powerful technology.
affordable growth.

4.60 Feature Package Manual

SAMSUNG

OfficeServ™ 7000 Series

Software V4.60 Feature Package Reference Manual

February 2012 ***v1.1***

Every effort has been made to eliminate errors and ambiguities in the information contained in this guide. Any questions concerning information presented here should be directed to SAMSUNG TELECOMMUNICATIONS AMERICA, 1301 E. Lookout Dr. Richardson, TX. 75082 telephone (972) 761-7300. SAMSUNG TELECOMMUNICATIONS AMERICA disclaims all liabilities for damages arising from the erroneous interpretation or use of information presented in this guide.

Publication Information

SAMSUNG TELECOMMUNICATIONS AMERICA reserves the right without prior notice to revise information in this publication for any reason. SAMSUNG TELECOMMUNICATIONS AMERICA also reserves the right without prior notice to make changes in design or components of equipment as engineering and manufacturing may warrant.

Copyright 2012

Samsung Telecommunications America

All rights reserved. No part of this manual may be reproduced in any form or by any means—graphic, electronic or mechanical, including recording, taping, photocopying or information retrieval systems—without express written permission of the publisher of this material.

PRINTED IN THE USA

1. TABLE OF CONTENTS

2. INTRODUCTION

The purpose of this manual is to introduce and explain the version **V4.60** main system feature package for the **OfficeServ 7000 Series** of business telephone systems. Version **4.60** represents a major overhaul of the **OS 7000 Series**' IP capabilities to bring the system more in line with modern customer needs.

In addition to adding support for multiple SIP Service Providers and synchronizing the system clock to a **N**etwork **T**ime **P**rotocol (**NTP**) server, version **4.60** also makes some fundamental changes to the way that IP calls are processed allowing for a much more efficient use of both **M**edia **G**ateway **I**nterface (**MGI**) and **M**edia **P**roxy **S**ervice (**MPS**) channels. Version **4.60** also adds and extends a variety of system features

The chart in the next section lists the features and changes supported by V4.60 along with the OfficeServ 7000 Series system(s) supported.

3. FEATURE LIST AND SYSTEM SUPPORT

FEATURE	7030	7100	7200S	7200	7400
Conference Card Enhancements	**No**	**No**	Yes	Yes	Yes
DID Max Calls Per Ring Plan	Yes	Yes	Yes	Yes	Yes
Download phone book to SMT-I phones	Yes	Yes	Yes	Yes	Yes
DTMF Support on SIP Stations	Yes	Yes	Yes	Yes	Yes
Emergency 911 Conference Feature	Yes	Yes	Yes	Yes	Yes
Enhanced Plug-N-Play	Yes	Yes	Yes	Yes	Yes
Error Log via E-Mail	Yes	Yes	Yes	Yes	Yes
Malicious Call Restriction	Yes	Yes	Yes	Yes	Yes
Max Calls in Queue Feature	Yes	Yes	Yes	Yes	Yes
MGI Allocation Change	Yes	Yes	Yes	Yes	Yes
MOBEX Enhancements	Yes	Yes	Yes	Yes	Yes
MP Enhancements	Yes	Yes	Yes	Yes	Yes
Multicast Paging Support	Yes	Yes	Yes	Yes	Yes
Multiple SIP Service Providers	Yes	Yes	Yes	Yes	Yes
NTP Server Support	Yes	Yes	Yes	Yes	Yes
Presence Awareness Enhancements	Yes	Yes	Yes	Yes	Yes
Secure RTP (sRTP) Support	**No**	**No**	**No**	Yes	Yes
Security Enhancements	Yes	Yes	Yes	Yes	Yes
SIP Trunk Enhancements	Yes	Yes	Yes	Yes	Yes
TLS Support on SIP Trunks / Stations	**No**	**No**	**No**	Yes	Yes
Upload VM prompts in .wav format	Yes	Yes	Yes	No	No

4. FEATURE DESCRIPTION

This chapter lists the features in the V4.60 software package. Each feature is broken down into up to five sections corresponding to the traditional OfficeServ 7000 Series Technical Manual sections:

- General Description
  - This section will describe the purpose and market usage of the feature
- Installation
  - For hardware or applications this section will detail the installation of the equipment or program
- Programming
  - This section will detail any relevant Device Manager menu changes relating to the feature
- User Instructions
  - For features that are user-facing this section will describe how a user can access and use the feature

4.1 Emergency 911 Conference Feature

GENERAL DESCRIPTION

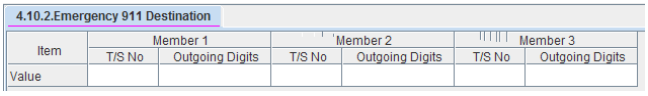
For networked systems or large enterprise businesses it is critically important that **911** calls be monitored and tracked not only so that the right people are aware of emergency situations, but also so emergency personnel can be directed properly.

Version 4.60 adds a new **911 Conference** feature that monitors the system for any user dialing **911** and performs a series of actions:

1. The **caller** who dials **911** will be routed by highest priority to emergency services. This means that if **all trunks** are **busy** or **all MGI channels** are **in use** the system will **automatically drop a call in progress** in order to make available resources for the **911** call.
2. The **911 call** will be **logged** to the **System Alarm Log**.
3. Up to **3 predefined monitoring stations** will ring with an **alert** of a **911** call. Upon answering the call the **monitoring station** will be **added to a conference** with the **station who dialed 911** and the **trunk connected to the 911** operator. If the **monitoring station** user wishes to **speak** to the **911** caller or the **911** operator they can **unmute** their phone to speak.

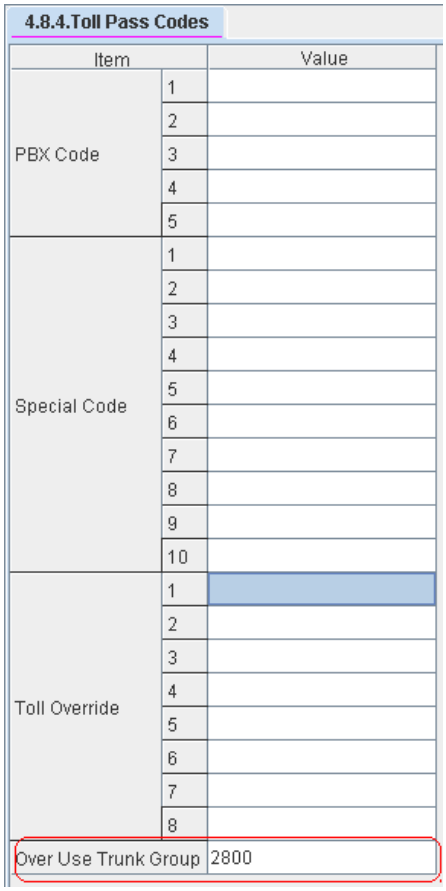
PROGRAMMING

The **4.10.2 Emergency 911 Destination** Device Manager Menu has been added to support the **911 Conference** feature.



FIELD	PURPOSE
Member 1 ~ 3	Sets up to **3 stations** that will be **auto-conferenced** in when any user dials **911**. These can be **local station numbers**, **SPNet stations**, or **external numbers.**

The trunk group for 911 uses needs to be added in **4.8.4 Toll Pass Codes**.



FIELD	PURPOSE
Over Use Trunk Group	Sets up one trunk group for 911 call to use.

Note: 911 conference feature supports PRI and SIP trunking only.

4.2 Conference Card Enhancements OfficeServ 7200-S/ 7200 / 7400 Only

GENERAL DESCRIPTION

Version 4.60 system software for the OfficeServ 7000 Series also marks the launch of Phase 2 of the 24-port OfficeServ Conference Card. Phase 2 does not change any hardware or alter the way a Conference Card is installed, but rather provides a significant number of feature additions and enhancements to the Conference Card's software. The new and enhanced features are:

- **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 any personal or business calendar.

- **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 whereas older software would disconnect immediately on an invalid entry.

- **Conference Email Login Instructions Support**

  In Phase 1 the login instructions sent in the conference email had to be reentered 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. Phase 2 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.

  NOTE: ***Conference Login Instructions will still need to be entered in the correct language if the prompt language is 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 rejoin. 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**

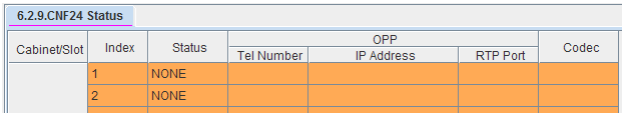
  Version 4.60 software and the Phase 2 Conference Card software now allow users to enter their own email address to be used when they are invited to attend a conference. Technicians and system administrators may still enter the list of addresses, but it is now possible for users to add or edit their own information.

PROGRAMMING

Two Device Manager Menus, **9.1.1 Conference Options** and **9.1.7 CNF24 Voice Management**, have been edited and three new menus, **6.2.9 CNF24 Status**, **9.1.6 Email Address**, and **9.1.8 Email Conference Instructions**, have been added to support the Phase 2 software.

6.2.9 CNF24 Status

This menu is used to monitor the status of channels on the **Conference Card**.

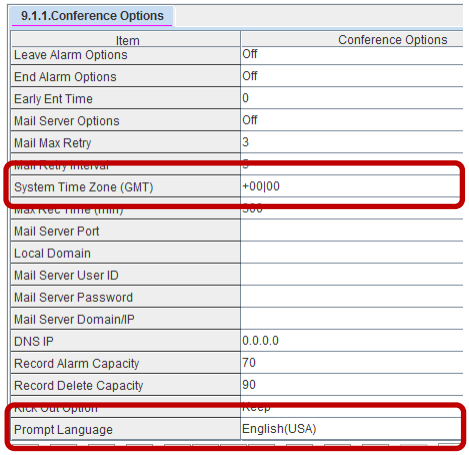


6.2.9.CNF24 Status

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

9.1.1 Conference Options

This menu is used to set system-wide **meet-me conference** parameters.



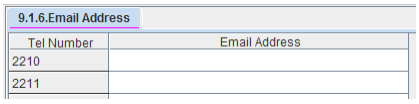
9.1.1.Conference Options

Item	Conference Options
Leave Alarm Options	Off
End Alarm Options	Off
Early Ent Time	0
Mail Server Options	Off
Mail Max Retry	3
[illegible]	[illegible]
System Time Zone (GMT)	+00|00
[illegible]	[illegible]
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
[illegible]	[illegible]
Prompt Language	English(USA)

FIELD	PURPOSE
System Time Zone (GMT)	Sets the **time zone** of the system based on the offset from **Greenwich Mean Time** (**GMT**)
Prompt Language	Sets the **language** of the voice prompts used by the **Conference Card**

9.1.6 Email Address

This menu is used to set the **email addresses** for each **station** user in the system.



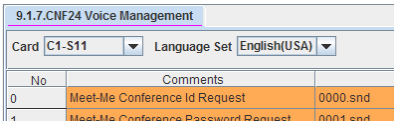
9.1.6.Email Address

Tel Number	Email Address
2210	
2211	

FIELD	PURPOSE
Email Address	Sets the **email address** of the user associated with the selected **extension number** for the purpose of sending **Conference Invite Emails**.

9.1.7 CNF24 Voice Management

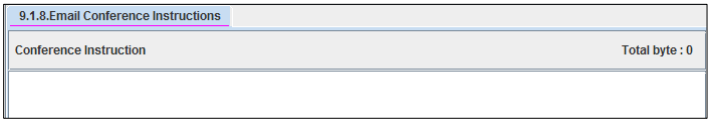
This menu is used to set **voice prompt** settings for the **Conference Card**.



FIELD	PURPOSE
Language Set	Sets the language for voice prompts on the specific **Conference Card**

9.1.8 Email Conference Instructions

This menu is used to set the **default login instructions** that will be sent in every **Conference Invite Email**.



4.3 Multiple SIP Service Providers

GENERAL DESCRIPTION

The use of **SIP** telephone lines is quickly being adopted in place of traditional CO lines. As **SIP trunking** usage grows carriers are beginning to see much of the competition the telecommunications industry saw during the launch of **T1** and **PRI** circuits. It is becoming common for a business to need more than one **SIP carrier** to get the best possible cost and flexibility for their operation by, for example, having one provider for domestic long distance and another for international calls or having one account as a backup for another.

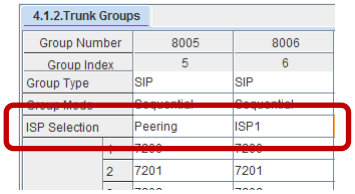
Version 4.60 addresses this need by adding the ability to register to up to **four** SIP carriers **simultaneously**.

