powerful technology.
affordable growth.

4.65 Feature Package Manual

SAMSUNG

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.

PRINTED IN THE USA

1. TABLE OF CONTENTS

2. INTRODUCTION

The purpose of this manual is to introduce and explain the new features offered in **V4.65** main system feature package for the **OfficeServ 7000 Series** of business telephone systems.

The major focus of Version **4.65** is Security. The need for remote access and connectivity brings challenges to protect the phone system from malicious internet requests from unwanted sources. Who and what gets access and how to control them required new system settings. New password encryption, larger 6 digit passwords, improved voice mail security and various IP White lists are all new tools in V4.65 to make the OfficeServ system more secure from malicious hackers.

In addition to the added security, several enhancements have been added to improve support for and use of standard SIP phones, a simpler 2 digit directory search and a few default setting have changed.

There is no new hardware introduced with V4.65. However a new Device Manager Version 4.65 is required to support these new settings and encryption. The PC running Device Manager V4.65 must run **Java 6**. Device Manager is not compatible with Java 7.

The chart in the next section lists the features and changes supported by V4.65 along with the OfficeServ 7000 Series system(s) supported.

3. FEATURE & HARDWARE LIST

FEATURE	7030	7100	7200S	7200	7400
Password Encryption	Yes	Yes	Yes	Yes	Yes
Secure DM Login	Yes	Yes	Yes	Yes	Yes
SIP Station Security	Yes	Yes	Yes	Yes	Yes
VM/AA Password Change	Yes	Yes	Yes	Yes	Yes
DM IP White List	Yes	Yes	Yes	Yes	Yes
Phone IP White List	Yes	Yes	Yes	Yes	Yes
Management IP White List	Yes	Yes	Yes	Yes	Yes
IP Address Range Rule	Yes	Yes	Yes	Yes	Yes
Add Trunk Access Code for SIP Phone Log	Yes	Yes	Yes	Yes	Yes
2 Digit Directory Name Search	Yes	Yes	Yes	Yes	Yes
Unconditional Ring for SIP Phones	Yes	Yes	Yes	Yes	Yes
SIP Cause Message Display	Yes	Yes	Yes	Yes	Yes
TOS Field for SIP Packet	No	No	No	No	Yes
SIP Privacy Header	Yes	Yes	Yes	Yes	Yes
Single CID Number	Yes	Yes	Yes	Yes	Yes
No Response for SIP Comm Exclusive Option	Yes	Yes	Yes	Yes	Yes
Default Data Value Changes	Yes	Yes	Yes	Yes	Yes
Change Telenet ID & Password	Yes	Yes	Yes	Yes	Yes
New SMTi Series Phone Software	Yes	Yes	Yes	Yes	Yes

HARDWARE	7030	7100	7200S	7200	7400
No New Hardware	**No**	**No**	**No**	**No**	**No**

4. FEATURE DESCRIPTION

This chapter lists the features in the V4.65 software package. Each feature is broken down into four 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

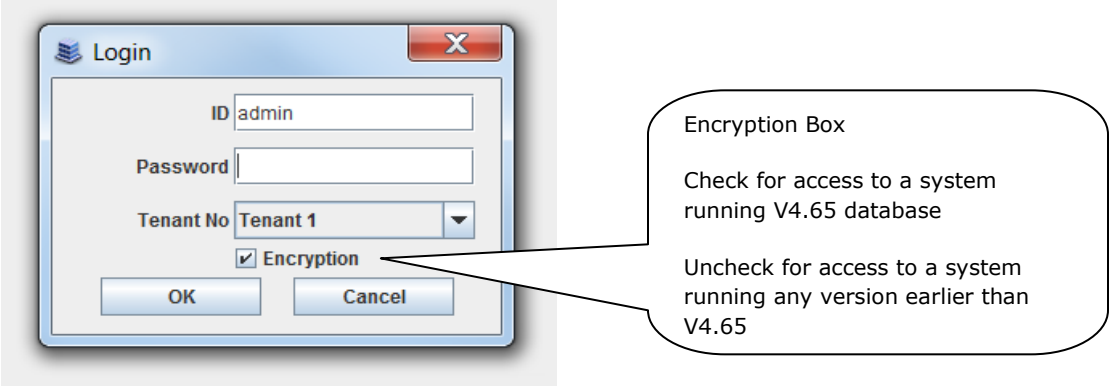
4.1 Password Encryption

GENERAL DESCRIPTION

The following passwords are encrypted for enhanced security. They are appear as "****" in each menu and can't be read from backup database.

- DM 2.1.7 Admin Password for Device Manager Login
- DM 2.7.2 SIP Phone Password
- DM 5.2.13 Authorization Password for SIP Carrier

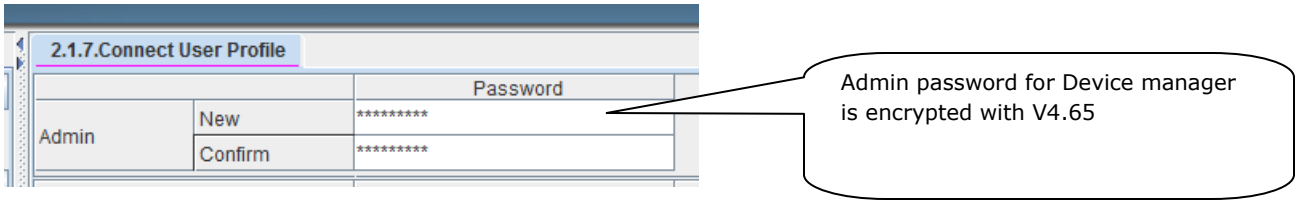
Technician should access V4.65 system with V4.65 DM**.** When using an earlier version of DM, access to the system is not permitted because the passwords are encrypted in V4.65. When using DM V4.65 to access an earlier database technician must uncheck (deactivate) the Encryption Box at time of login.



PROGRAMMING

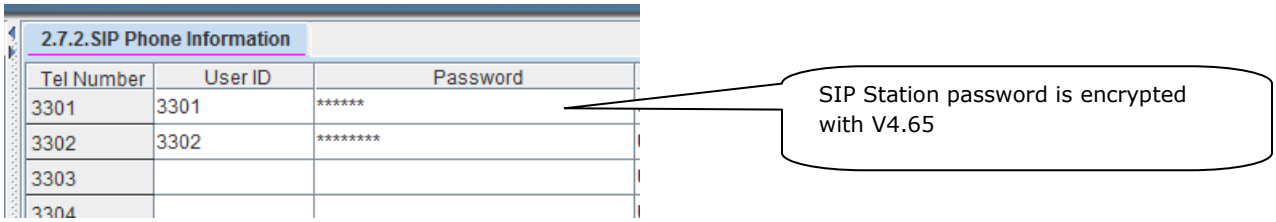
Admin Password for Device Manager

Device Manager Menu **2.1.7 Connect User Profile** shows the encrypted Admin Password as *******



SIP Phone Password

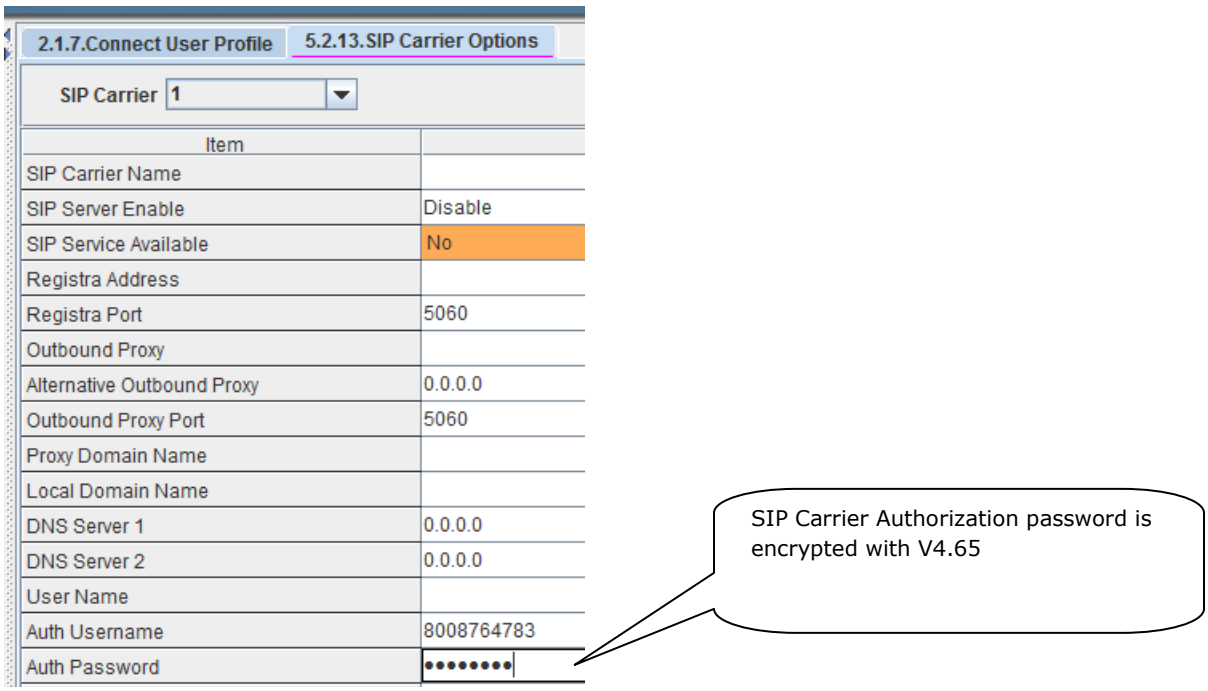
Device Manager Menu **2.7.2 SIP Phone Information** shows the encrypted Admin Password as *******. SIP station password must be minimum 6 digits up to a maximum of 8 digits.



