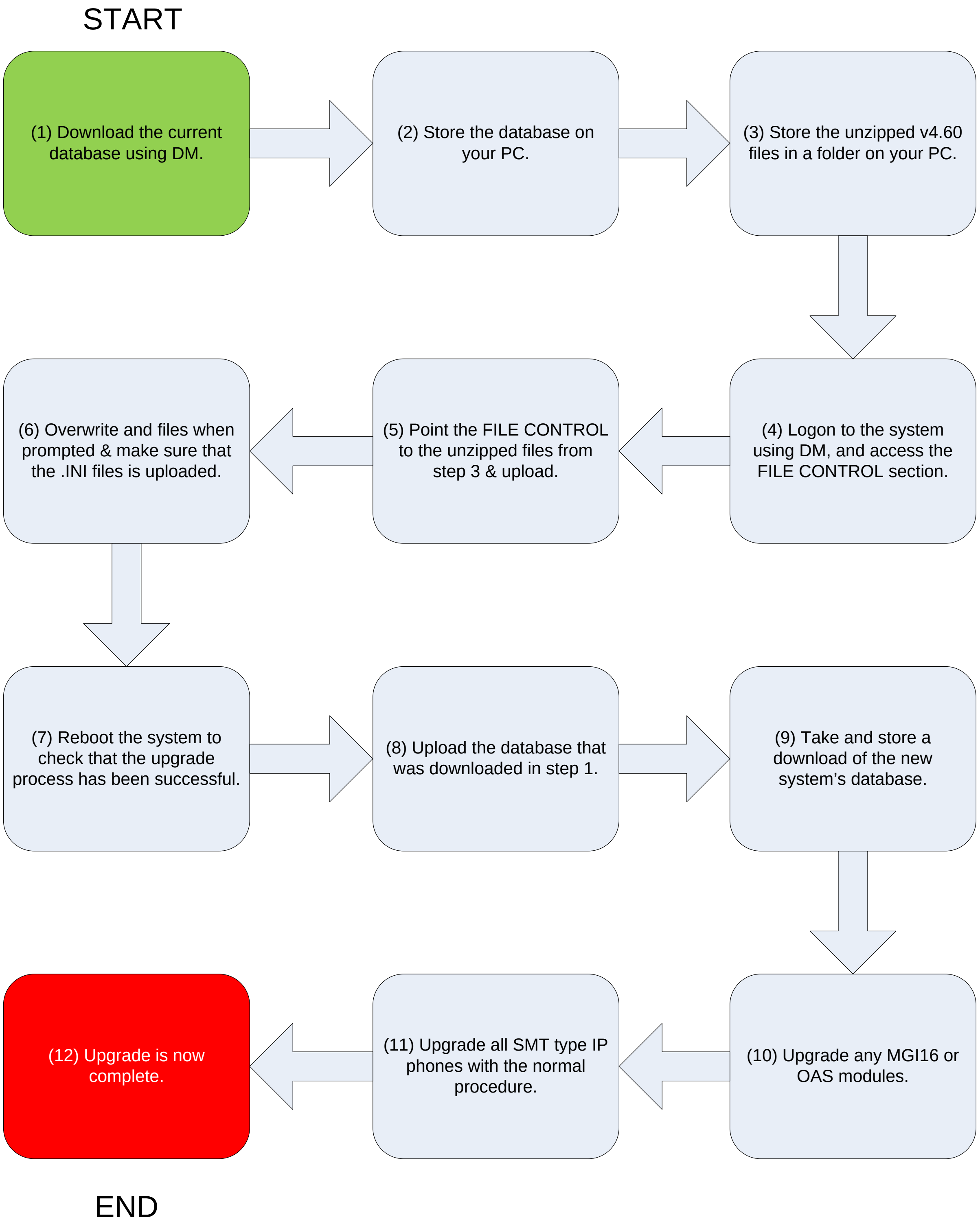
(11) Upgrade all SMT type IP phones with the normal procedure.

(12) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

UPGRADING THE OFFICESERV 7100 (MP10A)



START

(1) Download the current database using DM.

(2) Store the database on your PC.

(3) Store the unzipped v4.60 files in a folder on your PC.

(4) Logon to the system using DM, and access the FILE CONTROL section.

(5) Point the FILE CONTROL to the unzipped files from step 3 & upload.

(6) Overwrite and files when prompted & make sure that the .INI files is uploaded.