PROGRAMMING

Two Device Manager Menus have been modified to allow the use of multiple SIP carriers: **4.1.2 Trunk Groups** and **5.2.13 SIP Carrier Options**.

4.1.2 Trunk Groups

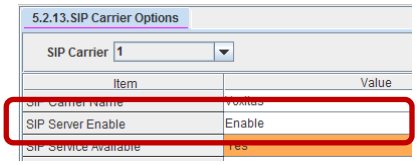
This menu is used to configure **Trunk Groups** and their members.



FIELD	PURPOSE
ISP Selection	For **Trunk Groups** with a **Group Type** of **SIP** this value sets which **SIP Carrier** the **Trunk Group** will service **or** if it will be available for **SIP Peering**.

5.2.13 SIP Carrier Options

This menu is used to set up **SIP Carrier Trunk** connections.



FIELD	PURPOSE
SIP Server Enable	**Enables** or **Disables** the ability to use this **SIP Carrier** for **trunking**. **Up to 4 SIP Carriers** may be **Enabled** simultaneously.

NOTE: Please refer to 4.19 SIP Trunk Enhancement for important new feature.

4.4 TLS Support on SIP Trunks / Stations OfficeServ 7200 / 7400 Only

GENERAL DESCRIPTION

With the expansion of IP telephone usage is an expansion of threats to business security. **V**oice-**o**ver-**IP** puts business communications on a data network where it is exposed to common data security threats like hackers or network attacks, and the compromise of business communications can be devastating to a company. To help mitigate the risks of **VoIP** telephony, version 4.60 allows **SIP Trunks** and **SIP Stations** on **OfficeServ 7200** or **7400** systems to use the **TLS encryption protocol** to prevent unauthorized access to the system. **TLS** is an industry-standard data cryptography protocol developed specifically to prevent unauthorized access to sensitive network data.

TLS can be enabled for **SIP Trunks**, **SIP Peering Trunks**, and/or **SIP Stations**. However, current softphone and Communicator softphone do not support sRTP.

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

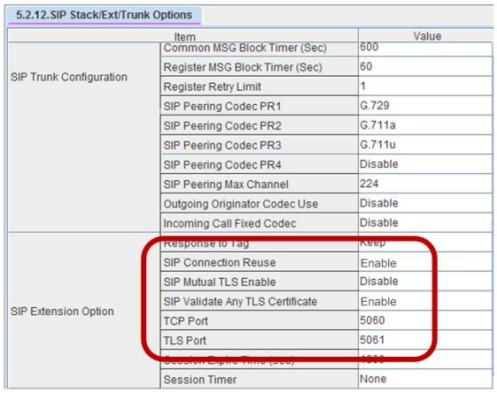
- For SIP trunking and SIP peering, the impact is **1:3.5**. That means one TLS connection will use 3.5 SIP channels. For example, if 4 TLS connection are required, the OfficeSrerv system will reserve 14 (= 4 x 3.5) SIP channels. The overall usable SIP channels for system will reduce because of TLS connection. Each SIP account can be set to TLS individually.
- For 3rd party SIP station, the impact is **1:3**. That means one TLS connection will use 3 SIP stations slot. For example, if 4 TLS connection are required for 3rd party SIPO station, the OffcieServ system will reserve 12 (= 4 x 3) 3rd party SIP station capacity.

PROGRAMMING

Three Device Manager Menus have been modified to support **TLS** on **SIP Trunks** and **SIP Stations**: **5.2.12 SIP Stack/Ext/Trunk Options**, **5.2.13 SIP Carrier Options**, and **5.2.17 VoIP Peering**.

5.2.12 SIP Stack/Ext/Trunk Options

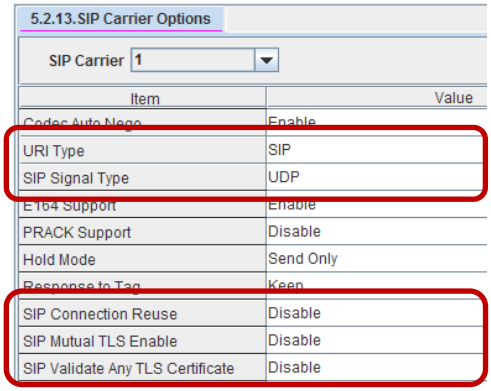
This menu is used to configure connectivity options for **SIP Stations** and **Trunks**.



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**.

5.2.13 SIP Carrier Options

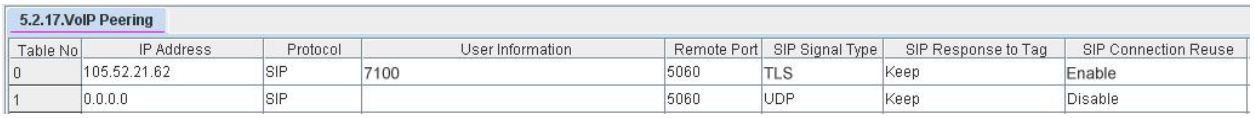
This menu is used to set up connections to **SIP Carriers**.



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 **signaling 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**

5.2.17 VoIP Peering

This menu is used to set up connections to **SIP Peers**.



5.2.17.VoIP Peering

Table No	IP Address	Protocol	User Information	Remote Port	SIP Signal Type	SIP Response to Tag	SIP Connection Reuse
0	105.52.21.62	SIP	7100	5060	TLS	Keep	Enable
1	0.0.0.0	SIP		5060	UDP	Keep	Disable

FIELD	PURPOSE
User Information	The **User Information** must match on both systems
Remote Port	Sets the **TCP** or **UDP port** used to communicate with the **SIP Peer**. For **TLS** this value is typically **5061**.
SIP Signal Type	Sets the **signaling 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**

4.5 Secure RTP (sRTP) Support — OfficeServ 7200 / 7400 Only

GENERAL DESCRIPTION

Encrypting a data channel with **TLS** goes a long way toward securing a business' **VoIP** communications, but still leaves open the ability for dedicated hackers to reconstruct an audio conversation. Version 4.60 addresses this security gap by adding support for **S**ecure **RTP** (**sRTP**) audio streams. **sRTP** is an encryption protocol developed specifically for **VoIP** audio streams and prevents hackers from reconstructing audio even in the event that packets are captured.

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

Note: When sRTP is in use, the MGI 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 accordingly. That means all OAS cards in the system will use the sRTP setting. The following are the system capacity table.

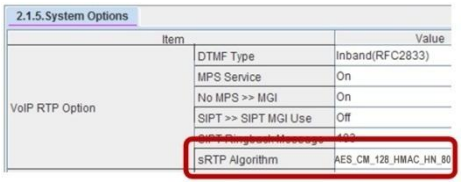
Module	VoIP (RTP)	VoIP (sRTP)
OAS		
MPS/RTG (no impact)	**32**	**32**
MGI	**16**	**10**
MGI16		
MGI	**16**	**10**
MGI64		
MGI	**64**	**40**

PROGRAMMING

Five Device Manager Menus have been modified and one has been added to support sRTP. The changed menus are **2.1.5 System Options**, **2.7.1 ITP Information**, **2.7.3 WIP Information**, **3.3.1 System Link ID**, and **5.2.16 MGI Options**.

2.1.5 System Options

This menu is used to set various system-wide options such as RTP options and area code options.



FIELD	PURPOSE
sRTP Algorithm	Sets the encryption algorithm for **sRTP** in the system (if any). The default value of **Disable** turns **sRTP** off for the system.

2.7.1 ITP Information

This menu is used to set options relating to individual IP phones.

FIELD	PURPOSE
USE sRTP	Sets whether the **SMT-i Series** IP phone will use **sRTP** or not.

2.7.3 WIP Information

This menu is used to set option relating to individual WiFi handsets.

FIELD	PURPOSE
USE sRTP	Sets whether the **SMT-W5120** WiFi handset will use **sRTP** or not.

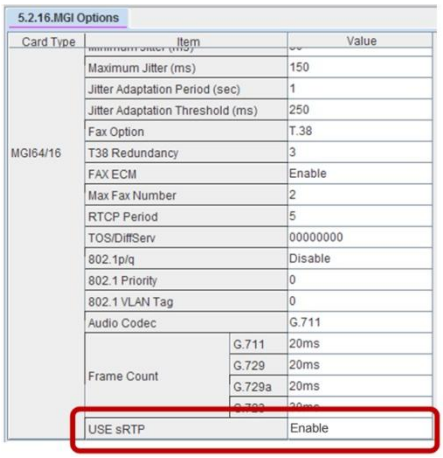
3.3.1 System Link ID

This menu is used to set up communications with other **SPNet** nodes.

FIELD	PURPOSE
USE sRTP	Sets whether the **SPNet** node will use **sRTP** or not.

5.2.16 MGI Options

This menu is used to set operational parameters for **MGI channels**.



FIELD	PURPOSE
USE sRTP	Sets whether the **MGI channels** on an **OAS** or **MGI64** card.

4.6 MGI Allocation Change

GENERAL DESCRIPTION

When the **OfficeServ 7000 Series** premiered all IP traffic was governed by **M**edia **G**ateway **I**nterface (**MGI**) channels. MGI channels allow IP devices and non-IP devices to talk to each other. Version 4.40 brought a brand new type of resource called **M**edia **P**roxy **S**ervice (**MPS**) channels. **MPS** channels allow IP devices to talk to other IP devices without using a more costly **MGI** channel. **MGI** channels were still used to connect IP devices to non-IP devices, however, so **MGI** channels would be assigned to an IP-to-IP call any time ringtone was playing or a caller was on hold. This meant that systems had to be overstocked with **MGI** channels to support these brief services.

Version 4.60 changes this **MGI** allocation by allowing specialized **MPS** channels called **R**ing **T**one **G**eneration (**RTG**) channels to provide **ringback tone**, **hold tone**, **music on hold and DTMF (RFC 2833) tone detection for executive Mobex feature**. 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).

NOTES:

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 the RTG ports are opened in the 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 used, they will be 7 MPS calls (or 7 RTG) available for use.***

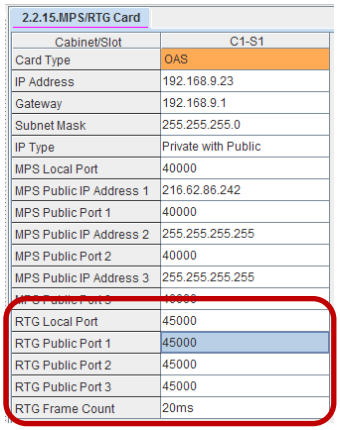
PROGRAMMING

One Device Manager Menu has been changed and one has been added to support this new MPS functionality. The new menu is **6.2.10 RTG Status** and the modified menu is **2.2.15** which has had a name change from **MPS Card** to **MPS/RTG Card**.

MPS Service has to be set to **On** in Device Manager, Port Base Menu, **2.2.5 System Options**, **VoIP RTP Option** for this feature to be functional.

2.2.15 MPS/RTG Card

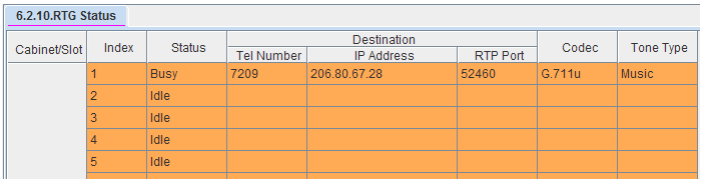
This menu is used to configure options for the **OAS card** (**OS7200-S, OS7200, and OS7400 systems**) or built-in **MPS** and **RTG** channels (**OS7030, OS7100, OS7200-S systems**) as shown below:



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***

6.2.10 RTG Status

This menu is used to monitor the connection status of RTG channels. This is extremely helpful in troubleshooting, training, and call tracing scenarios.



FIELD	PURPOSE
Index	Displays the RTG channel number ***The number of RTG channels in the system will always be half the number of MPS channels installed in the system***
Status	Displays the current busy / idle status of the port
Destination	Displays telephone number, IP address, and RTP port the RTG channel is connected to
Codec	Displays the audio codec the RTG channel is using
Tone Type	Displays the type of service being provided by the RTG channel. ***6 = Ringback tone*** ***9 = Hold TONE*** ***Music = Music on Hold***

4.7 Multicast Paging Support

GENERAL DESCRIPTION

With today's explosive growth of IP telephone usage in businesses it has become even more necessary to control the load on the data networks that support those IP phones. Samsung is addressing that need in version 4.60 by adding the ability to page to IP phones through **multicast** data packets. This means that instead of sending a separate data stream (and assigning a separate **MGI** channel) to each IP phone receiving the page, the system can send only one stream for all phones and use only one **MGI** channel. This not only reduces the load on the data network during a page, but may also reduce the number of **OAS** or **MGI64** cards or **MGI** licenses needed in the system.