NEW FIELD	PURPOSE
Password	Assign an encrypted SIP station password for each 3rd Party SIP station in the system. Must be 6 ~ 8 digits

Auth Password for SIP Carrier

Device Manager Menu **5.2.13 SIP Carrier Options** shows encrypted **Auth Password** as ********



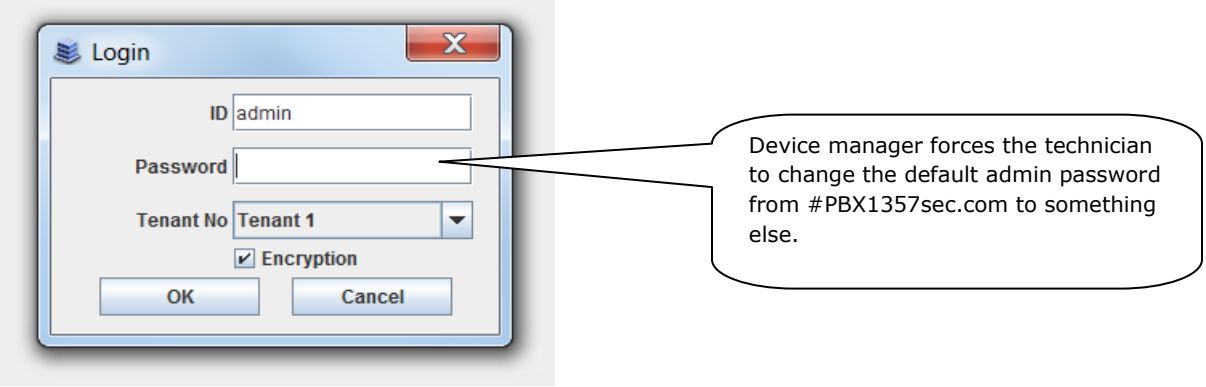
4.2 Secure Device Manager Login

GENERAL DESCRIPTION

System access using Device Manager is now more secure than with previous system software versions. Below are the changes.

- **Must Change Default DM Password**

  The new Default DM Password is " **#PBX1357sec.com** " and it must be changed immediately after the first login attempt. This will prevent future sites from sitting out there with the default "samsung" password just waiting for some hacker scanning Samsung MAC address.



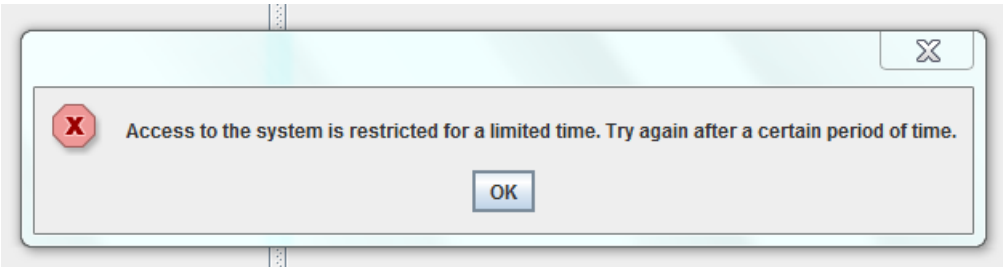
- **DM Repetitive Login Control**

  There are now two settings to control repeated attempts to login in with an incorrect DM password.

  DM Login Retry Limit – The number of unsuccessful attempts before DM is locked out.

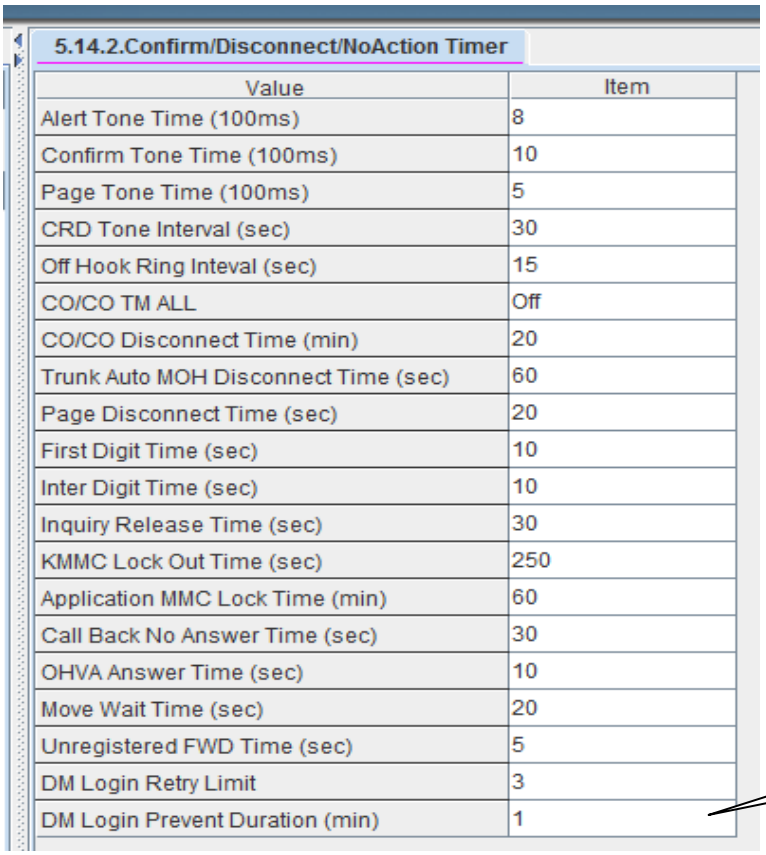
  DM Login Prevent Duration (min) – This value determines how many minutes the system prevents a user from logging in again after DM is locked out. The prevent duration is measured in minutes with a range of 1 ~ 60 minutes.

This is the message displayed after exceeding the number of incorrect login attempts



PROGRAMMING

Device Manager Menu **5.14.2 Confirm/Disconnect/No Action Timer** has a new field added to the end of the list to set the **DM Login Prevent Duration** time.



5.14.2.Confirm/Disconnect/NoAction Timer

Value	Item
Alert Tone Time (100ms)	8
Confirm Tone Time (100ms)	10
Page Tone Time (100ms)	5
CRD Tone Interval (sec)	30
Off Hook Ring Inteval (sec)	15
CO/CO TM ALL	Off
CO/CO Disconnect Time (min)	20
Trunk Auto MOH Disconnect Time (sec)	60
Page Disconnect Time (sec)	20
First Digit Time (sec)	10
Inter Digit Time (sec)	10
Inquiry Release Time (sec)	30
KMMC Lock Out Time (sec)	250
Application MMC Lock Time (min)	60
Call Back No Answer Time (sec)	30
OHVA Answer Time (sec)	10
Move Wait Time (sec)	20
Unregistered FWD Time (sec)	5
DM Login Retry Limit	3
DM Login Prevent Duration (min)	1

NEW FIELD	PURPOSE
DM Login Prevent Duration	This value determines how many minutes the system prevents a user from logging in again after DM is locked out. The prevent duration is measured in minutes with a range of 1 ~ 60 minutes. **Default is 1 minute**

4.3 SIP Station Security

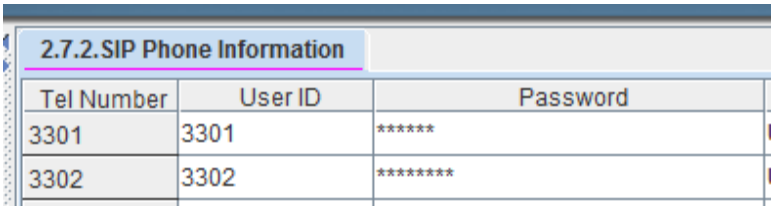
GENERAL DESCRIPTION

With V4.65 software, SIP stations do not have default ID and passwords assigned. This prevents unauthorized registration. The installing technician must create IDs and passwords for each SIP station. The password must be 6~8 digits.

When upgrading an earlier database to V4.65, the default ID and passwords for SIP stations will be deleted. The technician must assign new IDs and new passwords of 6~8 digits.

PROGRAMMING

Device Manager Menu **2.7.2 SIP Phone Information** is used to assign User IDs and Passwords for all SIP stations. These are not new fields to DM V4.65. However if there is a Tele Number assigned as a SIP station it must be assigned an ID and password.