(7) Reboot the system to check that the upgrade process has been successful.

(8) Upload the database that was downloaded in step 1.

(9) Take and store a download of the new system's database.

(10) Upgrade any MGI16 or OAS modules.

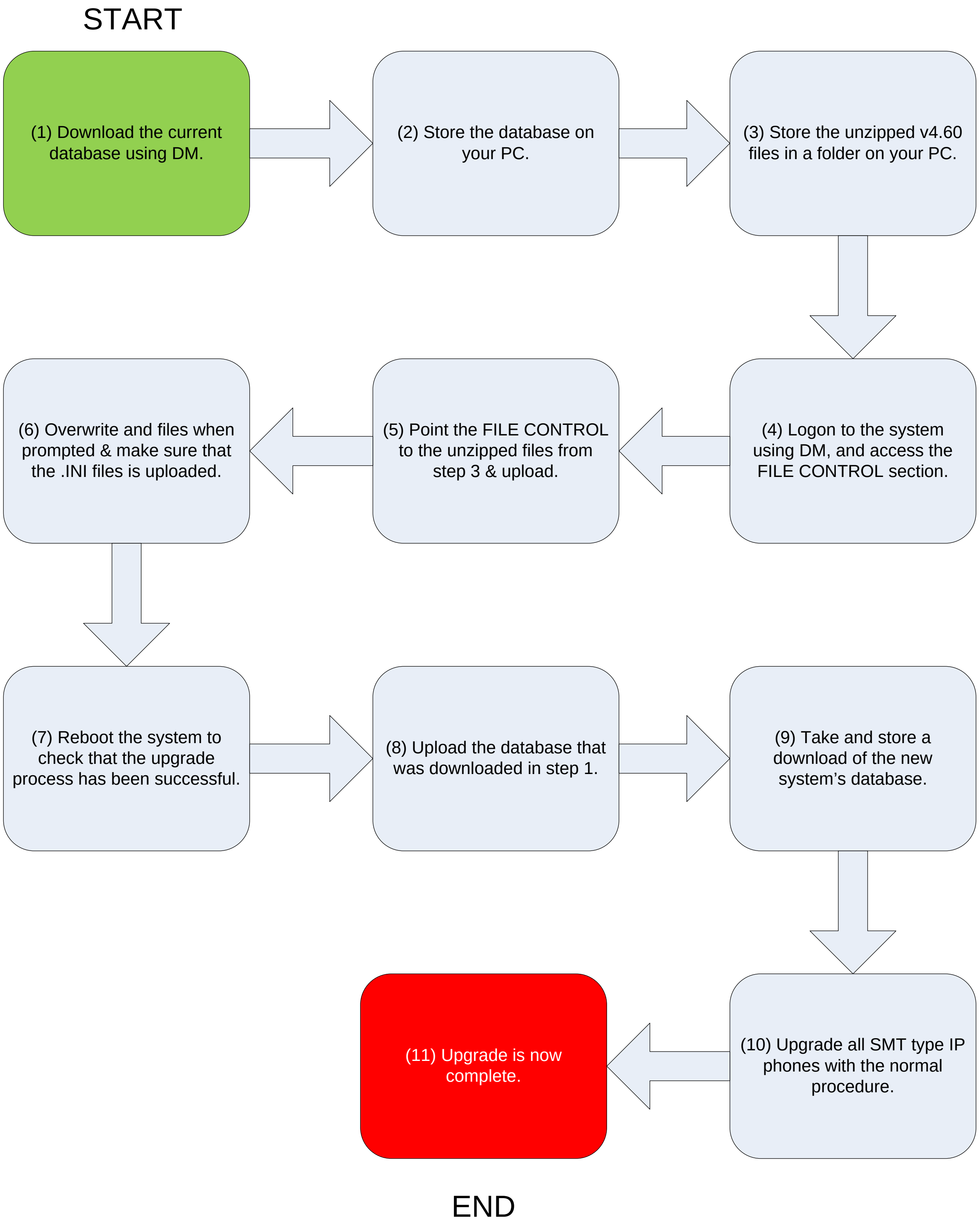
(11) Upgrade all SMT type IP phones with the normal procedure.

(12) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

UPGRADING THE OFFICESERV 7030 (MP03)



START

(1) Download the current database using DM.

(2) Store the database on your PC.

(3) Store the unzipped v4.60 files in a folder on your PC.