NOTE: Multicast paging feature applies to SMT-I IP phones only on the same local network as the OfficeServ 7000 system. Remote IP phones will still require separate MGI channels for each remote IP phone being paged, unless the router at the remote location can support the multicast feature. Many routers can support multicast.

PROGRAMMING

Two Device Manager Menus have been edited and one has been created in order to support multicasting. The new menu is **5.2.25 Multicast Page IP List** and the edited menus are **2.7.1 ITP Information** and **4.1.3 Page Groups**.

2.7.1 ITP Information

This menu is used to configure multicast options for Samsung **SMT-i** Series IP phones.

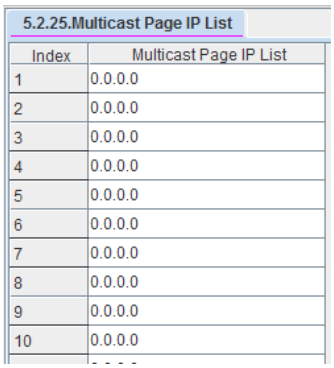
2.7.1.ITP Information

Tel Number	Type	Time Zone	Signal Type	Video Codec	Video Size	QoS Enable	USE sRTP	Multicast Page
2220		+00|00	UDP	H.263	CIF	Disable	Disable	Auto
2221		+00|00	UDP	H.263	CIF	Disable	Disable	Auto
2222		+00|00	UDP	H.263	CIF	Disable	Disable	Auto
2223		+00|00	UDP	H.263	CIF	Disable	Disable	Auto
2224		+00|00	UDP	H.263	CIF	Disable	Disable	Auto

NEW FIELD	PURPOSE
Multicast Page	Sets whether an IP device will use **multicast** paging (**ON**), use **unicast** paging (**OFF**), or **automatically** determine usage based on the device's registered IP address (**AUTO**). The default setting is **AUTO**.

5.2.25 Multicast Page IP List

This menu is used to configure up to **80** remote router IP **segments** or **addresses** that the system can **multicast** to.



FIELD	PURPOSE
Multicast Page IP List	Sets an IP segment or address that will accept multicast packets from the system. There is no need to enter any address if there is no remote router that support multicast. **You can enter .255 to cover all ranges in the subnet.**

4.1.3 Page Groups

This menu is used to configure **internal** and **external** page groups and the **multicast** address **internal** page groups should stream page announcements to, if any.

NEW FIELD	PURPOSE
Multicast Addr	Sets the broadcast IP address the **internal** page group will use to stream **multicast** packets to the IP phones in the page group. The default value of **255.255.255.255** means that no multicast will be used for this page group. **The valid range of multicast addresses is 224.0.1.0 through 239.255.255.254.**

4.8 Plug-N-Play

GENERAL DESCRIPTION

For companies with a large amount of IP telephones a significant number of man hours can be spent setting IP addresses, updating software, and registering phones. This directly affects a company's ability to stay efficient and keep costs down. To help alleviate many of the common time sinks involved with installing IP phones Samsung has developed a new **Plug-N-Play** feature for the **OfficeServ 7000 Series** and **OfficeServ SMT-i Series IP Phones**. This feature, enabled by version 4.60 system software and the latest IP phone software, allows SMT-i Series phones to find the OfficeServ 7000 Series system automatically and register with very minimal programming. Version 4.60 adds the ability to set the OfficeServ 7000 Series system as a **DHCP server** (***for OfficeServ 7030, 7100, and 7200-S 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 so upon connecting to the system it can be assigned the correct station registration. **New feature: Auto Registration (Auto PNP)**

  This mode, which is the system default, allows phones to register without any user or technician action at all. Each time an SMT-i Series 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 **7200-S** is set to operate as a **DHCP server**, but the same settings can be configured for sites with an **OfficeServ 7200** or **7400** and a customer-provided **DHCP server** already installed.

Note: **PNP is available for SMT-I series of phones only. It is not available on SMT-W5120 or ITP model**.

PROGRAMMING

A single Device Manager menu has been changed to support the Plug-N-Play feature, menu **5.2.10 System IP Options**, which is used to configure various IP Phone connection and registration options. In addition, the **SMT-i Series phones** can now recognize **DHCP options 66** and **128**. Configuration of a **DHCP server** is discussed below.

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

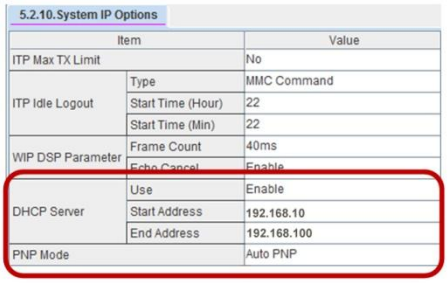
After receiving an **option 66** request the **DHCP server** will use **option 128** to send out the **IP address** of the server the requesting host should connect to. This value should be set to the **IP address of the OfficeServ 7000 Series system**.

Note: IP phone needs to be to PNP mode when connecting to the OfficeServ system with PNP or pre-MAC setting.

Auto PNP

5.2.10 System IP Options

This menu is used to configure various options relating to IP phones registration and communications.



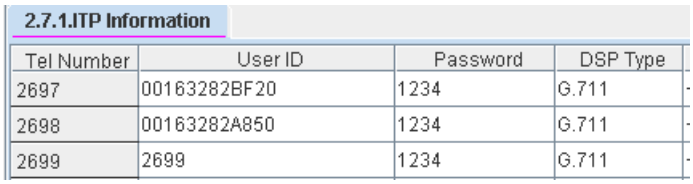
5.2.10.System IP Options

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

FIELD	PURPOSE
DHCP Server Use	Sets whether or not the OfficeServ will be used as a DHCP Server ***Available only on OfficeServ 7030 / 7100 / 7200-S***
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
PNP Mode	Sets the Plug-N-Play registration mode Auto PNP, pre-MAC address, or normal login

MAC Address Registration

Set DM 5.2.10 PNP Mode to Pre-Mac and enter the IP phone MAC address to the user ID section of DM 2.7.1. Alphabet character of MAC address has to be in capital letter.



2.7.1.ITP Information

Tel Number	User ID	Password	DSP Type
2697	00163282BF20	1234	G.711
2698	00163282A850	1234	G.711
2699	2699	1234	G.711

4.9 MOBEX Enhancements

GENERAL DESCRIPTION

In 2009 Samsung launched version 4.30 system software for the OfficeServ 7000 Series that added the **MOBEX** feature. Since then there has been overwhelmingly positive feedback about this feature and with version 4.60 we have enhanced it even further:

- **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 MOBEX phone. Users can specify whether **intercom callers**, **trunk callers**, or **SPNet callers** will reach their **MOBEX** phone. They can also determine whether or not calls to **Station Groups** they are a member of will ring to their **MOBEX** phone.

- **Executive MOBEX Callback**

  The downside of the **Executive MOBEX** feature is that sometimes it is a long distance call to get into the system, so toll charges can be incurred just to make a local call through the system. Version 4.60 allows an **Executive MOBEX User** to be set so that when they call in to the system it immediately hangs up on them 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 are a **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 **MOBEX cell 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 Pairs** work in the system.

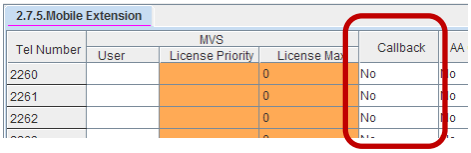
Note: Executive Mobex users can activate or deactivate Mobex feature already supported

PROGRAMMING

Three Device Manager Menus have been modified and two have been created to support the new MOBEX enhancements. **4.10.1 Mobex Scheduling Time** and **5.15.16 Mobex Caller** are the new menus. The changed menus are **2.7.5 Mobile Extension**, **4.2.5 Ring Group Pair**, and **5.14.3 Outgoing/Retry Options**.

2.7.5 Mobile Extension

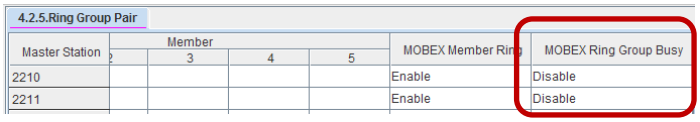
This menu is used to configure **Mobile Extension** and **Executive MOBEX** ports.



FIELD	PURPOSE
Callback	Turns **Executive MOBEX Callback on** or **off** for the **MOBEX** station.

4.2.5 Ring Group Pair

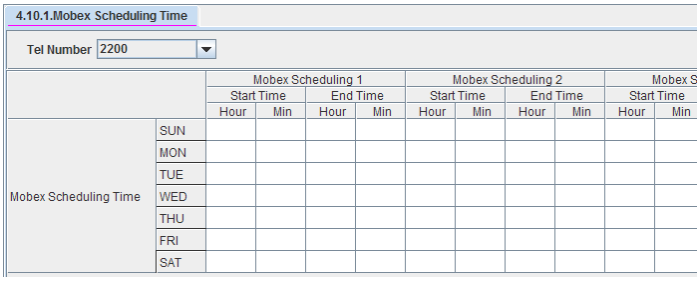
This menu is used to configure OfficeServ Connect ring groups.



FIELD	PURPOSE
MOBEX Ring Group Busy	When **Enabled every device** in the **OfficeServ Connect group** will be considered **busy** when **any** member device is on a call.

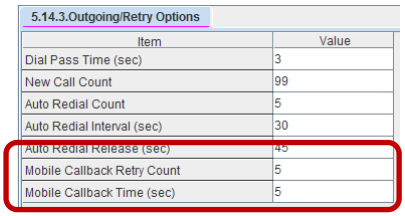
4.10.1 Mobex Scheduling Time

This menu is used to set up an activity schedule for each station with an OfficeServ Connect group.



5.14.3 Outgoing/Retry Options

This menu sets various timers or counters relating to outbound calls made by the system.

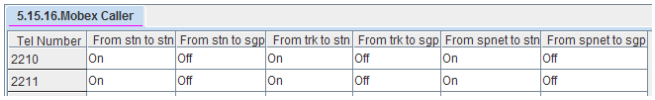

5.14.3.Outgoing/Retry Options

Item	Value
Dial Pass Time (sec)	3
New Call Count	99
Auto Redial Count	5
Auto Redial Interval (sec)	30
Auto Redial Release (sec)	45
Mobile Callback Retry Count	5
Mobile Callback Time (sec)	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

5.15.16 Mobex Caller

This menu is used to determine **which types** of callers will be able to reach a member at their **MOBEX** station.