FIELD	PURPOSE
User ID	No default ID is provided. Technician must enter this value
Password	No default password is provided. Technician must enter this value

4.4 VM/AA Password Change

GENERAL DESCRIPTION

OfficeServ V4.65 system software and SVMi-20i V6.02 combined with Device Manager V4.65 provides improved VM/AA security settings to control use of voice mailbox/subscriber passwords. Mailboxes with default password are a security risk for toll fraud. Below are the three settings available in **DM 8.5 System Parameters**

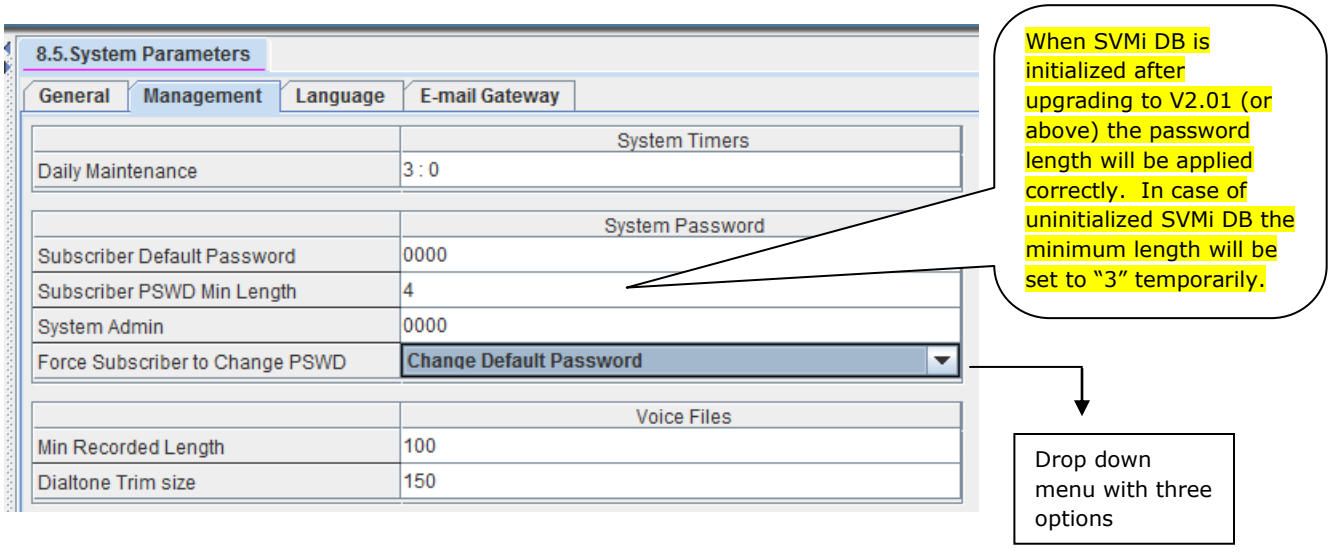
1. None: this is the same as previous password policy for embedded SVM and SVMi-201
2. Change Default Password: When a subscriber logins in for the first time the user is forced to change the default password before they gain access to the voice mailbox. This is the default setting in V4.65 software. Password can be a simple one. This is the **DEFAULT** setting for North America
3. Change Default and Deny Simple One: Same as option 2 above plus the password cannot be a simple repeating numbers (like 1111, 2222) ascending or descending numbers (like 1234, 4321) or users own extension number. Highly recommended.

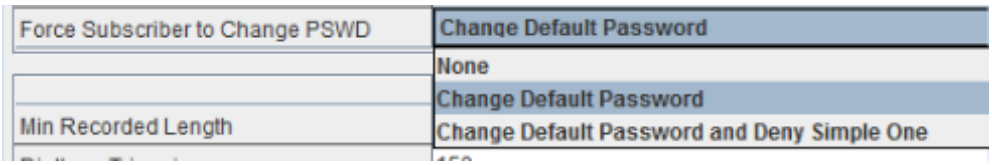
Note: SVMi-20i software must be upgraded to V6.02 to support these options. Embedded SVM in V4.65 system package support these options. DM V4.65 must be used to view and select these options.

PROGRAMMING

Device Manager Menu **8.5. VMAA /System Parameters / Management** has a new field with a drop down menu to select Subscriber Password Options.

8.5 System Parameters





FIELD	PURPOSE
Force Subscriber to change PSWD	Used to select password control options. Click on arrow to see menu.
None	Same as previous software. Can keep the default simple password like 1234
Change Default Password	Forces user to change password first time they log in. Can be a simple password
Change Default Password and Deny Simple One	Must use a password that does not repeat numbers in ascending or descending order.

4.5 DM IP White List

GENERAL DESCRIPTION

This new DM IP White List adds another level of security by controlling what PCs can access the system using Device Manager. Only the IP addresses listed can connect to the system using DM.

There are two ways to input DM IP addresses. Either enter each IP address individually or input an IP address range.

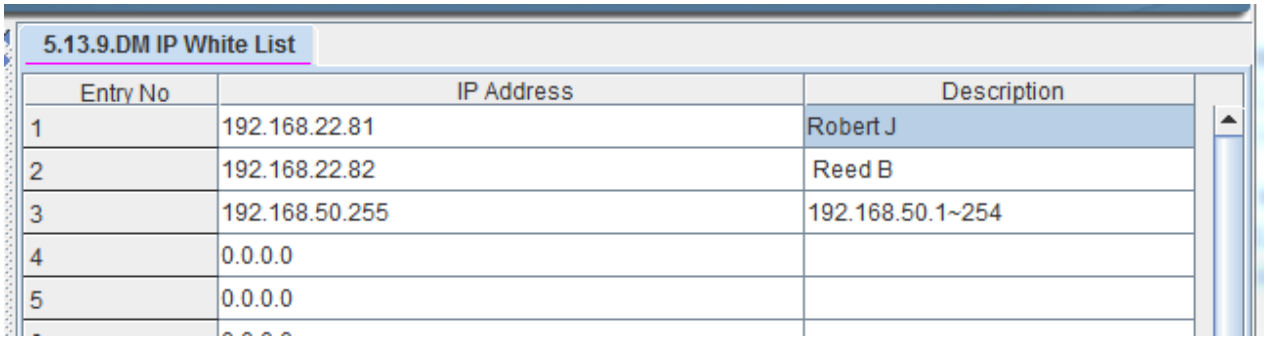
Note: If there are no IP addresses in the list, then the system is *fully open* so any PC using DM can access the system. After upgrading a system to V4.65 the DM IP White List has no valid IP address so the system is vulnerable to hacking.

If current PC is not listed in DM IP White List the following message will be displayed:

> **"Current PC in not allowed to access system database. Please use another PC or check DM Access IP List in DM 5.13.9"**

PROGRAMMING

Device Manager Menu **5.13.9 DM IP White** is a list of IP address of PCs that can access Device Manager.



FIELD	PURPOSE
IP Address	Enter an individual IP address or an IP address range
Description	A 16 character description of who or where this IP address is, or identifies the range of IP addresses.

4.6 Phone IP White List

GENERAL DESCRIPTION

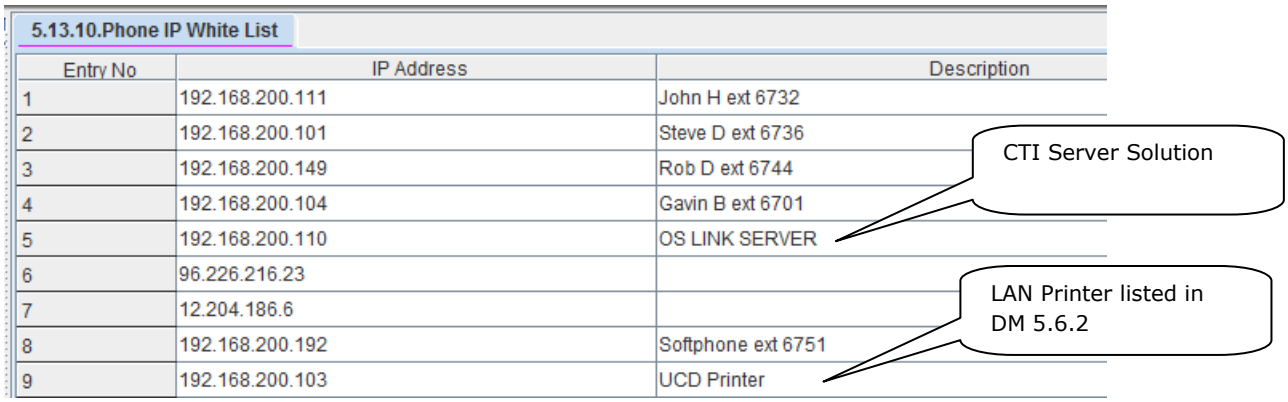
The Phone IP White List in V4.65 provides another level of security by identifying what Samsung IP phones, SIP Phones, PCs or Servers running CTI solutions and LAN Printers can access the OfficeServ system.

After upgrading a system to V4.65 using Device Manager V4.65 the IP White is has no valid IP addresses so all IP/SIP/WIP phones, CTI Solutions or LAN printers can't register to the system. A technician has three options to restore connectivity for these devices

1. Use DM menus 6.2.2 & 6.2.3 to set each IP & SIP phone to IP White List 'DISABLE".
2. Enter an IP address range in IP Phone White List to cover all IP devices.
3. Copy and Paste IP addresses from DM menu 6.2.2 & 6.2.3 or MMC 840.