(4) Logon to the system using DM, and access the FILE CONTROL section.

(5) Point the FILE CONTROL to the unzipped files from step 3 & upload.

(6) Overwrite and files when prompted & make sure that the .INI files is uploaded.

(7) Reboot the system to check that the upgrade process has been successful.

(8) Upload the database that was downloaded in step 1.

(9) Take and store a download of the new system’s database.

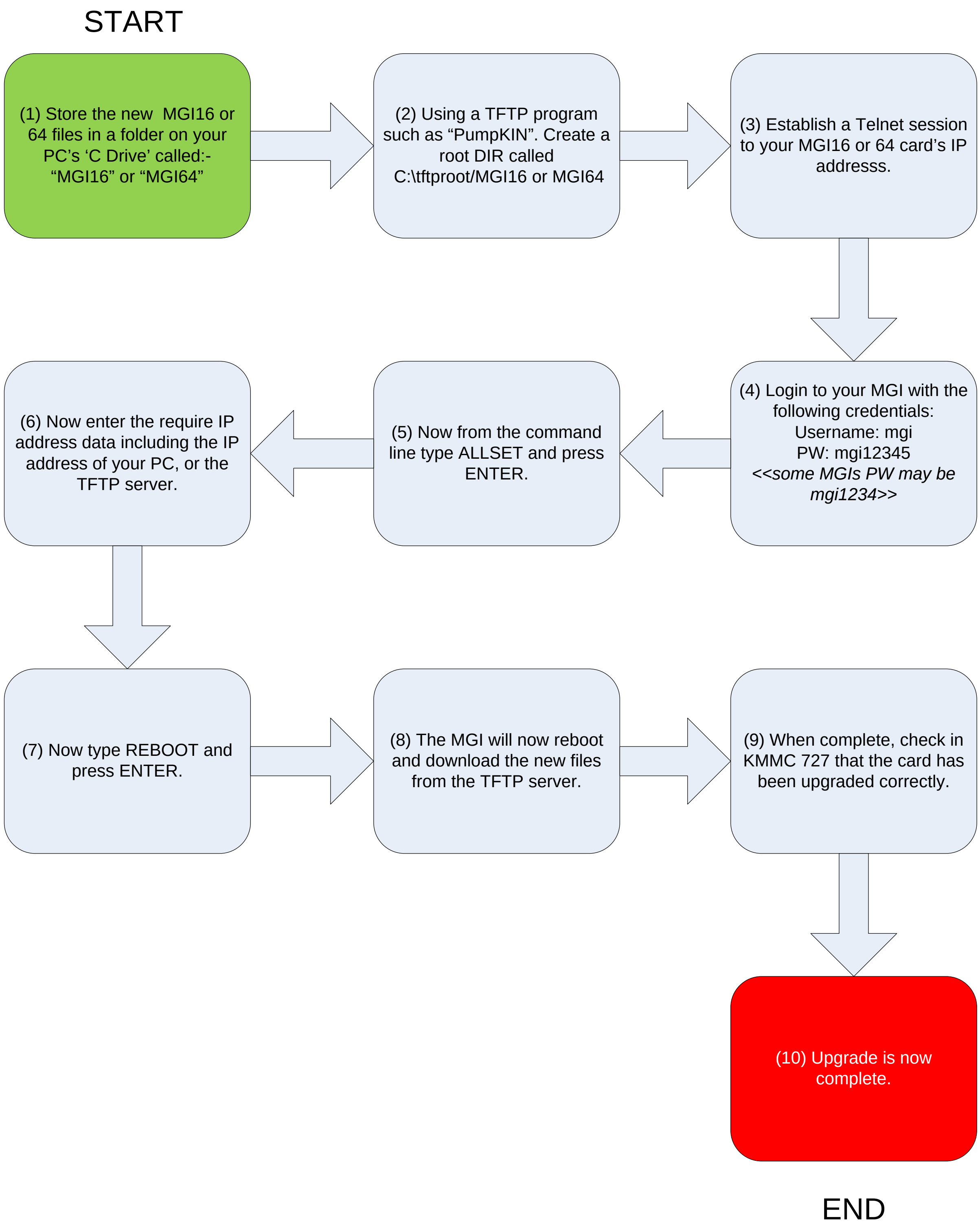
(10) Upgrade all SMT type IP phones with the normal procedure.