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
2210	On	Off	On	Off	On	Off
2211	On	Off	On	Off	On	Off

FIELD	PURPOSE
From stn to stn	**Allows** or **denies** calls from **another station** to reach the **MOBEX station** when calling the **MOBEX user's extension**
From stn to sgp	**Allows** or **denies** calls from **another station** to reach the **MOBEX station** when calling **a station group the MOBEX user's extension is a member of**
From trk to stn	**Allows** or **denies** calls from a **CO trunk** to reach the **MOBEX station** when calling the **MOBEX user's extension**
From trk to sgp	**Allows** or **denies** calls from a **CO trunk** to reach the **MOBEX station** when calling **a station group the MOBEX user's extension is a member of**
From spnet to stn	**Allows** or **denies** calls from **another SPNet node** to reach the **MOBEX station** when calling the **MOBEX user's extension**
From spnet to sgp	**Allows** or **denies** calls from **another SPNet node** to reach the **MOBEX station** when calling **a station group the MOBEX user's extension is a member of**

USER INSTRUCTIONS

To set a MOBEX Schedule:

- Press **TRANSFER** plus **129**
- Press **VOLUME UP** or **DOWN** to select the desired day of the week
- Press the **RIGHT SOFTKEY** twice
- Use the keypad to enter the 4-digit hour and minute to turn MOBEX on (i.e. **0730**)
- Use the keypad to enter the 4-digit hour and minute to turn MOBEX off (i.e. **1700**)
- Press **TRANSFER** to save your changes and exit

4.10 SVM Prompt File Uploading

GENERAL DESCRIPTION

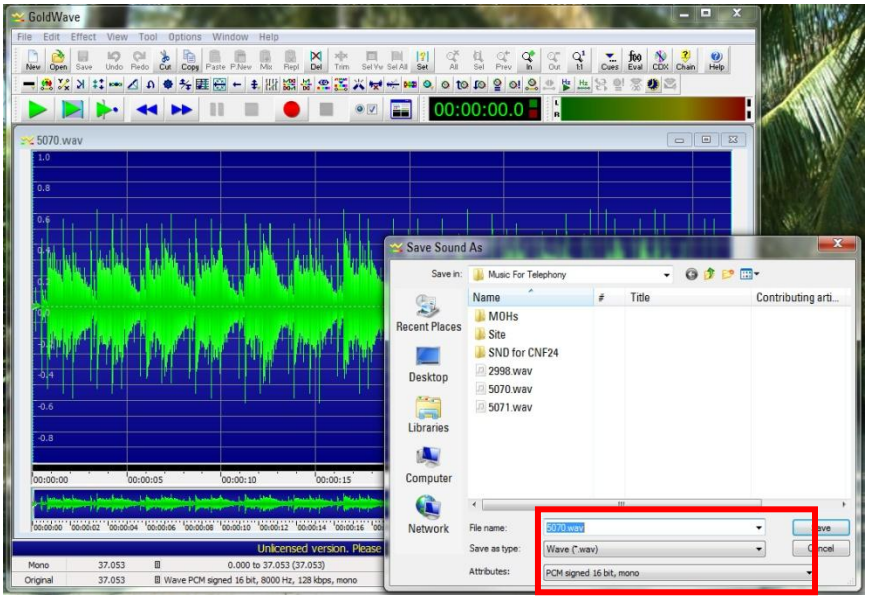
The Samsung voicemail (SVM) has been enhanced to automatically convert the format of uploaded audio **WAV** files to the voicemail system. If the administrator uploads an existing **WAV** file using the SVM voice studio, the voice mail application will automatically convert the WAV file to the format required for the SVM. This enhancement is applied to the OfficeServ 7030, 7100 (MP10a), and 7200-S systems.

Notes:

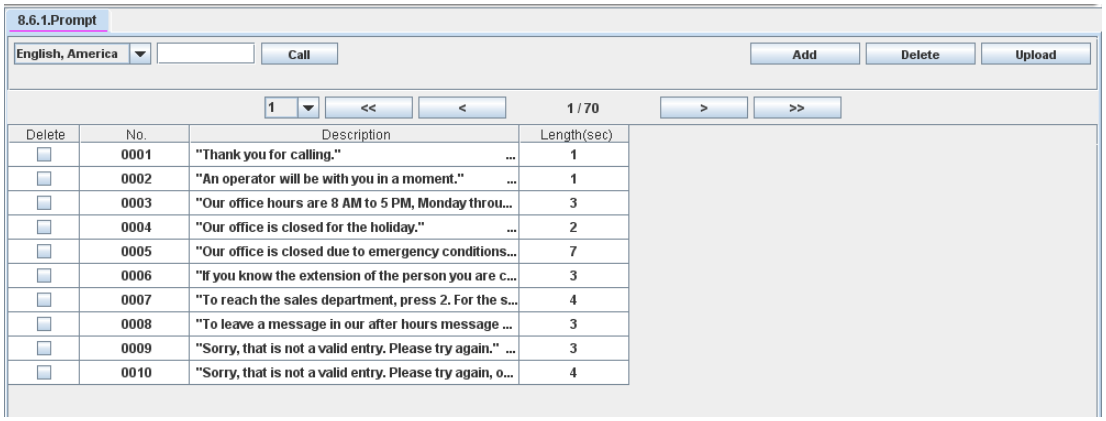
1. *Wav file prompt conversion is supported on the OS 7030, 7100, 7200-S with 4.60 software.*
2. *This enhancement is not supported on the 7200 and 7400 with the SVMi20E installed.*
3. *The SVM only supports one wav file format (8kHz, mono, 16 bit signed, 128kps).*

PROGRAMMING

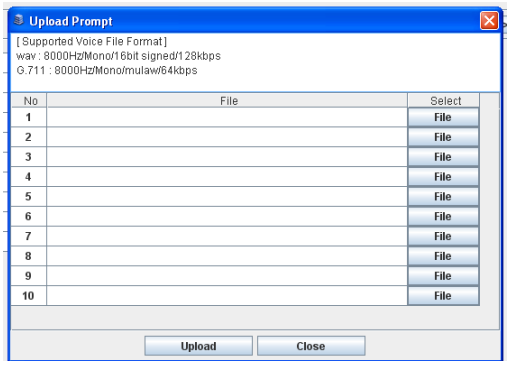
When using an application such as this example (GoldWave) to record audio prompt in to a wav format, the store audio prompt file can then be automatically converted to a useable format and uploaded directly into the SVM application using the embedded voice studio. Make sure to save the file as WAV *(8kHz, Mono, 16 bit signed, 128kps).*



Once the audio file is stored in a wav format, use **Device Manager to access the VM/AA function and go to voice studio menu 8.6, prompts 8.6.1.** In this screen, press the upload button to select the location of the wav file to be uploaded and converted.



Next select the location of the wav file to be converted and uploaded, then click on upload at the botton of the screen. See the example below.



4.11 NTP Server Support

GENERAL DESCRIPTION

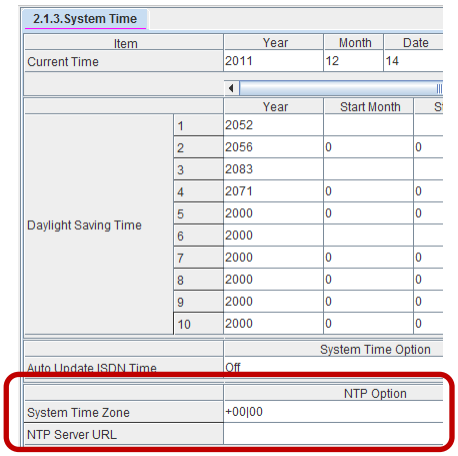
Due to overwhelming demand from the customer base Samsung has added the ability in version 4.60 software for the OfficeServ 7000 Series systems to synchronize the **internal system clock** with a **N**etwork **T**ime **P**rotocol (**NTP**) **Server**. This means that the system will automatically monitor its own internal clock so that customers do not need to worry about drifting clocks or resetting them after power outages or Daylight Savings Time changes. **NTP Servers** can be entered as a **static IP address** or as a **DNS name** if the system **DNS Server** options have been set.

PROGRAMMING

Two Device Manager Menus have been changed to support NTP synchronization: **2.1.3 System Time** and **5.6.1 System I/O Parameter**.

2.1.3 System Time

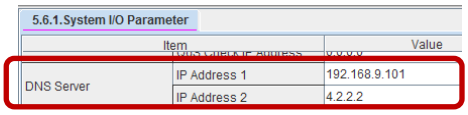
This menu is used to configure the system date and time, as well as the start and end dates of Daylight Savings Time each year.



FIELD	PURPOSE
System Time Zone	Sets the **time zone** of the system based on the offset from **Greenwich Mean Time** (**GMT**)
NTP Server URL	Sets the **web address** (or **URL**, for example **us.pool.ntp.org**) of the **Network Time** (**NTP**) server the system should synchronize the internal clock to

5.6.1 System I/O Parameter

This menu is used to set various options relating to application connectivity to the system.



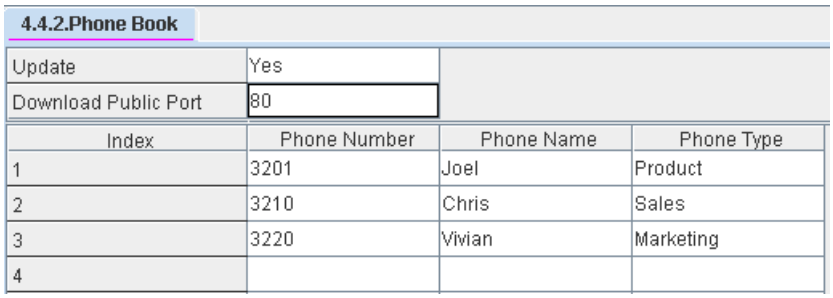
FIELD	PURPOSE
DNS Server IP Address 1 ~ 2	Sets the **primary** (for example 208.67.222.222) and **alternate** servers to use for **DNS queries**. This allows the system to resolve a **DNS name**, such as www.samsung.com, to a physical IP address.

4.12 Phone Book Download for SMT-i Phones

GENERAL DESCRIPTION

The new **System Phone Book** feature allows up to **100 phone numbers and names** to be stored in the system where they can be pushed to the phonebook entries of **SMT-i phones**. This eliminates the work of creating separate company phonebooks for each employee.**4.4.2 Phone Book**

This menu is used to set up the system phone book that can be pushed to **SMT-I series phones**.



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**")

4.13 Presence Awareness Enhancements

GENERAL DESCRIPTION

Since the early days of the Samsung Business Communications feature package there has been a feature called **Programmed Messages**. **Programmed Messages** allow a user to set a status message on their phone display that will show up in the display of any intercom caller who dials them. This is ideal for situations where a manager must go to a meeting, for example, because they can set their **Programmed Message** to "**IN A MEETING**" and any time someone else in the office tries to dial them the message will alert the caller that the manager is in a meeting.

With version 4.60 Samsung, with the assistance of dealers like you, has revisited the usefulness of the **Programmed Message** feature and expanded it to become an even more robust component of the OfficeServ 7000 Series' built-in presence awareness feature by adding the ability to specify **actions** that will occur along with the **Programmed Message** as well as what **cadence** the **LED** of the programmable button assigned to the message will show.

The available actions to take when a **Programmed Message** is activated are: **Set DND without Forward**, **Set DND with Forward**, **Set Forward All**, **Clear DND + FWD All**, or **None** (do nothing). Available **LED** cadences are **Steady**, **Flashing**, or **Off**.

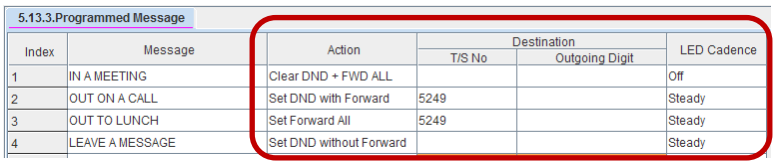
This allows a user to, for example, have a button labeled **Vacation** that when pressed changes their **Programmed Message** to say "**ON VACATION**" and set **Forward All to voicemail**, or a button labeled **On Call** that, when pressed, changes their **Programmed Message** to "**ON THE ROAD**" and sets **DND with forwarding** to their cell phone.

PROGRAMMING

Two Device Manager Menus have been changed to support the new Programmed Message features: **5.13.3 Programmed Message** and **5.15.9 User Programmed Message**.

5.13.3 Programmed Message

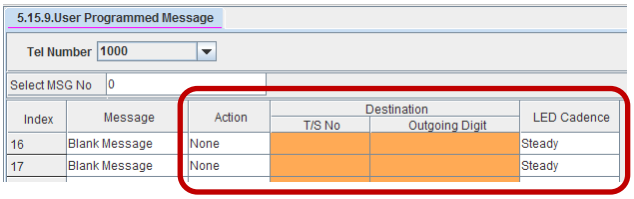
This menu is used to configure system-wide **Programmed Messages**.



FIELD	PURPOSE
Action	Sets what **action** will take place when this **Programmed Message** is **activated**. By default all **Programmed Messages** have an action of **None**.
Destination T/S No	Set the local **trunk**, **station**, **trunk group**, or **station group** that the station will forward to according to the chosen **Action**.
Destination Outgoing Digit	Set the **external number** to forward to if the chosen **Action** should **forward externally**.
LED Cadence	Sets the **cadence** of the **LED** when the **Programmed Message** button is **activated**. When deactivated the **LED** will always be **off**.

5.15.9 User Programmed Message

This menu is used to configure user-specific **Programmed Messages**.



FIELD	PURPOSE
Action	Sets what **action** will take place when this **Programmed Message** is **activated**. By default all **Programmed Messages** have an action of **None**.
Destination T/S No	Set the local **trunk**, **station**, **trunk group**, or **station group** that the station will forward to according to the chosen **Action**.
Destination Outgoing Digit	Set the **external number** to forward to if the chosen **Action** should **forward externally**.
LED Cadence	Sets the **cadence** of the **LED** when the **Programmed Message** button is **activated**. When deactivated the **LED** will always be **off**.

USER INSTRUCTIONS

When you will be away from your phone for any length of time, you can leave a programmed station message. Display stations calling you will see this message and be informed of your status or follow your instructions. In addition you can assign any of four possible actions to be taken on your station when you activate the programmed message. These actions are:

DND W/FWD – Sets Do Not Disturb (**DND**) on your station and forwards all calls to another station or to voicemail.