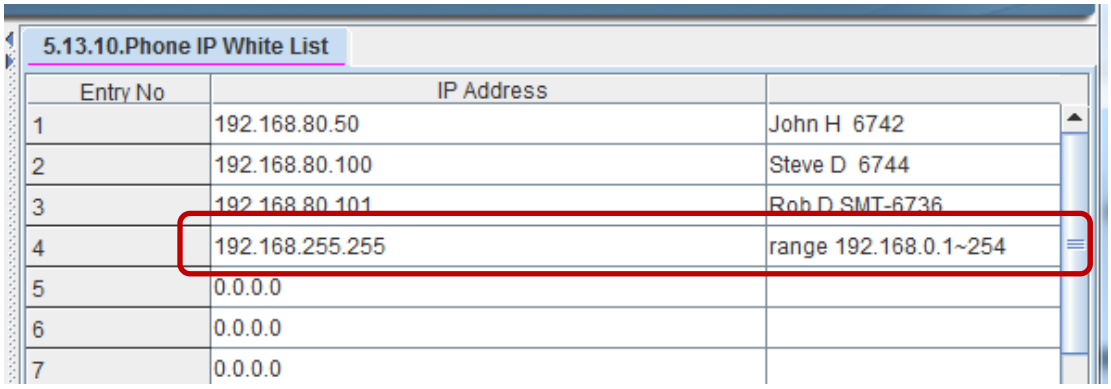
PROGRAMMING

Device Manager Menu **5.13.10 Phone IP White List**. Even though this menu is named Phone IP white list it is also used for CTI solutions and LAN printers as pointed out below.

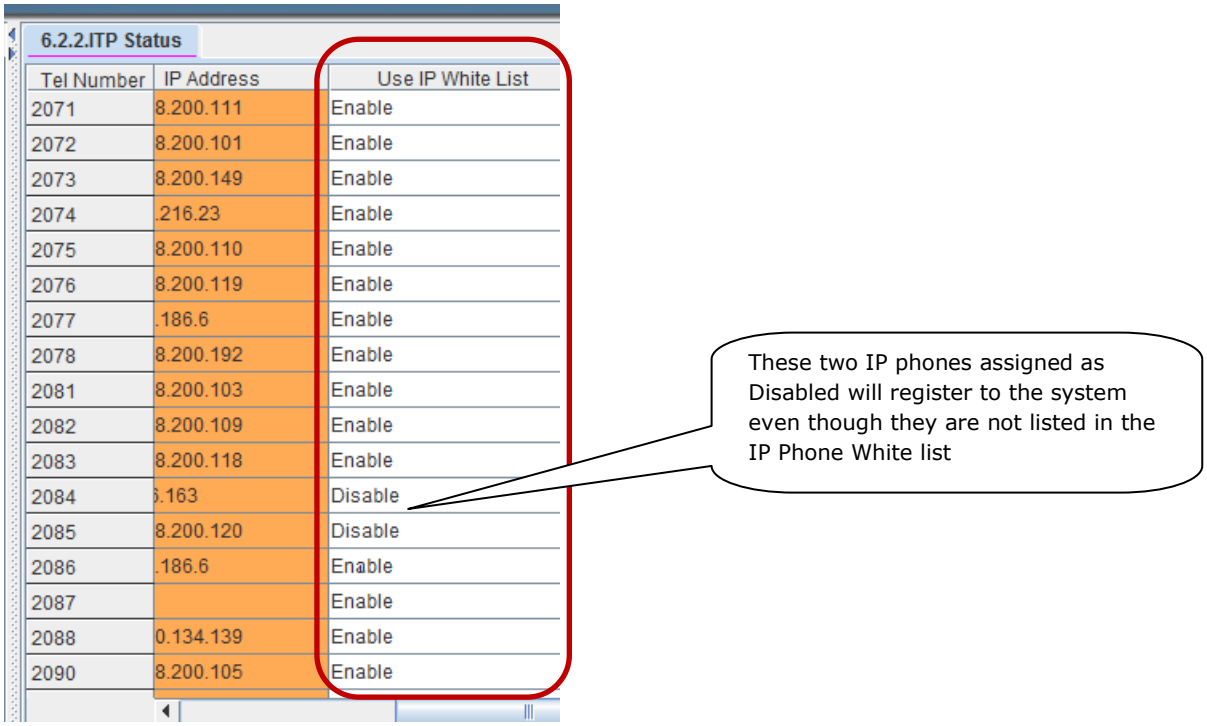


FIELD	PURPOSE
IP Address	Enter an individual IP address or an IP address range
Description	A 16 character description of who or where this IP address is, or identifies the range of IP addresses.

Device Manager Menu **5.13.10 Phone IP White List** with an entry showing an IP address range highlighted in the in red box

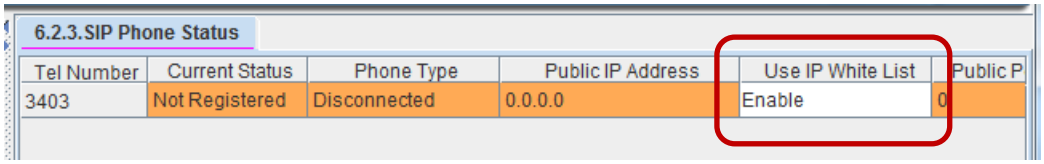


Device Manager Menu **6.2.2 ITP Status** is used to Enable or Disable the IP White List on an individual basis.



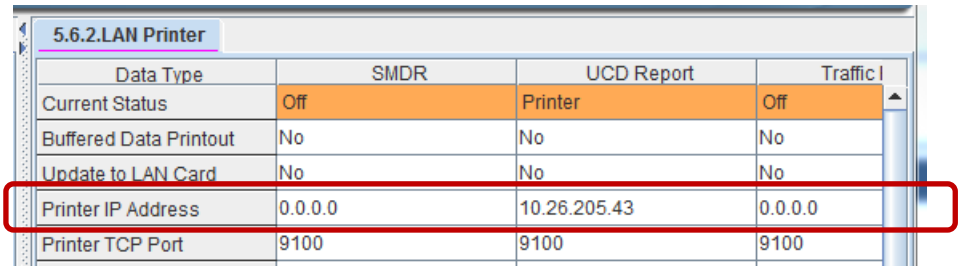
FIELD	PURPOSE
Use IP White List	Set to Enable or Disable. If set to Disable this IP phone can be registered to the system even though it is not listed in the Phone IP white List

Device Manager Menu **6.2.3 SIP Phone Status** is used to Enable or Disable the IP White List on an individual basis.



FIELD	PURPOSE
Use IP White List	Set to Enable or Disable. If set to Disable this IP phone can be registered to the system even though it is not listed in the Phone IP white List

LAN printers listed in Device Manager Menu **5.6.2 LAN Printer** must be added to the IP Phone White List if the White List is used. There is no IP White List Enable/Disable option for LAN printers.



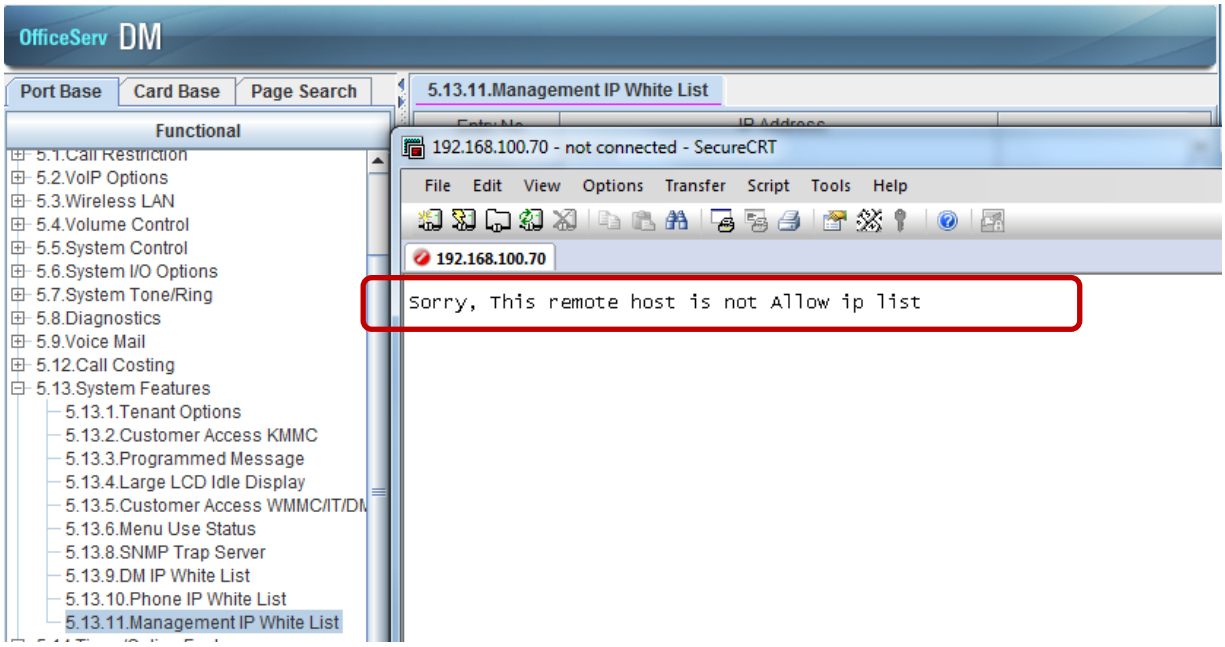
4.7 Management IP White List

GENERAL DESCRIPTION

For added security the Management IP White List defines the IP addresses that are allowed for Telenet, FTP Server, and SMDR. These IP address are defined in DM menu 5.13.11. If there are no entries in this list these functions will not be available.