(11) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

UPGRADING THE MGI 16 & MGI 64 MODULES



START

(1) Store the new MGI16 or 64 files in a folder on your PC's 'C Drive' called:- "MGI16" or "MGI64"

(2) Using a TFTP program such as "PumpKIN". Create a root DIR called C:\tftproot/MGI16 or MGI64

(3) Establish a Telnet session to your MGI16 or 64 card's IP addresss.

(4) Login to your MGI with the following credentials:
Username: mgi
PW: mgi12345
<<some MGIs PW may be mgi1234>>

(5) Now from the command line type ALLSET and press ENTER.

(6) Now enter the require IP address data including the IP address of your PC, or the TFTP server.

(7) Now type REBOOT and press ENTER.

(8) The MGI will now reboot and download the new files from the TFTP server.

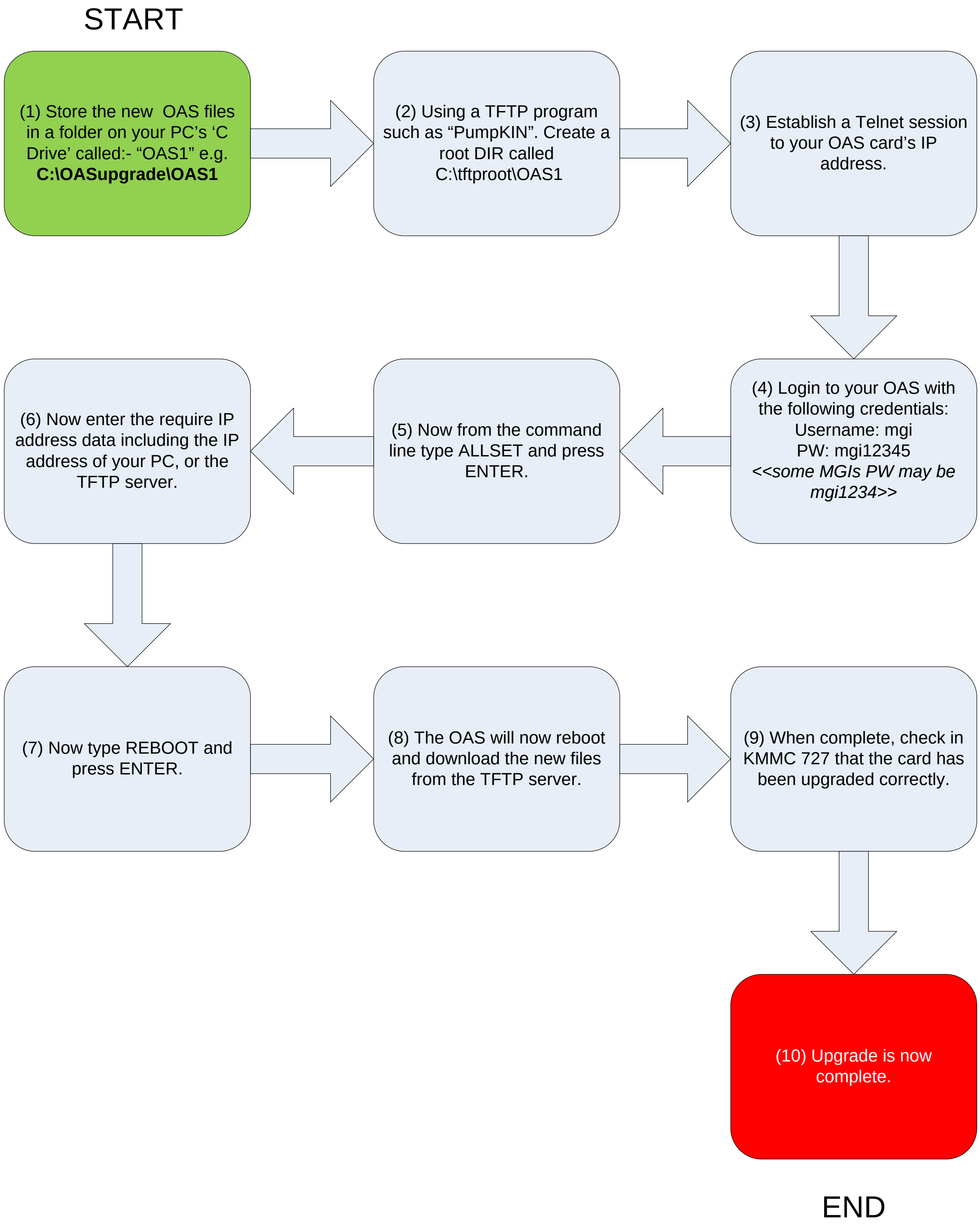
(9) When complete, check in KMMC 727 that the card has been upgraded correctly.