DNDW/OFWD – Sets **DND** on your station but does not forward calls; callers will receive a fast busy tone when calling to your station.

FWD ALL – Sets **Forward All** on your station so that all incoming callers will be immediately forwarded to another station or to your voicemail.

CLEARBOTH – Clears both **DND** and **Forward All** from your station. This is typically used when the programmed message is telling your callers that you are at your desk and available.

To set an action to take place along with a programmed message:

- Press **TRANSFER** plus **115**.
- Dial any of the message codes (**16**-**20**) listed on the back of your user guide.

  NOTE: ***Actions may only be set for the user-customizable messages numbered 16 through 20.***
- Use the keypad to enter a message to show to display stations calling you.
- Press the **RIGHT SOFTKEY** to save the message.
- Press **VOLUME UP** or **DOWN** to select the desired action.
- Press the **RIGHT SOFTKEY** to save the action.
- If the desired action requires you to set a forwarding location, such as another station or your voicemail box, dial that destination and press the **RIGHT SOFTKEY** to save the destination.
- Press **VOLUME UP** or **DOWN** to set how the button light should appear (**STEADY**, **FLASHING**, or **OFF**) on any programmed message (**PMSG**) buttons that use this programmed message.
- Press **TRANSFER** to exit and save your changes.

To activate a programmed station message:

- Dial **48** plus any of the message codes (**01**-**20**) listed on the back of your user guide.
- To cancel any of these messages you might have selected, dial **48** plus **00**.

NOTE: If the Hot Keypad feature has been turned off, you must first lift the handset or press the SPEAKER key.

You can have multiple programmed message keys (**PMSG**) and each one can have a different message code and action:

- Press any programmed message (**PMSG**) button. The message is set, any assigned action will take effect, and the button will light according to the setting assigned to the chosen programmed message.
- Pressing an active programmed message (**PMSG**) button again will turn the programmed message off.
- Pressing another programmed message (**PMSG**) button will turn the previous one off and set the new programmed message.

4.14 DTMF Support on SIP Stations

GENERAL DESCRIPTION

Version 4.60 system software enhances **third-party SIP phones** connected to the system by allowing them to receive **DTMF** digits during a call and by allowing them to utilize the **H.264** codec to provide video during calls.

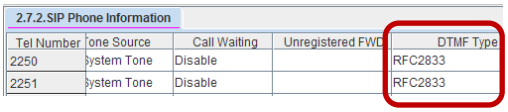
DTMF digits can be sent to the phone by either of two protocols: **RFC2833**, which is an **in-band DTMF** delivery method, or by **INFO**, which is a special **out-of-band** method in the **SIP** protocol. This is particularly useful for certain types of **third-party SIP** voicemail systems, door phones, and other third party devices that require **DTMF** digits to activate.

PROGRAMMING

One Device Manager Menu, **2.7.2 SIP Phone Information** has been edited to support the **DTMF** sending options.

2.7.2 SIP Phone Information

This menu is used to configure options for specific **3rd-Party SIP Stations**.



FIELD	PURPOSE
DTMF Type	Sets the DTMF protocol to use for the **3rd-Party SIP Station**.

NOTE: 3rd Party SIP video phone is not supported in North America.

4.15 MP Enhancements

GENERAL DESCRIPTION

The version 4.60 feature package also includes some new convenience features to assist in troubleshooting and system installation.

The new **SMDR Buffering** feature allows up to **10,000 SMDR records** to be stored in **RAM** in the event that the call accounting package, billing system or printer that gathers **SMDR data** loses connection from the system. When the device reconnects the buffered **SMDR data** are sent immediately.

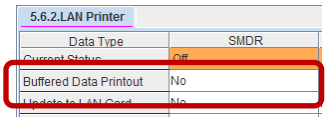
A new **Alarm Email** feature allows **system alarms** and **crash reports** to be **automatically emailed** to **up to four** system administrators, managers, or necessary personnel. Emails can be sent immediately **when an error occurs**, or they can be buffered and sent **on demand** or **daily**.

PROGRAMMING

One Device Manager Menu, **5.6.2 LAN Printer**, has been changed to support the **SMDR Buffering** feature. Two new Device Manager Menus, **6.1.4 System Alarm Mail Server Info** and **6.1.5 System Alarm Email Address**, have been created to support the **Alarm Email** feature. One Device Manager Menu, **4.4.2 Phone Book**, has been created to support the **System Phone Book** feature.

5.6.2 LAN Printer

This menu is used to configure the various data output streams the **OfficeServ 7000 Series** offers.

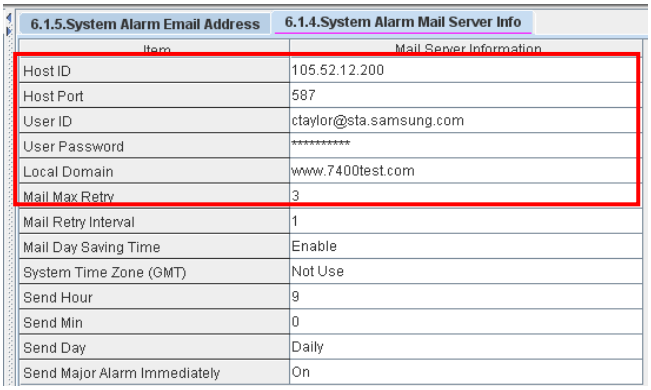


FIELD	PURPOSE
Buffered Data Printout	Sets whether the system should **buffer** the data stream in memory in the event the connected device loses connection. Up to **10,000** records will be buffered.

4.15.1 ALARM NOTIFICATION [Future Release]

6.1.4 System Alarm Mail Server Info

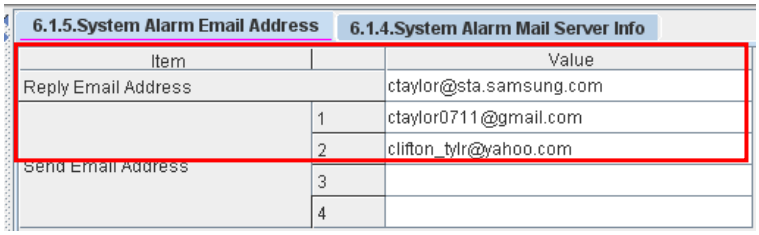
This menu is used to configure the connection to the email server where alarm email notifications are sent.



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**

6.1.5 System Alarm Email Address

This menu is used to configure the email address(es) alarm emails will be sent to.



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

4.16 DID Max Calls Per Ring Plan

GENERAL DESCRIPTION

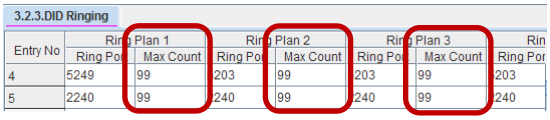
The OfficeServ 7000 Series has always had the ability to restrict the maximum number of simultaneous calls that can be received on a **DID** number. This has been modified in version 4.60 by allowing each **DID** to have a separate **Maximum Call Count** for each **Ring Plan**. This means that companies can have a much greater degree of control over how their **DID** numbers are used. As an example, a call center agent's personal **DID** number might accept only one call during normal business hours, but three calls at lunch or after hours.

PROGRAMMING

One Device Manager Menu, **3.2.3 DID Ringing**, has been changed to support the new **Max Calls** per **Ring Plan**.

3.2.3 DID Ringing

This menu is used to configure **DID** numbers for **SIP**, **SPNet**, and **PRI** trunks.



FIELD	PURPOSE
Ring Plan 1 ~ 6 Max Count	Sets the **maximum** number of simultaneous calls for the **DID number** during the specific **Ring Plan**.

4.17 Max Calls in Queue Feature

GENERAL DESCRIPTION

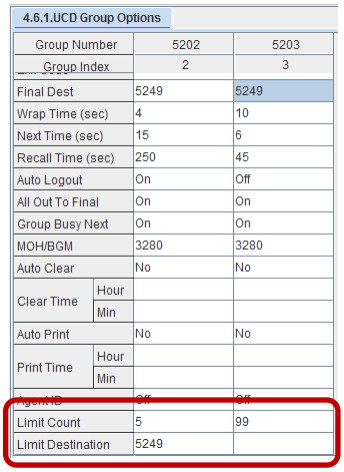
In order to keep pace with the rapidly evolving needs of small call centers a new feature has been added to version 4.60 software that allows the number of waiting calls for a **UCD Group** to be capped at a **desired limit**. Any calls above this maximum threshold will be automatically rerouted to a **predefined destination**. This allows a call center manager to, for example, have the call center configured so that a maximum of 4 calls may be in queue, and any calls beyond that go immediately to a voicemail box.

PROGRAMMING

The **4.6.1 UCD Group Options** Device Manager Menu has been changed to allow the new maximum call limit.

4.6.1 UCD Group Options

This menu is used to configure **Call Center Groups** and their options.



4.6.1.UCD Group Options

Group Number		5202	5203
Group Index		2	3
Final Dest		5249	5249
Wrap Time (sec)		4	10
Next Time (sec)		15	6
Recall Time (sec)		250	45
Auto Logout		On	Off
All Out To Final		On	On
Group Busy Next		On	On
MOH/BGM		3280	3280
Auto Clear		No	No
Clear Time	Hour		
	Min		
Auto Print		No	No
Print Time	Hour		
	Min		
Agent NB		Off	Off
Limit Count		5	99
Limit Destination		5249	

FIELD	PURPOSE
Limit Count	Sets the **maximum** number of calls that can be queued for a **UCD Group** before **forwarding** to **Limit Destination**.
Limit Destination	Sets the **destination station** or **station group** that calls ringing to a **UCD group** after the **Limit Count** has been reached will **forward** to.

4.18 Security Enhancements

GENERAL DESCRIPTION

Each model of the OfficeServ 7000 Series system family contains an embedded web server that is used for the Device Manager and, in the case of the OfficeServ 7030 / 7100 / 7200-S, the embedded voicemail programming interface. Since the last release of software there have been a number of security and performance patches released for the **Apache** web server and **PHP** engine used. With version 4.60 these packages have been updated to the latest versions (as of the date of this document) to ensure the highest level of performance and security.

There are no programming or installation steps to take in order to gain the advantages of these new packages; they are automatically updated and launched when a system boots on version 4.60.

4.19 SIP Trunk 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 Carrier**

  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 on which service. 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 Carrier 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** use is increasing more and more **Fax machines** and **data modems** are being connected to **SIP** lines and becoming subject to these same error correction techniques. This can be quite devastating to **fax** and **modem** transmissions, however, so in version 4.60 it is now possible for **MGI**s to use the **V**oice **B**and **D**ata (**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: ***Many SIP Carriers do not support hiding the host ID. Be sure to check with the 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, however, 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(default setting for MP40)**, meaning that the system will **ignore** all SIP messages from unauthorized IP addresses and block the relevant IP address. The OfficeServ system will not send back any response message.
  - **Response (default setting for MP03/10a/20s/20)**, which means that the system will not allow SIP calls from unauthorized IP to go through. The OfficeServ system will respond with a deny message (403 forbidden), and
  - **None**, which means that the system will **allow** all SIP calls.

- **Specify codec used for SIP Trunks**

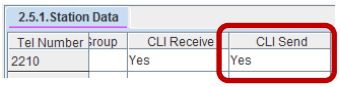
  Version 4.60 adds the ability to specify the **audio codec** used for **SIP** conversations. Different **codecs** can be chosen for each **SIP Carrier** and each **SIP Peer**. Additionally there are four **codec priority levels** that can be set so that if the desired **codec** cannot be used the next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

PROGRAMMING

Six Device Manager Menus have been modified to support these new SIP Trunking enhancements: **2.5.1 Station Data**, **4.1.2 Trunk Groups**, **5.2.12 SIP Stack/Ext/Trunk Options**, **5.2.13 SIP Carrier Options**, **5.2.16 MGI Options**, and **5.2.17 VoIP Peering**.

2.5.1 Station Data

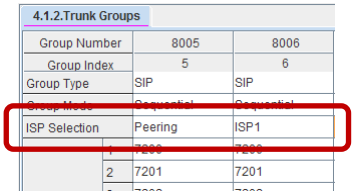
This menu is used to configure various options for individual telephones connected to the OfficeServ 7000 Series system.