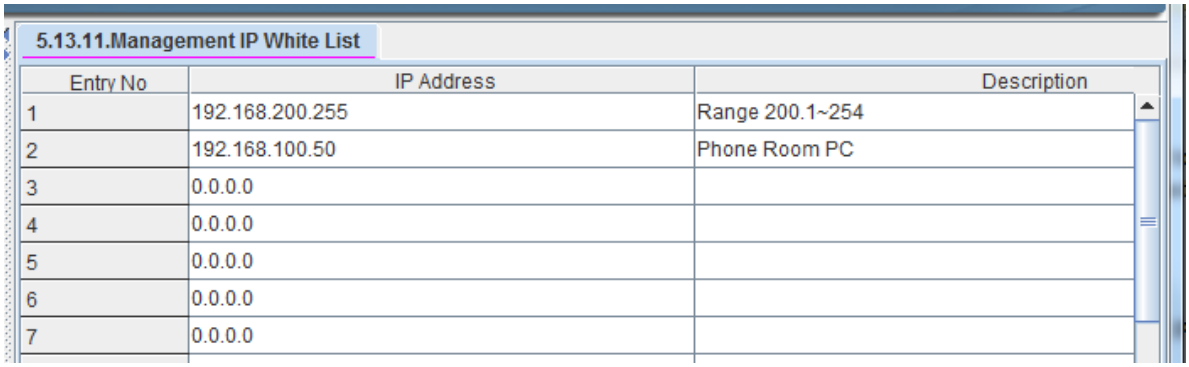
After upgrading to V4.65 the Management IP White List has no valid IP address so all Telenet, FTP or SMDR access is denied. Technician must enter IP address to use these functions.

Note: If Management IP White List has no entries a user will see this error when attempting to set up a Telenet session.



PROGRAMMING

Device Manager Menu **5.13.11 Management IP White List** is used to list the IP address of PCs that will be used for SMDR, FTP and Telenet functions. The example below shows an IP range that can be used and a single IP address of the PC in the Phone Room.



FIELD	PURPOSE
IP Address	Enter an individual IP address or an IP address range for Telenet, FTP or SMDR access.
Description	A 16 character description of what or where this IP address is, or identifies the range of IP addresses.

4.8 IP Address Range Rule

GENERAL DESCRIPTION

When listing IP addresses in the IP Phone White List, DM White List or Management IP White List, it may be easier or more suitable to enter them as a range of IP addresses instead of individual entries.

This table shows the three schemes to enter a range of IP addresses.

IP address format	IP address range	
A.B.C.255	A.B.C.1 ~ A.B.C.254	
A.B.255.255	A.B.0.1 ~ A.B.255.254	**See sample of this entry below**
A.255.255.255	A.255.255.254	

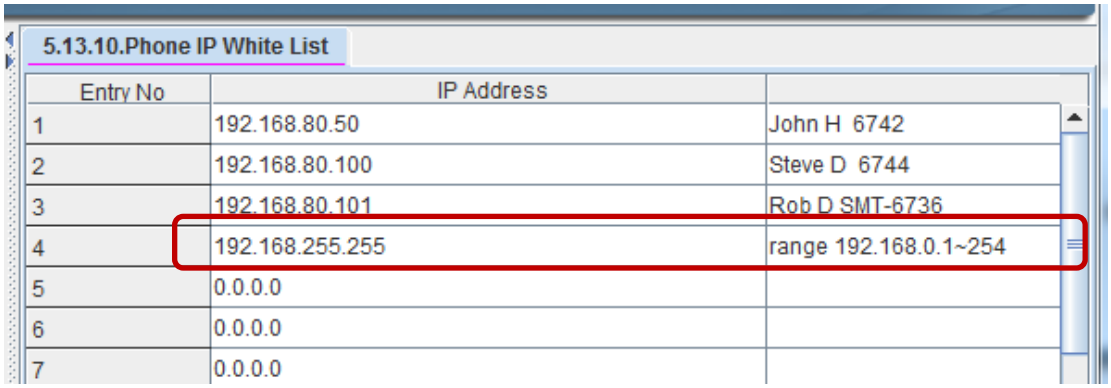
PROGRAMMING

These Device Manager Menus can use the IP address range method.

5.13.9 DM IP White Options

5.13.10 Phone IP White List. See the sample range entry below in red box.

5.13.11 Management IP White List

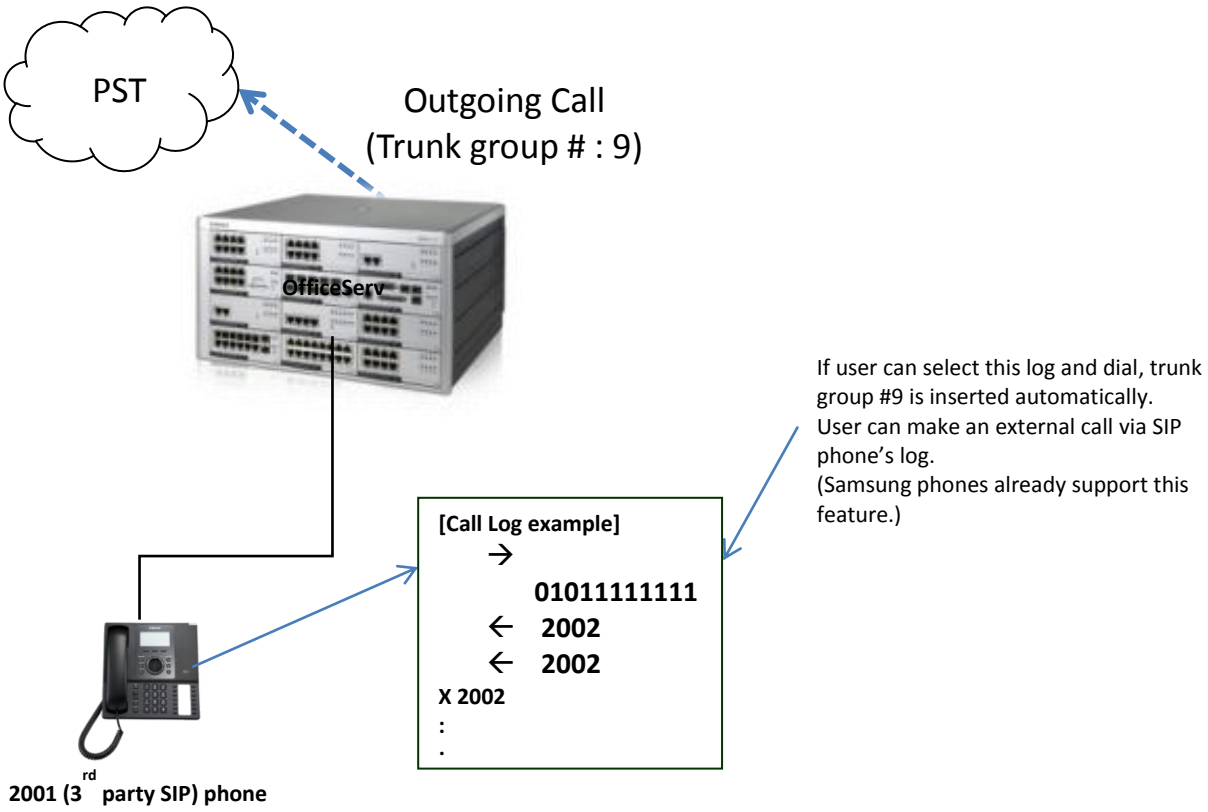


FIELD	PURPOSE
IP Address	List the IP address allowed. Can be an individual address or a range as indicated in the red box.
Description	Describe who or where this IP address is, or identifies the range of IP addresses.

4.9 Add Trunk Access Code for SIP Phone Log

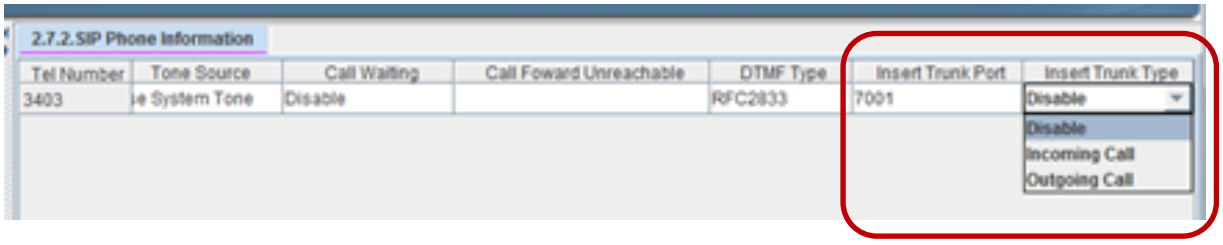
GENERAL DESCRIPTION

With V4.65 system software the trunk access code can be automatically inserted when user selects a number to dial from the Call Log of a SIP phone. Samsung IP phones already support this feature.



PROGRAMMING

DM Menu 2.7.2 SIP Phone Information has two new fields to control use of third party SIP Phone call log for incoming and outgoing calls.



FIELD	PURPOSE
Insert Trunk Port	Enter the LCR access code, TRK number or TRK Group to be inserted. When dialing numbers from the SIP phone call log this access code is automatically inserted. In the case of incoming calls this access code is inserted in front of the CID number stored in the SIP phone call log. **Default** : Blank
Insert Trunk Type	Select **Outgoing Call** setting to insert the Trunk Port entry automatically for outgoing calls from SIP Phone Log. Select **Incoming Call** setting to insert the Trunk Port entry automatically in front of CID number when storing in the SIP phone Call Log. Select **Disable** to not use this feature. **Default**: Disabled

Hint: Use "9" LCR access code in Insert Trunk Port and select Incoming Calls for Insert Trunk Type. If LCR access code is stored in front of each number in call log then it will be available for outgoing calls.