(10) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

UPGRADING THE OAS MODULE



START

(1) Store the new OAS files in a folder on your PC's 'C Drive' called:- "OAS1" e.g. **C:\OASupgrade\OAS1**

(2) Using a TFTP program such as "PumpKIN". Create a root DIR called C:\tftproot\OAS1

(3) Establish a Telnet session to your OAS card's IP address.

(4) Login to your OAS with the following credentials:
Username: mgi
PW: mgi12345
<<some MGIs PW may be mgi1234>>

(5) Now from the command line type ALLSET and press ENTER.

(6) Now enter the require IP address data including the IP address of your PC, or the TFTP server.

(7) Now type REBOOT and press ENTER.

(8) The OAS will now reboot and download the new files from the TFTP server.

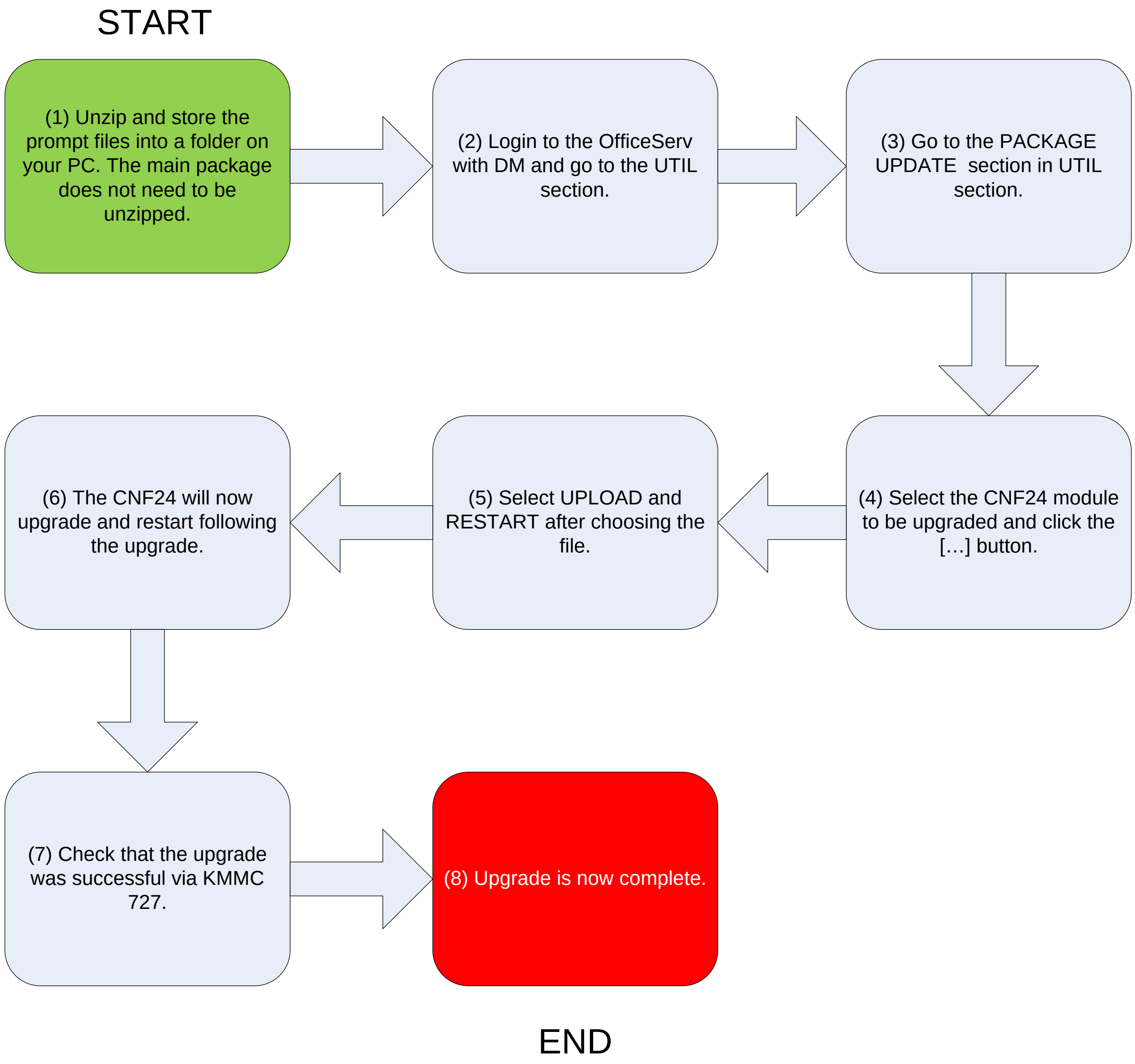
(9) When complete, check in KMMC 727 that the card has been upgraded correctly.