FIELD	PURPOSE
CLI Send	Sets whether or not this station will send caller ID information when making a CO call. **NOTE:** ***This option remains unchanged from prior software, but in version 4.60 it will also affect calls made to SIP Carrier Trunks.***

4.1.2 Trunk Groups

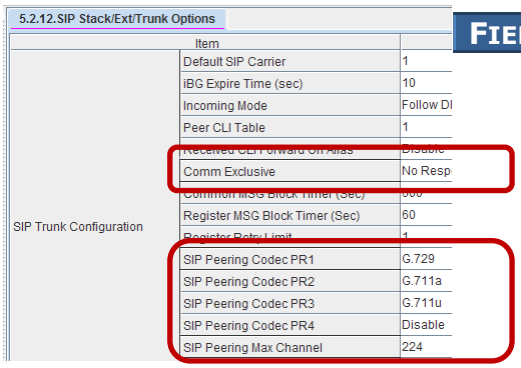
This menu is used to configure **Trunk Groups** and their members.



FIELD	PURPOSE
ISP Selection	For **Trunk Groups** with a **Group Type** of **SIP** this value sets which **SIP Carrier** the **Trunk Group** will service **or** if it will be available for **SIP Peering**, allowing the technician to segregate **SIP Carrier** and **SIP Peering** traffic.

5.2.12 SIP Stack/Ext/Trunk Options

This menu is used to set various options relating to how **SIP Stations** and **Trunks** connect to, and communicate with, the system.



FIELD	PURPOSE
Comm Exclusive	Sets the method the **OfficeServ 7000 Series** system will respond to **SIP** traffic from unknown sources. ○ **No Response(default setting for MP40)**, meaning that the system will **ignore** all SIP messages from unauthorized IP addresses and block the relevant IP address. The OfficeServ system will not send back any response message. ○ **Response (default setting for MP03/10a/20s/20)**, which means that the system will not allow SIP calls from unauthorized IP to go through. The OfficeServ system will respond with a deny message (403 forbidden), and ○ **None**, which means that the system will **allow** all SIP calls. See note below.
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, etc.
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 signal.

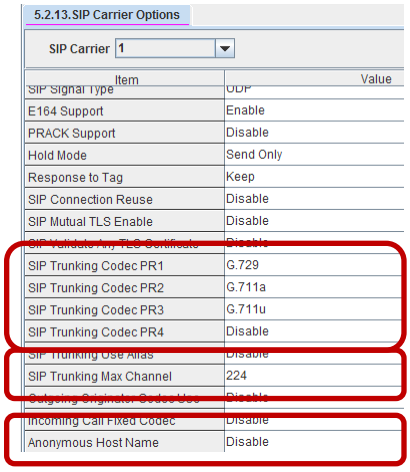
NOTE:

Valid SIP traffics are SIP messages come from known IP addresses. IP addresses come from the following different places are considered valid:

- DM 5.2.13 SIP Carrier Option
  - The IP address in the Outbound Proxy field, or
    - If IP address is used in this field, OfficeServ will accept SIP trunk call from this IP address only. If the SIP provider sends call from other server (different IP addresses), OfficeServ may reject the call depends on the setting of Comm Exclusive.
    - It is not recommended to use IP address in this field. If IP address is used, you need to set Comm Exclusive to None.
  - The resolution of domain name in the Outbound Proxy field
- DM 5.2.17 VoIP Peering
  - IP addresses in this table.

5.2.13 SIP Carrier Options

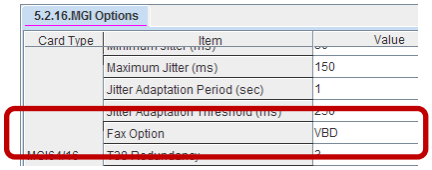
This menu is used to configure SIP Carrier accounts.



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 call for this SIP Carrier will have an anonymous host name, so the Caller ID information sent will be in the form <[stationID]@anonymous.invalid>

5.2.16 MGI Options

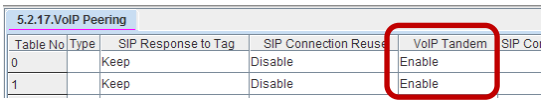
This menu is used to configure connection options and set up **MGI** cards and channels.



FIELD	PURPOSE
Fax Option	Determine whether **FoIP** calls will use **T.38**, **Pass Through**, or the new **VBD** protocol.

5.2.17 VoIP Peering

This menu is used to create and configure **SIP Peering** connections to third-party devices or phone systems.



FIELD	PURPOSE
VoIP Tandem	Set whether or not **incoming calls** from this **SIP Peer** can be routed out to local **analog**, **PRI**, or **SIP Carrier** trunks

4.20 Malicious Call Restriction

GENERAL DESCRIPTION

The Malicious Call Restriction feature has been added to software version 4.60 and is used to protect the OfficeServ system against fraudulent SIP calls.

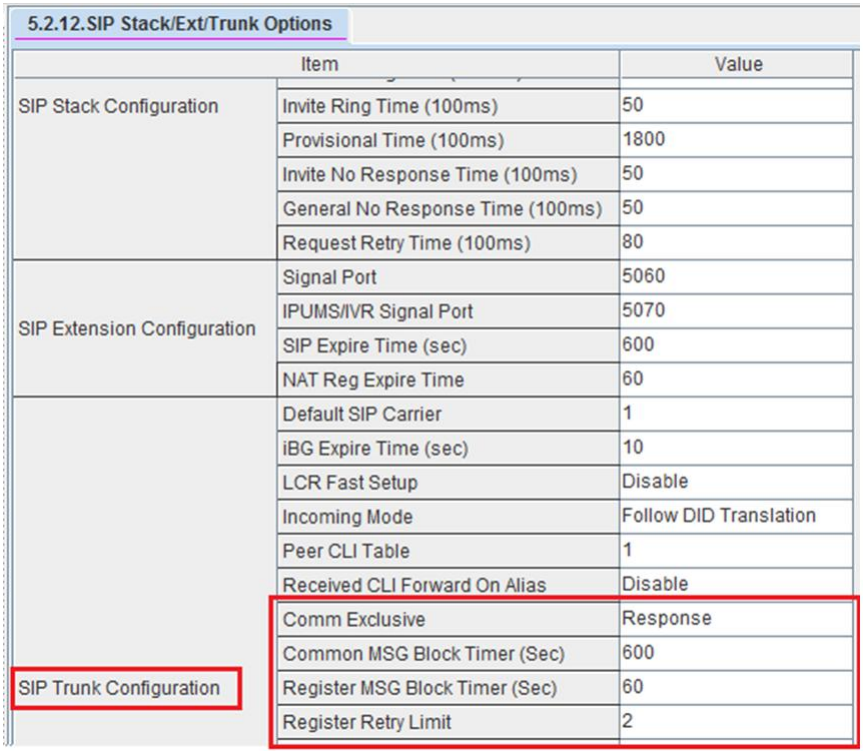
By enabling this feature you can prevent unauthorized SIP calls going through the system via the SIP trunk or SIP peering. The OfficeServ system blocks the IP address when a SIP phone tries to register to the system with a wrong User ID or Password.

The system will recognize the following IP list as valid:

1. Registered SIP station IP address (Device Manager 6.2.3)
2. VoIP peering IP addresses (Device Manager 5.2.17)
3. Carrier's IP addresses (Device Manager 5.2.13).

PROGRAMMING

The **5.2.12 SIP Stack/Ext/Trunk Options** Device Manager Menu has been updated. **SIP Trunk Configuration** options have been added to support the **Malicious Call Restriction** feature.



5.2.12.SIP Stack/Ext/Trunk Options

Item		Value
SIP Stack Configuration	Invite Ring Time (100ms)	50
	Provisional Time (100ms)	1800
	Invite No Response Time (100ms)	50
	General No Response Time (100ms)	50
	Request Retry Time (100ms)	80
SIP Extension Configuration	Signal Port	5060
	IPUMS/IVR Signal Port	5070
	SIP Expire Time (sec)	600
	NAT Reg Expire Time	60
SIP Trunk Configuration	Default SIP Carrier	1
	iBG Expire Time (sec)	10
	LCR Fast Setup	Disable
	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

FIELD	PURPOSE
Comm Exclusive	Sets how OfficeServ system responds to SIP messages from unauthorized IP address. None: Disable this feature and system will respond to SIP calls from all IP addresses Response: OfficeServ system will respond with the deny message (403 forbidden) when receiving SIP/Peering messages from unauthorized IP addresses No Response: OfficeServ system will ignore all SIP messages from unauthorized IP address and block the relevant IP address. The system will also block the IP address for a specified time period when a SIP phone tries to register to the system several times with an invalid User ID or password
Common MSG Block Timer	Sets how long OfficeServ blocks the SIP messages except from unauthorized IP address. Timer value is from 1 ~ 84600 seconds
Register MSG Block Timer	Sets how long OfficeServ blocks the REGISTER message for unauthorized IP address. Timer value is from 1 ~ 84600 seconds
Register Retry Limit	Sets the number of times (1~5) a user can try to register a SIP phone using an invalid User ID or password. The OfficeServ system blocks the IP address of the SIP phone after the maximum limit is reached.

4.21 SVM E-Mail Gateway with SSL/TLS Security

GENERAL DESCRIPTION

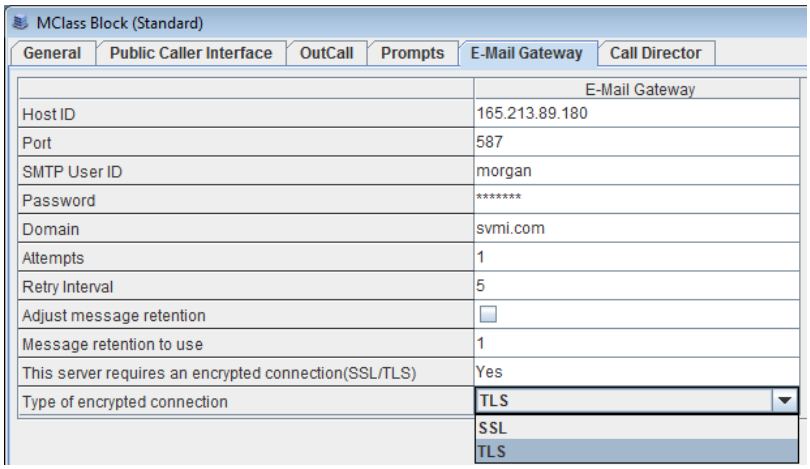
The Samung voicemail (SVM) has been enhanced to include both SSL and TLS encryption for secured communications between the voicemail email gateway application and the local/remote mail server(s). With the growing amount of threats to business data security, VoIP communications are exposed to data security threats such as hacking and network virus attacks which could be devastating to business communications. To ease or eliminate the risk, both SSL (secure socket layer) and TLS (transport layer security) options have been added to the OfficeServ SVM.

Notes:

1. *Requires Version 4.60 software or higher on the OfficeServ 7030, 7100(Mp10a), and 7200-S.*
2. *SSL and TLS security is not supported on the 7200 and 7400 with the SVMi20E.*
3. *Multiple email service providers or accounts can be used at the same time based on mailbox user to MClass assignment*.

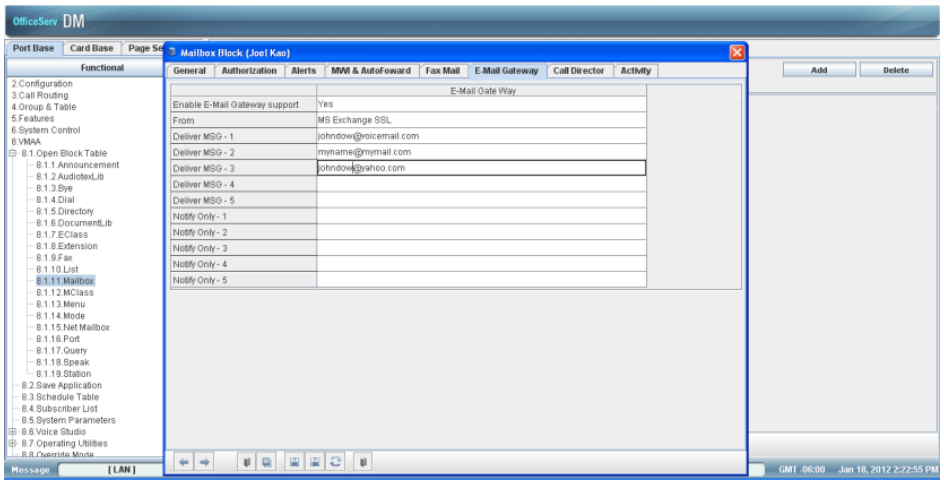
PROGRAMMING

On Device Manager, 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, Domain, enable encryption**, and set the **encryption type**. See the example below.