4.10 2 Digit Directory Name Search

GENERAL DESCRIPTION

With system software earlier than V4.65 users could only search directories on the first digit, then volume UP/Down to find a specific directory name. If there were 50 names under the letter "J" the user had to look through all of them. With V4.65 users can enter two letters to refine the search. Now when searching the directory for the name "John" in a list of 50 names beginning with "J" a user can enter "JO" and the list begins with the first name matching "JO".

2001	janet
2002	jackie
2003	john
2004	joseph
2005	jacob
2006	jay
2007	joanne
2008	jeff
2009	jimmy
2010	joel
2011	joe
2012	janet
2013	jenniffer
2014	jose
2015	jean
2016	jessica

Pressing "5" to search on "J" will provide a list of the 16 directory names in this list, starting with jackie, then press volume up to continue through these names; jacob, janet, jay, jean, jeff, jenniffer, jessica, jimmy, joanne, joe, joel and then john.

Use two digits search, press "5" then # to enter the second digit. Press"6" three times to enter "O". The list starts with joanne, joe, joel and then john

PROGRAMMING

There is no programming necessary to use two digit directory search feature.

USER INSTRUCTIONS

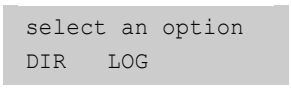
To use two-digit directory search feature from any Samsung OfficeServ Display phone:

At any iDCS, ITP-51xx, DS-50xx or SMTi series phone

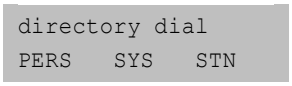
a. Press 'Scroll' button and select the 'CALL' soft key.

```
3100:Admin
CALL  OTHER ANS->
```

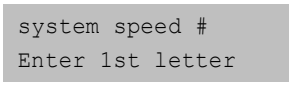
b. Select the 'DIR soft key.



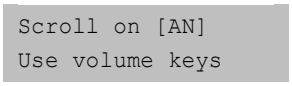
c. Choose one soft key among 3 directory options.



d. Enter one or two characters to search a name you are looking for.



e. You can press '**#**' key then enter 2nd letter.

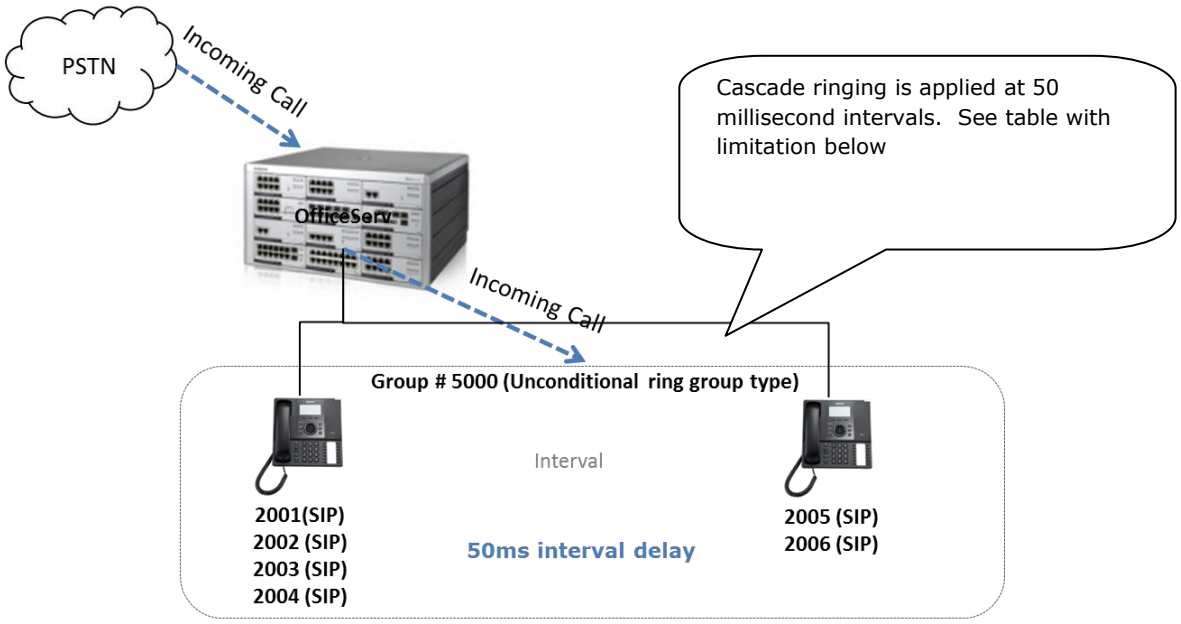


4.11 Unconditional Ring for SIP Phones

GENERAL DESCRIPTION

V4.65 supports "Unconditional Ring" mode for SIP stations assigned as a member of a Station Group. With previous versions SIP station would not ring if assigned to a station group using unconditional ring mode.

Note: If SIP extensions are added in this group, system provides **cascade ringing**, not simultaneous ringing.



Limitation

In case of 'Unconditional Ring' mode, the maximum members of an UCD group are reduced as indicated below.

System	Number of Members	Number of SIP phone Member
OS7030	16	8
Other Systems	32	10

Interval processing delay

a. OfficeServ system sends 'SIP INVITE' message to 4 group members at once.

b. And every interval delay for the SIP INVITE is 50ms.

c. Logically, total delay will be '400ms' between 1st and 9th SIP INVITE message.

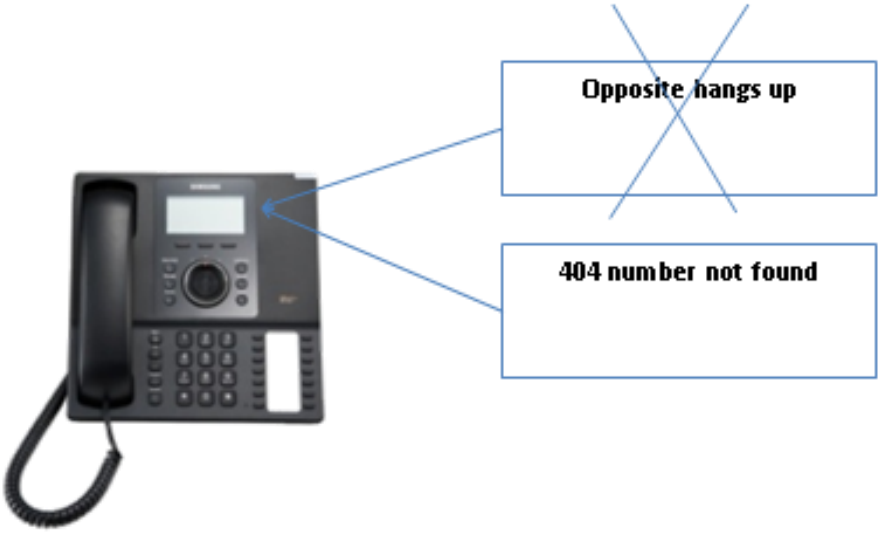
PROGRAMMING

There are no special steps required to support a station group set to "Unconditional Ring" mode with SIP stations as members. Programing procedure has not changed. DM menu 4.1.1 (MMC601) supports SIP extension as member of a group with unconditional ring mode assigned.

4.12 SIP Cause Message Display

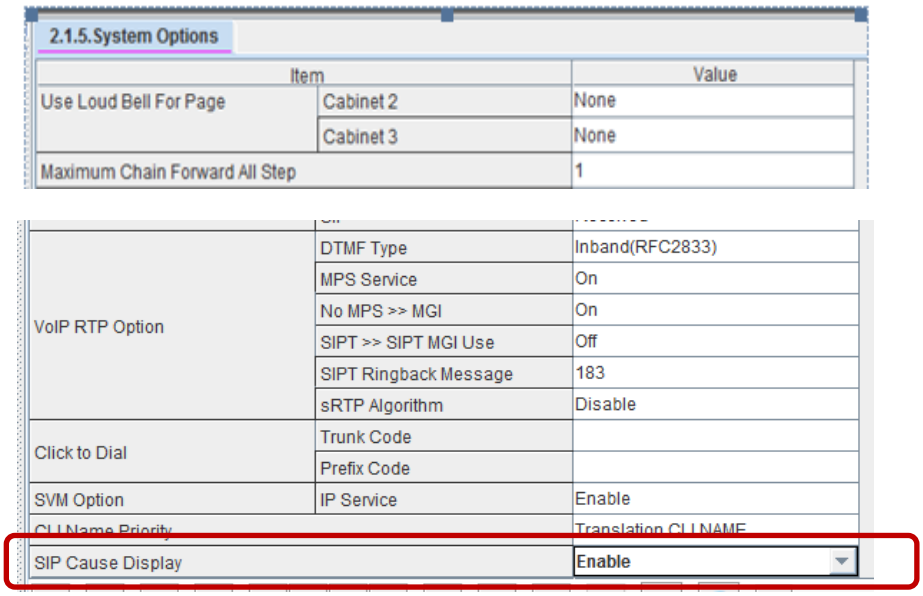
GENERAL DESCRIPTION

SIP Cause Messages such as 4xx, 5xx and 6xx can be optionally displayed on the phone instead of OfficeServ messages.