(10) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

UPGRADING THE CNF24 MODULE



START

(1) Unzip and store the prompt files into a folder on your PC. The main package does not need to be unzipped.

(2) Login to the OfficeServ with DM and go to the UTIL section.

(3) Go to the PACKAGE UPDATE section in UTIL section.

(4) Select the CNF24 module to be upgraded and click the […] button.

(5) Select UPLOAD and RESTART after choosing the file.

(6) The CNF24 will now upgrade and restart following the upgrade.

(7) Check that the upgrade was successful via KMMC 727.

(8) Upgrade is now complete.

END

Version 4.60 Upgrade Procedures

GENERAL UPGRADE NOTES AND RULES

1. The OS7200 MCP module is not compatible with V4.60. Where a customer wants to upgrade to V4.60, the MCP must be replaced with an MP20.

2. When upgrading a full system - including MP and any LP or LCP modules – you should first of all upgrade the MP module and not the LP or LCP. So for example, if you are upgrading an OS7400 from V4.53c to V4.60, you should always upgrade the MP40 first, followed by any LP40 modules. *This is because the LP40 file name has changed from LPxxxxx.PGM to SPxxxxx.PG, and only V4.60 can recognise the new file name.*

    a. This new SP.PGM file contains not only the main upgrade files, but also the necessary BOOT ROM files required for V4.60 compatibility.
    b. When you perform the LP40 upgrade, the system will at first upgrade the BOOT ROM and then the main software. This process will take about 15 minutes. **DO NOT INTERRUPT THIS PROCESS IN ANY WAY.**

3. When upgrading an OS7200 or OS7400 system to V4.60, due to the file size of the main software – about 20Mb – the upgrade cannot be done directly into the system using the DM procedure. The relative files must be copied onto the SD card as explained in the previous upgrade procedure pages.

4. V4.60 and DM have a new IP phone security measure: the IP phone's ID and password cannot be the same.

    a. DM will not allow you to save an IP phone's data if the ID and password match.
    b. DM will allow an old database to be uploaded that has matching IP and PW data.

Version 4.60 Software Tables & Version Data

In this section you will find the necessary software and system tables outlining all fully released versions and build dates for each main package and the relevant modules.

OFFICESERV 7400 & 7200 SOFTWARE TABLES

System	OS7400 (MP40)	OS7200 (MP20)
MP	V4.60 ‘12.02.06	V4.60 ‘12.02.06
LP40	V2.00 ’11.12.09	N/A
LCP	N/A	V4.30 ’11.12.09
TEPRI2/TEPRIa	V4.28 ‘10.09.07	V4.28 ‘10.09.07
4BRI	V6.03 ’10.06.29	V6.03 ’10.06.29
MGI16/64	V1.28 ‘11.12.09	V1.28 ‘11.12.09
SVMi-20E	V5.4.1.1 ’10.12.27	V5.4.1.1 ’10.12.27
SVMi-20i[3]	V6.0.0.i ’11.12.19	V6.0.0.i ’11.12.19
OAS	V2.03 ’11.12.09	V2.03 ’11.12.09
DM	V4.60 ‘12.02.06	V4.60 ‘12.02.06
CNF24	V1.02 ’11.11.25	V1.02 ’11.11.25
OS Link	V3.0.0.4	V3.0.0.4
IP-UMS	V1.3.6.9 ’11.08.16	V1.3.6.9 ’11.08.16
SNMP	V1.61 ’11.09.01	V1.61 ’11.09.01-
Bootrom	V1.02 ‘09.02.27 (checksum: u11(8560), u36(0000)	V1.00 ‘08.12.16