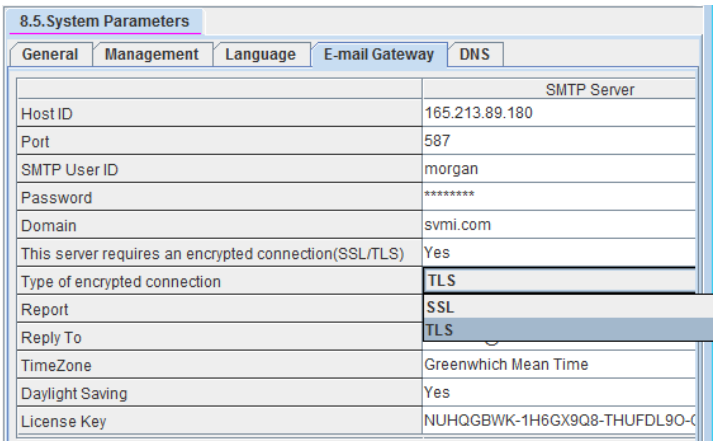
FIELD	PURPOSE
This server requires an encrypted connection (SSL/TLS)	Set this option if the mail server requires encrypted connection (SSL/TLS). This option should be set to yes.
Type of encrypted connection	**TLS:** SVM first send "STARTTLS" command to the mail server before it begins encrypted connection. **SSL:** SVM starts encrypted connection with the mail server directly. Please contact your E-Mail server administrator which one is supported in your mail server.

Next go to **Mailbox block 8.1.11** and **enable email gateway** and setup the **delivery MSG(s)** for each mailbox user that is using the email gateway application. See the example below.



NOTE: The from field in the mailbox block may require a valid address from the mail server (MS Exchange). For example, from: jdow.samsung.com.

System Parameters settings for email gateway in menu **8.5** is optional. This table can be setup to send out mail to notifiy the on or off-site system administration of errors in sending out mail. These SMTP server parameters are not use for subscriber email delivery and/or message notification. The parmerters set in SMTP servers section of this page are use for sending mail to the address set in the "report" field. See the example below.



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	Two types of connections are supported: **TLS:** The client issues a STARTTLS command. If the server accepts this, the client and the server negotiates an encryption mechanism. **SSL:** Encryption negotiation starts immediately without STARTTLS command.

5. APPENDIX

5.1 Media Resource Usage Chart

GENERAL DESCRIPTION

Three types of media resources are used in the OfficeServ system to process the audio stream.

1. Media Gateway Interface (MGI): Main service of MGI is to convert time-division-multiplex digital stream to IP packets and vice versa. It can be assigned one channel at a time as required.
2. Media Proxy Service (MPS): Main service of MPS is to translate the IP address of IP packets from one network to the other. Each usage requires two channels: one for private address and one for public IP address. For each MPS call, it takes two MPS channels. MPS service always uses as a pair. It cannot be used as one MPS channel only. For example, 1 MPS = 1 MPS call = 2 MPS channels.
3. Real-time Tone Generation Service (RTG): This is new service introduced in v4.60 software. The usage guide is equivalent to MPS resource. One RTG call uses two channels. It always comes as a pair. For example, 1 RTG = 1 RTG channel = 1 RTG call = 2 MPS channels. Its main services are to support ringback and hold tone in all IP calls and to support DTMF (RFC 2833) detection in Mobex feature.

Usage Chart

Call Conversation State

	IP Trunk (SIP, SPnet, H323)	PSTN Trunk (PRI, Analog)	Local IP Phone	Remote IP Phone	Voice Mail
Local IP phone (ITP, or SMT-I, or SMT-w, or 3rd party SIP phone)	2 MGI chs or 1 MPS call	1 MGI ch	0	2 MGI chs or 1 MPS call	1 MGI ch
Remote IP phone (ITP, or SMT-I, or SMT-w, or 3rd party SIP phone)	2 MGI chs or 1 MPS call	1 MGI ch	2 MGI chs or 1 MPS call	2 MGI chs or 1 MPS call	1 MGI ch
Non-IP phone (TDM, or analog, Fax machine, or SVMi)	1 MGI ch	0	1 MGI ch	1 MGI ch	0

Trunk Ringing State

	IP Trunk (SIP, SPnet, H323)	PSTN Trunk (PRI, Analog)
Local IP phone (ITP, or SMT-I, or SMT-w, or 3rd party SIP phone)	2 MGI chs or 1 RTG call	1 MGI ch
Remote IP phone (ITP, or SMT-I, or SMT-w, or 3rd party SIP phone)	2 MGI chs or 1 RTG call	1 MGI ch
Non-IP phone (TDM, or analog, Fax machine, or SVMi)	1 MGI ch	0

Hold/Music-On-Hold State

	IP Trunk (SIP, SPnet, H323)	PSTN Trunk (PRI, Analog)
Local IP phone (ITP, or SMT-I, or SMT-w, or 3rd party SIP phone)	1 MGI ch or 1 RTG call	0
Remote IP phone (ITP, or SMT-I, or SMT-w, or 3rd party SIP phone)	1 MGI ch or 1 RTG call	0
Non-IP phone (TDM, or analog, Fax machine, or SVMi)	1 MGI ch	0

Paging State

	Receiving Local IP Phones supporting multicast paging (SMT-I, or SMT-w5120)	Receiving Local IP Phone **NOT** supporting multicast paging (ITP, or 3rd party SIP)	Receiving Remote IP Phone supporting multicast paging (SMT-I, or SMT-w5120) **AND** router supporting multicast	Receiving Remote IP Phone supporting multicast paging (SMT-I, or SMT-w5120) **but** router **NOT** supporting multicast	Receiving Trmote IP Phone **NOT** supporting multicast paging (ITP, or 3rd party SIP)
Originator Local/Remote IP Phone (ITP, or SMT-I, or SMT-w, or 3rd party SIP)	**2 MGI chs** (1 for originator and 1 for all receiving IP phone)	**2+ MGI ch** (1 for originator and 1 for each receiving IP phone)	**2 MGI chs** (1 for originator and 1 for all receiving IP phone)	**2+ MGI ch** (1 for originator and 1 for each receiving IP phone)	**2+ MGI ch** (1 for originator and 1 for each receiving IP phone)
Non-IP phone (TDM, or analog, Fax machine, or SVMi)	**1 MGI ch** (0 for originator and 1 for all receiving IP phones)	**1+ MGI ch** (0 for originatora and 1 for each receiving IP phone)	**1 MGI ch** (0 for originator and 1 for all receiving IP phones)	**1+ MGI ch** (0 for originatora and 1 for each receiving IP phone)	**1+** (0 for originatora and 1 for each receiving IP phone)

5.2 System Port Usage

Module	Service	Protocol	Port
MP	SIP	UDP/TCP TCP	5060 5061
	H.323	TCP UDP	1720 1719
	SPNET	TCP	6100
	ITP	UDP	6000, 9000
	WIP	UDP	8000, 8001
	MVS	TCP	9012
	DM	TCP	5090,5091
	DM FTP	TCP	21
	DM Data	TCP	5090
	DM File Control	TCP	5003
	DM Embedded VM	TCP	6001, 6002
	ITT	TCP	5090, 5091
MGI16 MGI64 OAS	MGI	UDP	30000~ (2*NumOfChannel -1)
	MPS	UDP	40000~ (2*NumOfChannel -1)
	RTG	UDP	45000 ~ (2*NumOfChannel-1)
CNF24	Conference	UDP	30000 ~ (2*NumOfChannel -1)
	FTP	TCP	21
	Upgrade Port	TCP	60000
SVMi-20i [FUTURE RELEASE]	VM Control	TCP	6001,6002
	VM	UDP	30000 ~ (2*NumOfChannel -1)
	FTP	TCP	21
	Upgrade port	TCP	60024

5.3 Software Package

Data Base File

The data base file from previous software version is **not compatible** with v4.60 software. You will need to use new DM software from v4.60 to download the old data base file to a PC. After upgrading OfficeServ system to v4.60, upload the data base file which was save on the PC to the OfficeServ system.

V4.60 Software Compatibility Chart

	Card Software Version	MP V4.53c	New Release: MP V4.60 7030/7100/7200s: v4.60 (20120216) 7200/7400: v4.60 (20120206)
(SVMi-20E)	previous version	**Yes**	**Yes**
LP40 (SP40)	previous version	**Yes**	**Yes:** (New features not supported)
	V2.00, 20111209 (New version)	**Yes:** (New features not supported)	**Yes**
LCP	previous version	**Yes**	**Yes:** (New features not supported)
	V4.30, 20111209 (New version)	**Yes:** (New features not supported)	**Yes**
MGI-16/64	previous version	**Yes:** (New features not supported)	**Limitation(*)**
	V1.28, 20111209 (New version)	**Limitation(*)**	**Yes**
(Discontinued MGI cards)	previous version	**Yes**	**Yes:** (New features not supported)
OAS	previous version	**Yes**	**Limitation(**)**
	V2.03, 20111209 (New version)	**Limitation(*)**	**Yes**
CNF24	previous version	**Yes**	**Yes:** (New features not supported)
	V1.02, 20111125 (New version)	**Yes:** (New features not supported)	**Yes**
SMT-I Phones	previous version	**Yes**	**Yes:** (New features not supported)
	SMT-i3105: v1.56 (‘12.01.20) SMT-i5210: v1.36 (’12.01.20) SMT-i5220: v2.31 (’12.01.26) SMT-i5230: v1.26 (’12.02.04) SMT-i5243: v1.85 (’12.01.20) SMT-i5264: v1.25 (’11.11.16)	**Yes:** (New features not supported)	**Yes**
SMT-w5120	previous version	**Yes**	**Yes:** (New features not supported)
	V2.03.05 (’11.05.31)	**Yes:** (New features not supported)	**Yes**

Limitation(*)	Sending & Receiving DTMF on SIP Trunk and SPNET (Both in-band and out-band are not supported. So The feature using DTMF like Mobex is not supported.
Limitation(**)	If MPS is used on old OAS software, new feature is supported. If MGI is used on old OAS software, new feature is not supported.

The data base conversion principal stays the same. You will need to use the latest DM to download the old data base file. Then upload the old data base file to the system after the system is upgraded to new software.

There are some changes on the software upgrade procedure.

1) IT Tool

IT tool is no longer supported from v4.60. IT tool is replaced by embedded DM (Device Manager) and standalone DM.

2) DM (Device Manager)

a) DM has new security measure. ID and password of a IP phone cannot be set to the same. DM will not let you save the password if it is the same as ID. However, DM will let you upload the previous database that contains the same IP and password.
b) You can use either standalone DM or embedded DM to access the OfficeServ system. If you use standalone DM, make sure you are use the latest version. It is recommended to use embedded DM because it always synchronizes with the system software. Embedded DM (device manager) is available to all OfficeServ 7000 system now. Access to the embedded DM is as simple as type in the OfficeServ IP address from the Internet Explorer. It doesn't matter the access in from the private or public network. For example, if the OfficeServ IP address is 222.33.44.555. You can access the embedded DM by type in either

- http:// 222.33.44.555
- https:// 222.33.44.555

Note: Please always use the latest Java script on your PC.

c) DM can access embedded VM, ie. OS 7030, OS 7100, and OS 7200s now.

Device Manager with version 4.60 software is designed to support local and remote programming of the OfficeServ systems via LAN/WAN (IP) or serial (modem) connection. LAN/WAN connectivity should be the preferred option because of the speed and availability of the internet. In some cases were internet connectivity is not available, a serial modem connectivity can be used as an alternative to LAN connection, but with limitations. The Device Manager via modem is much slower and is limited in functionality.

Notes:

- *Device Manager (via modem) connectivity **cannot** be used to support **voicemail configuration or software package upgrading.***
- *The OS730, 7100, 7200s with IT Tool/Web Management did support voicemail configuration or software package upgrading via modem but **IT Tool/Web Management** is **not available** on OfficeServ **4.60 or higher** products.*
- *Understand the limitations with Device Manger (via modem) before electing to use it as an option to the IT toolWeb Management or Device Manager via LAN/WAN connectivity.*

DM has several advantages over IT.

a) Embedded DM is integrated with MP. If you use the embedded DM, you are sure you always use the same software version as MP.
b) DM is based on the Java technology. It means OS independent. DM can be used in Linux and Mac OS. However, DM saves system data base in the PC format. Don't run DM in other operation system to perform database conversion.