PROGRAMMING

Device Manager Menu **2.1.5 System Options**



2.1.5.System Options

Item		Value
Use Loud Bell For Page	Cabinet 2	None
	Cabinet 3	None
Maximum Chain Forward All Step		1
VoIP RTP Option	DTMF Type	Inband(RFC2833)
	MPS Service	On
	No MPS >> MGI	On
	SIPT >> SIPT MGI Use	Off
	SIPT Ringback Message	183
	sRTP Algorithm	Disable
Click to Dial	Trunk Code	
	Prefix Code	
SVM Option	IP Service	Enable
CLI Name Priority		Translation CLI NAME
SIP Cause Display		Enable

NEW FIELD	PURPOSE
SIP Cause Display	To Enable or Disable display of SIP Cause Messages

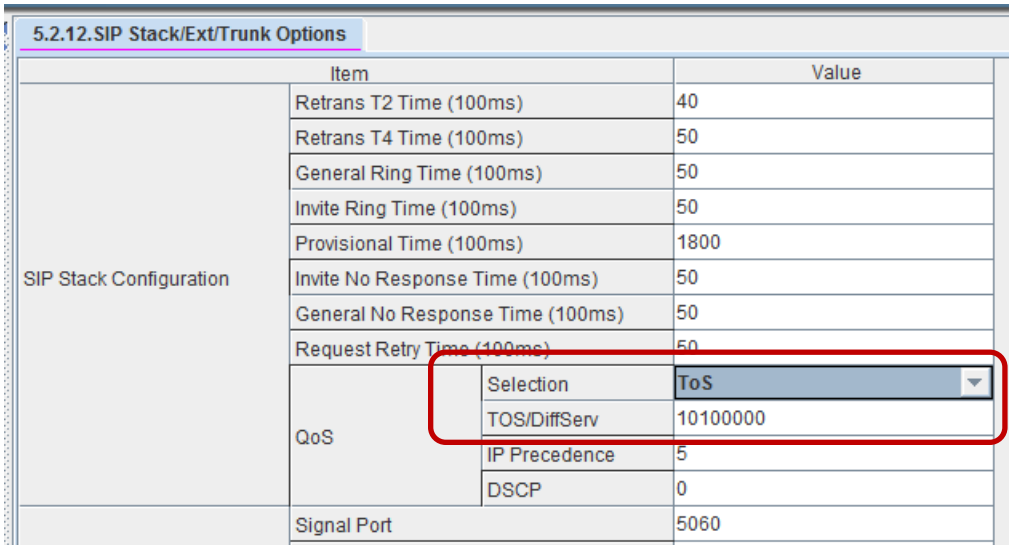
4.13 TOS Field for SIP Packet

GENERAL DESCRIPTION

With V4.65 software technicians can change the TOS field of the IP Header that enables CoS Settings as required. This option is only available on OfficeServ 7400 systems.

PROGRAMMING

Device Manager Menu **5.2.12 SIP Stack/EXT/Trunk Options** provides drop down menu to select the TOS and modify settings to change TOS bit field for a SIP Signaling packet.



FIELD	PURPOSE
Selection	Select ToS, IP Precedence or DSCP
TOS/DiffServ	Modify the TOS bits as required to adjust pack-flow grouping or allow for more CoSs

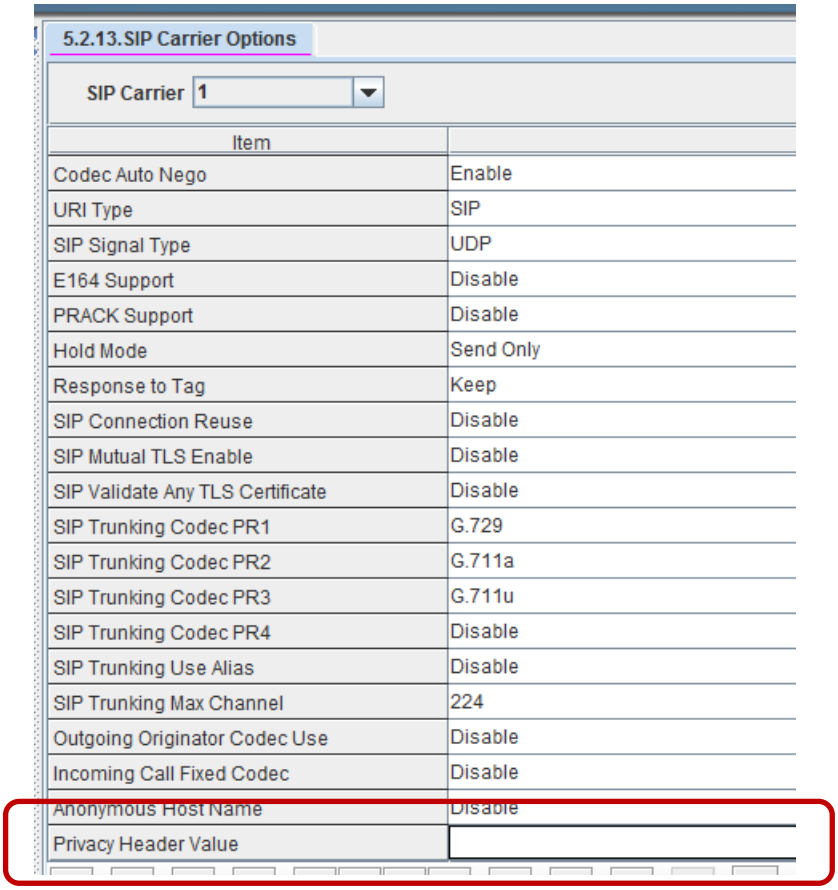
4.14 SIP Privacy Header

GENERAL DESCRIPTION

Version 4.65 system software provides a new SIP Privacy Header Value setting so it can be changed as required. With previous versions the SIP Privacy header could not be changed.

PROGRAMMING

Device Manager Menu, **5.2.13 SIP Carrier Options** provides a new setting for the Privacy header Value.



FIELD	PURPOSE
Privacy Header Value	Used to change the header value to : header, session, user, none, critical, token ID …….

4.15 Single CID Number

GENERAL DESCRIPTION

With V4.65 system software users with **Station Pair** can send a single Caller ID Number for both paired extensions. This is an ON or OFF setting.

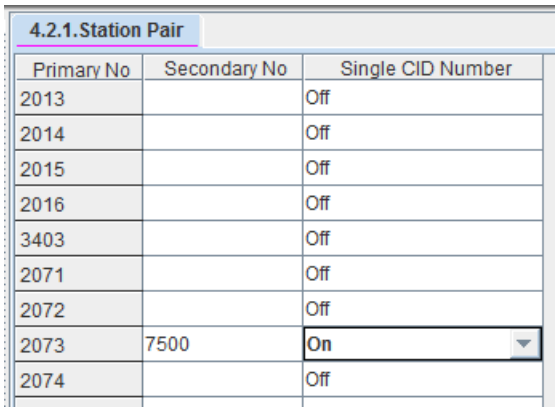
Single CID Number

ON: Send a single CID number for both paired extensions. The number sent will be the CID number assigned to the Primary extension in DM 2.4.3 Send CLI Number. (MMC 321).

OFF: The Primary and Secondary extensions will each send the number assigned in DM 2.4.3 Send CLI Number (MMC 321).

PROGRAMMING

Device Manager Menu **4.2.1 Station Pair** has a new field titled Single CID Number. Setting ON or OFF will determine whether the system sends a single CID number for both the Primary and Secondary numbers.



FIELD	PURPOSE
Single CID Number	Used to select Single CID Number option. **ON** = send a single CID number **OFF** = send individual CID numbers for both the Primary and Secondary numbers. **Default is OFF**

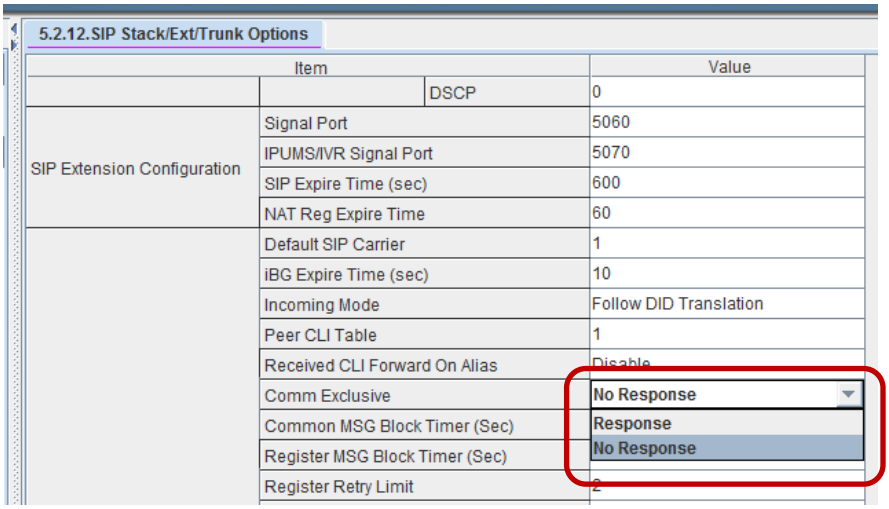
4.16 No Response for SIP Comm Exclusive Option

GENERAL DESCRIPTION

For additional security against anonymous hacker via SIP trunk connection the "None" option has been replaced with a new option titled "No Response" to the SIP Communication Exclusive settings. With this Carrier Exclusive selection the OfficeServ system will ignore all the SIP messages from an unauthorized IP address. The previous "None" option did not prevent any unauthorized traffic.