[3] SVMi-20i not available until the end of June, 2012

OFFICESERV 7200S & OS7100 (MP10A & MP11) SOFTWARE TABLES

System	OS7100 (MP10a)	OS7100 (MP11)	OS7200 (MP20S)
MP	V4.60 ‘12.02.16	V4.60 ‘12.02.06	V4.60 ‘12.02.16
SP	V2.60 ‘12.01.12	V2.60 ‘12.01.12	V2.60 ‘12.01.12
VM	V2.81p ‘11.12.19	V2.81p ‘11.12.19	V2.81p ‘11.12.19
MGI	V2.06 ‘11.12.09	V2.06 ‘11.12.09	V2.06 ‘11.12.09
BRI	V4.22f ‘09.11.30	V4.22f ‘09.11.30	V4.22f ‘09.11.30
WEB	V4.12h ‘10.04.13	V4.12h ‘10.04.13	V4.12h ‘10.04.13
MPS	V2.01 ‘11.12.09	V2.01 ‘11.12.09	V2.01 ‘11.12.09
SNMP	V1.61 ’11.09.01	V1.61 ’11.09.01-	V1.61 ’11.09.01-
Router	-	V1.11 ‘09.09.23	-
Boot	V1.07 ‘09.02.24	V1.07 ‘09.03.07	V0.30 ‘09.09.22-
DM	V4.60 ‘12.02.06	V4.60 ‘12.02.06	V4.60 ‘12.02.06
RTG	V1.00 ’11.12.09	V1.00 ’11.12.09	V1.00 ’11.12.09

OFFICESERV 7030 SOFTWARE TABLES

System	OS7030 (MP03)
MP	V4.60 ‘12.02.16
SP	V2.60 ‘12.01.12
VM	V2.81p ‘11.12.19
MGI	V2.06 ‘11.12.09
BRM	V4.22f ‘09.11.30
WEB	V4.12h ‘10.04.13
MPS	V2.01 ‘11.12.09
SNMP	V1.61 ’11.09.01
Boot	V4.40 ‘09.04.21
DM	V4.60 ‘12.02.06
RTG	V1.00 ’11.12.09