3) MP20/MP40

The v4.60 software packages cannot be upgrade through DM because the main software file size is over the 20M bytes limitation. You will need to copy v4.60 software to the SD card.

4) OS 7030/MP10a/MP20s

For these systems, you can either use DM or SD card to upgrade the system software. However, the numbers of software files have been increased from 7 to 9.

- <Previous>

  ap1av460.pkg, cs1av440.pkg, dr1av460.pkg, ms1av460.pkg, rd1av460.pkg, rt1av460.pkg, ws1av460.pkg
- <Current>

  ap1av460.pkg, cs1av440.pkg, dr1av460.pkg, ms1av460.pkg, rd1av460.pkg, rt1av460.pkg, ws1av460.pkg, **osdm.jar, osdmhelp.jar**

When upgrading system software to v4.60, the embedded voice mail (VM) data base is remained un-touched. That means, **you don't need to convert the embedded VM data base file**. You just need to convert the system data base file.

If you want to save embedded VM data base file, you need to use the following procedure.

a) System software is between v4.1x to v4.5x
   (1) You have to use **Web management** to download VM data base file. Same procedure as before.
   (2) You cannot use latest DM to save VM data base file when system has old software.
b) System software is v4.60
   (1) You have to use latest **DM** to download the VM data base file.
   (2) You can upload the VM data base file (which is either saved by the previous Web management or save by latest DM) to the system.

5) LP 40

- MP40 should be upgraded to V4.60 before upgrading LP40 because only new MP40 software version can recognize new LP40 file name.
- The designation of LP40 package is changed from LP4xxxxx.PGM to SP4xxxxx.PGM.
- The new LP40 package, SP40V200.PGM contains both LP40 bootrom and LP40 software file. When you try to upgrade LP40 package to V2.00 from an earlier version than V2.00 in MMC818, it will take about 13 minutes because OS7400 system tries to upgrade bootrom for the first 7 minutes and then LP40 package for about 6 minutes.

5.4 Software Upgrade Procedures

1. The OS7400 Upgrade Procedures

Any upgrade to V4.60 will default the database, so doing a backup with DM (Device Manager) is a must. Also the new files must be manually copied to the SD card using a PC.

1) Backup the database by using the latest DM.
2) Delete all files off the SD card.
3) Unzip the zipped file on the PC and copy all unzipped contents to the SD card.
4) Insert the SD card back into the switch and power cycle the switch.
5) Copy the previous database file back onto the switch.
6) Access MMC 818 with a phone and upgrade the LP40 or multiple LP40 cards has needed. Each card will take around 15 minutes to upgrade. Do not stop this process.
7) Upgrade any MGI-16, MGI-64 or OAS cards to the latest software version using the MGI-16 procedure.
8) Upgrade all CNF-24 cards using the upgrade procedure.
9) Do a backup onto a PC using DM program and complete a backup using KMMC to the SD card using MMC 815.
10) Upgrade all SMT-I phones.
11) Upgrade complete.

2. The OS7200 MP20 Upgrade Procedure

Any upgrade to V4.60 will default the database, so do a backup with Device Manager is a must.

1) Backup the Database to the PC.
2) Take the SD card out of the switch and put in PC. Delete all files off the SD card.
3) Unzip the zipped file on the PC and copy all unzipped contents to the SD card.
4) .
5) Insert the SD Card back into the switch and power cycle the switch.
6) Re-login into the switch after it boots into service and copy the database back to the switch. This restores the database to the switch.
7) Access MMC 818 and upgrade the LCP Card if this is a two cabinet OS7200 system.
8) Upgrade any MGI-16 and OAS card to be able to use any new features and hardware.
9) Upgrade all CNF-24 cards using the upgrade procedure.
10) Do a backup onto a PC using DM program and complete a backup using KMMC 815 to the SD card.
11) Upgrade all SMT-I phones.

12) Upgrade Completed.

3. The OS7200S MP20S Upgrade Procedure

Any upgrade to V4.60 will default the database, so doing a backup with Device Manager is a must. Start with downloading the latest DM program and using it to download the database.

1) Download the database to the PC using the latest DM program.
2) Download the MP20S program off the FTP site and UNZIP the files onto a folder.
3) Login with DM and access the FILE CONTROL section.
4) Select the folder with the unzipped version of 4.60 software and upload the files to the SD card. Overwrite any files showing duplicated. Make sure the INI is updated selecting the new files uploaded.
5) Reboot the switch and verify that the software shows V4.60 in MMC 727.
6) Login with DM and upload the database that was just downloaded.
7) Verify that the switch is stable and calls can be made.
8) Download a new database for a backup.
9) Upgrade any OAS or MGI-16 cards installed with the latest software.
10) Upgrade all SMT-I phones.
11) Upgrade Completed.

4. The OS7100 MP10A Upgrade Procedure

Any upgrade to V4.60 will default the database, so doing a backup with Device Manager is a must. Start with downloading the latest DM program and using it to download the database.

1) Download the database to the PC using the latest DM program.
2) Login with DM and access the FILE CONTROL section.
3) Select the folder with the unzipped version of 4.60 software and upload the files to the SD card. Overwrite any files showing duplicated. Make sure the INI is updated selecting the new files uploaded.
4) Reboot the switch and verify that the software shows V4.60 in MMC 727.
5) Login with DM and upload the database that was just downloaded.
6) Verify that the switch is stable and calls can be made.
7) Download a new database for a backup.
8) Upgrade any OAS or MGI-16 cards installed with the latest software.
9) Upgrade all SMT-I phones.
10) Upgrade Completed.

5. The OS7030 Upgrade Procedure

Any upgrade to V4.60 will default the database, so doing a backup with Device Manager is a must. Start with downloading the latest DM program and using it to download the database.

1) Download the database to the PC using the latest DM program.
2) Login with DM and access the FILE CONTROL section.
3) Select the folder with the unzipped version of 4.60 software and upload the files to the system. Overwrite any files showing duplicated. Make sure the INI is updated selecting the new files uploaded.
4) Reboot the switch which will take 15 minutes and verify the software shows V4.60 in MMC 727.
5) Login with DM and upload the database that was just downloaded.
6) Verify that the switch is stable and calls can be made.
7) Download a new database for a backup.
8) Upgrade all SMT-I phones.
9) Upgrade Completed.

6. MGI-16 andMGI-64 Upgrade Procedure

1) Unzip the files in the C drive in a folder called (MGI16) OR (MGI64)
2) Access a TFTP Program example (SOLAR WINDS) and select file and configure the access to the (C:\) drive only.
3) Access the START, RUN, CMD to access a telnet session from PC.
4) Type (TELNET XXX.XXX.XXX.XXX) to access the MGI card for programming. XX is the IP address of the MGI.
5) The IP address will be the one in MMC 831 for that card.
6) Login onto the card with user name of mgi and password of mgi12345.
7) Type in (ALLSET)
8) The system will respond with current IP Address which should be the MGI card IP address.
   a. Change this address if it needed.
9) The next prompt will be the SUBNET MASK which is 255.255.255.000
10) The next prompt will be the GATWAY. Put in your gateway.
11) The next prompt will be the I/O Server which is the **PC IP address**.
12) When the system responds, 20 seconds later, type in (REBOOT) to reboot the card.
13) The telnet session will disconnect after 20 seconds and 10 seconds later, the
    a. TFTP solar winds window will show the files loading. The card will reboot after the
    b. Upload.
14) After a few minutes, access DM 2.2.0 (MMC 727) and verify the software load and date is correct.
15) Upgrade Complete.

7. OAS Upgrade Procedure

1) Unzip the files in the C drive in a folder called (OAS1).
2) Access a TFTP Program example (SOLAR WINDS) and select file and configure the access to the (C:\) drive only.
3) Access the START, RUN, CMD to access a telnet session from PC.
4) Type (TELNET XXX.XXX.XXX.XXX) to access the OAS card for programming. XX is the IP address of OAS card.
5) The IP address will be the one in DM 2.2.2 (MMC 831) for that card.
6) Login onto the card with user name of mgi and password of mgi12345.
7) Type in (ALLSET)
8) The system will respond with current IP Address which is the MGI card IP address. Change this address if it needed.
9) The next prompt will be the SUBNET MASK which is 255.255.255.000
10) The next prompt will be the GATWAY which is 105.52.21.1. Put in your gateway.
11) The next prompt will be the I/O Server which is the PC IP address.
12) When the system responds, 20 seconds later, type in (REBOOT) to reboot the card.
13) The telnet session will disconnect after 20 seconds and 10 seconds later, the TFTP solar winds window will show the files loading. The card will reboot after the upload.
14) After a few minutes, access MMC 727 and verify the software load and date is correct.
15) Upgrade Complete.

8. CNF-24 Upgrade Procedure

1) Unzip the voice prompts onto a folder on your PC. The main CNF-24 program should not need to be unzipped for this upgrade.
2) Login onto the switch using the latest DM program.
3) Access the UTIL section from the main screen.
4) Access the PACKAGE UPDATE from this UTIL section.
5) You will see CNF-24 card on the switch
6) Select the CNF-24 card and select the (…) to browse to the upgrade file.
7) Select upload and restart after selecting the file.
8) You will see the progress of the upgrade. 2 minutes max to complete.
9) The CNF-24 card will restart after the upgrade.
10) Login into the switch and access MMC 727 and verify the correct version.
11) Upgrade Completed.

9. CNF-24 PROMPT Upgrade

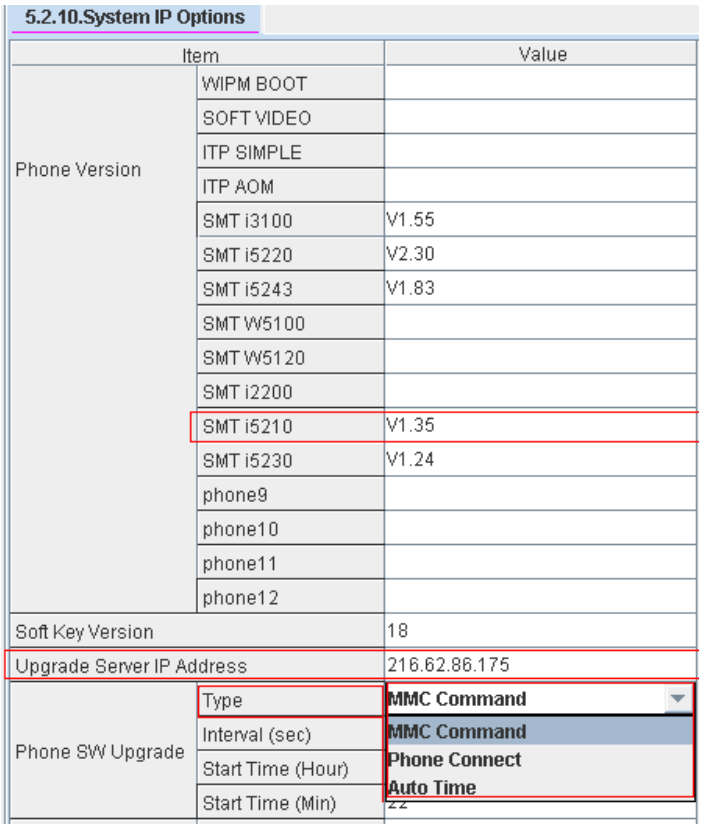
1) Download the PROMPT file and unzip it onto a folder on your pc.
2) Access a FTP program and Upload prompts to /mnt/nand0/prompt/ by using FTP. (ID: admin, PW: Samsung
3) Copy all the prompts onto this location in the previous step. You can override the prompts that show a duplicate.

10. SMT-I Phone Upgrade Procedure

Pull software from phone

1) Run TFTP or HTTP server on the PC. PC must be in the same network as the OfficeServ.
2) Set the root directory of TFTP or HTTP to the main unzipped phone software folder. Main folder must contain a subfolder called "ITP-SERIES".
3) Access phone software upgrade menu from the engineering mode. Two ways to enter to the engineering mode.
    a. Press and hold * key while powering up the phone, or
    b. Press ***153#** while phone displays the phone information.
        i. To display phone information, Menu -> Phone -> Phone Information
4) Set PC IP address to the "Upgrade Server" menu and start software upgrade

Push software to phones



1) Run TFTP or HTTP server on the PC. PC must be in the same network as the OfficeServ.

2) Set the root directory of TFTP or HTTP to the main unzipped phone software folder. Main folder must contain a subfolder called "ITP-SERIES".

3) In DM 5.2.10, set software version number, upgrade Server IP address (PC), and type (MMC command). Upon saving the DM setting, system will push the software to phone.