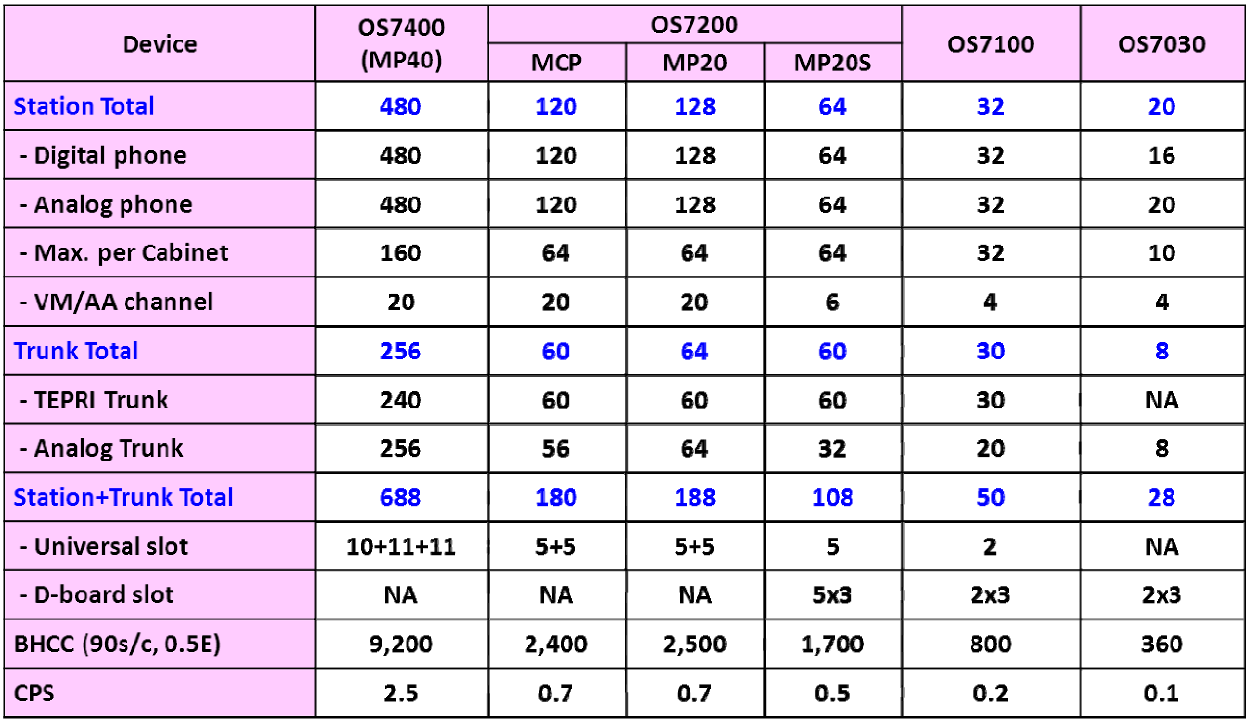
System Capacities

The following tables show the OfficeServ's station and trunk capacities as well as some generic data on busy hour call completion figures, calls per second and call capacities when TLS and sRTP is enabled on an IP solution.

ALL IP CONFIGURATIONS

Device	OS7400 (MP40)	OS7200			OS7100	OS7030
		MCP	MP20	MP20S		
Station Total	480	120	128	64	56	16
- ITP phone	480	120	128	64	56	16
- SIP phone	480	32	128	64	56	16
- WiFi phone	224	32	128	64	56	16
- UMS/IVR channel	128	32	64	NA	NA	NA
Trunk Total	256	60	64	32	64	8
- SIP Trunk	224	32	64	32	64	8
- H.323 Trunk	64	16	32	24	24	NA
- SPNet Trunk	224	60	64	32	64	8
Station+Trunk Total	736	180	192	96	120	24
- MPS Call	256	N/A	128	104	8	8
BHCC (90s/c, 0.5E)	10,800	2,100	3,600	1,800	1,800	320
CPS	3	0.6	1	0.5	0.5	0.1

ALL TDM/PCM CONFIGURATIONS



Device	OS7400 (MP40)	OS7200			OS7100	OS7030
		MCP	MP20	MP20S		
Station Total	480	120	128	64	32	20
- Digital phone	480	120	128	64	32	16
- Analog phone	480	120	128	64	32	20
- Max. per Cabinet	160	64	64	64	32	10
- VM/AA channel	20	20	20	6	4	4
Trunk Total	256	60	64	60	30	8
- TEPRI Trunk	240	60	60	60	30	NA
- Analog Trunk	256	56	64	32	20	8
Station+Trunk Total	688	180	188	108	50	28
- Universal slot	10+11+11	5+5	5+5	5	2	NA
- D-board slot	NA	NA	NA	5x3	2x3	2x3
BHCC (90s/c, 0.5E)	9,200	2,400	2,500	1,700	800	360
CPS	2.5	0.7	0.7	0.5	0.2	0.1

ALL IP & TDM/PCM CONFIGURATIONS

Device	OS7400 (MP40)	OS7200			OS7100	OS7030
		MCP	MP20	MP20S		
Station Total	480	120	128	64	60	20
- IP phone	480	120	128	64	56	16
- PCM phone	480	120	128	64	32	20
- UMS/IVR, VM/AA	128	32	64	6	4	4
- FMC/MVS	256	N/A	64	60	8	4
Trunk Total	256	60	64	60	120	16
- IP Trunk	256	60	64	32	64	8
- PCM Trunk	256	60	64	60	60	8
Station+Trunk Total	688	180	188	108	120	28
- MGI Channel	256	80	80	54	72	8
- MPS Call	256	N/A	128	104	8	8
BHCC (90s/c, 0.5E)	10,800	2,400	3,600	1,800	1,800	360
CPS	3	0.7	1	0.5	0.5	0.1

TLS CONFIGURATIONS

Device	OS7400 (MP40)	OS7200 (MP20)
Station Total	480	128
- IP phone	480	128
- PCM phone	480	128
- SIP phone (TLS)	160	64
IP Trunk Total	256	64
- SIP Trunk (TLS)	64	32
- SPNET Trunk	256	64
BHCC (90s/c, 0.25E)	3,600	1,800
CPS	1	0.5

SRTP & FOIP CONFIGURATIONS

Module	VoIP (RTP)	VoIP [A] (sRTP)	FoIP (T.38)
OAS	48	42	16
- MPS/RTG [B]	32	32	X
- MGI	16	10	16
MGI16	16	10	16
- MGI	16	10	16
MGI64	64	40	20
- MGI	64	40	20

Notes:

A) If sRTP is enabled, DM Menu ‘4.1.4 MGI Groups’ should be configured for sRTP density

B) MPS is measured by the number of calls & RTG by the number of channels