PROGRAMMING

Device Manager Menu, **5.2.12 SIP Stack/Ext/Trunk Options**, has a new "No Response" option for the **Comm Exclusive** setting. Click on the drop down menu and select "No Response" as shown below. Default in V4.65 is **"No Response".**



FIELD	PURPOSE
Comm Exclusive	**Response** = reply to SIP messages **No Response**. Do not respond to messages from unauthorized IP address. **Default**

4.17 Default Data Value Changes

GENERAL DESCRIPTION

Constant request from all global markets led to the some default settings to be changed in V4.65 software for all OfficeServ 7000 series systems. The changes are:

1. The default **Dial Mode** for IP phones changed from Enblock to **Overlap** dialing for all OfficeServ systems.
2. The default **Auto Hold mode** for all Keysets (Digital & IP) changed form OFF to **ON** for OS 7030, OS 7100 and OS 7200S systems.
3. The default **SIP Trunk Connect Delay Time** changed from 100ms to **200ms** for all OfficeServ systems.
4. The default **System Hold Recall Time** changed from 45 seconds, to **120 seconds** for all OfficeServ systems.

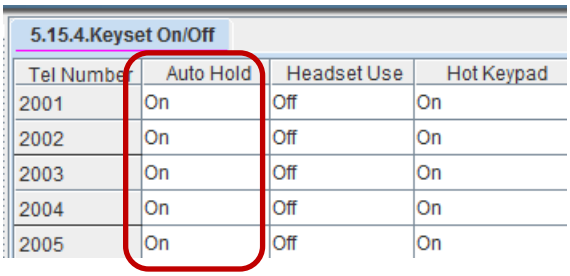
PROGRAMMING

DM menu **5.15.12 Large LCD Options** is used to assign the Dial Mode for IP phones. This menu inherited the name from previous ITP 51xx IP phone series but is used for all IP phones. **Default: Overlap**

5.15.12.Large LCD Options

Tel Number	Idle Display	DSS Key Type	Dial Mode	Screen Mode	Calendar
	Calendar	Tel Number	Overlap	Soft Menu First	Calendar
2071	Calendar	Tel Number	Overlap	Soft Menu First	Prev Screen
2072	Calendar	Tel Number	Overlap	Soft Menu First	Calendar
2073	Calendar	Tel Number	Overlap	Soft Menu First	Calendar
2074	Calendar	Tel Number	Overlap	Soft Menu First	Calendar
2075	Calendar	Tel Number	Overlap	Soft Menu First	Calendar

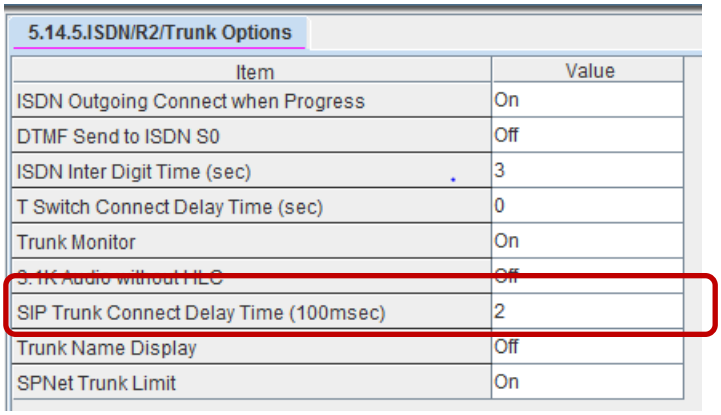
DM menu **5.15.4 Keyset ON/Off** is used to assign various telephone options as ON/Off. The Auto Hold option is one of them. With V4.65 the OS 7030, OS7100 and OS 7200S have **Auto Hold Default: On**



5.15.4.Keyset On/Off

Tel Number	Auto Hold	Headset Use	Hot Keypad
2001	On	Off	On
2002	On	Off	On
2003	On	Off	On
2004	On	Off	On
2005	On	Off	On

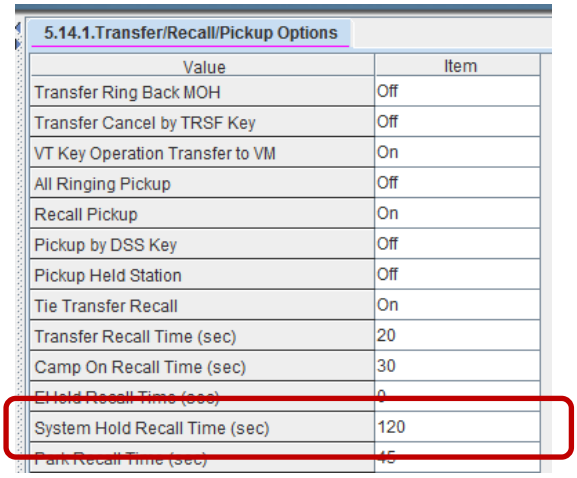
DM menu **5.14.5 ISDN/R2/Trunk Options** is used to assign the **SIP Trunk Connect Delay Time** in 100msec increments. **Default: 2** (200Msec)



5.14.5.ISDN/R2/Trunk Options

Item	Value
ISDN Outgoing Connect when Progress	On
DTMF Send to ISDN S0	Off
ISDN Inter Digit Time (sec)	3
T Switch Connect Delay Time (sec)	0
Trunk Monitor	On
3.1K Audio without HLC	Off
SIP Trunk Connect Delay Time (100msec)	2
Trunk Name Display	Off
SPNet Trunk Limit	On

DM menu **5.14.1 Transfer/Recall/Pickup Options** is used to set the **System Hold Recall Time** in seconds. **Default: 120** seconds



5.14.1.Transfer/Recall/Pickup Options

Value	Item
Transfer Ring Back MOH	Off
Transfer Cancel by TRSF Key	Off
VT Key Operation Transfer to VM	On
All Ringing Pickup	Off
Recall Pickup	On
Pickup by DSS Key	Off
Pickup Held Station	Off
Tie Transfer Recall	On
Transfer Recall Time (sec)	20
Camp On Recall Time (sec)	30
EHold Recall Time (sec)	0
System Hold Recall Time (sec)	120
Park Recall Time (sec)	45

4.18 Change Telenet ID & Password

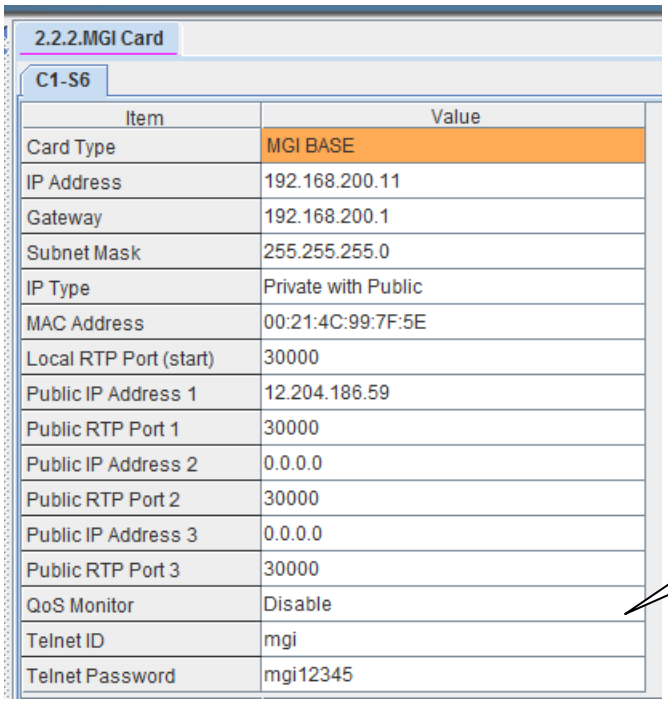
GENERAL DESCRIPTION

Prior to V4.65 the default Telenet ID and Password was fixed and could not be changed. Now it is possible to change the defaults:

	Default Data	Comments
Telenet ID	mgi	Suggest changing the default
Telenet Password	Mgi12345	Suggest changing the default

PROGRAMMING

Device Manager Menu **2.2.2 MGI Card** has two new entries to assign an ID and Password for a Telenet Session to MGI cards.



Caution: When you change either the Telenet ID or Telenet Password values then press "SAVE" **all MGI channels are restarted.**

FIELD	PURPOSE
Telenet ID	Assign ID for Telenet access 6~8 characters
Telenet Password	Assign the password for Telenet access 6 ~ 8 characters

4.19 New SMTi Series Phone Software

GENERAL DESCRIPTION

With the introduction of OfficeServ V4.65 system software, comes new software for the SMTi Series IP telephones. The tables below detail the new versions, features enhancements and bug fixes for individual models.

- The new features and some enhancement as indicated are only available when connected to an OfficeServ 7000 series system running V4.65.
- These new versions of SMT phone software will be introduced on a running change basis from Samsung's warehouse. If needed sooner these versions are available for download form GSBN

	SMT-i3105	V1.64 2013.03.07
1	Polish language added.	New feature
2	Phone ID and password increased from 4 to a range of 6~8 characters. Requires V4.65 MP	Enhancement
3	In idle state volume keys should operate Directory Search feature but instead controlled volume.	Fixed
4	When Multicast packet comes into a specific port on SMT phone it will cause the phone to reboot.	Fixed
5	SMT Phone will notify new updated DHCP IP address to the OfficeServ system.	Enhancement
6	**Some phones would not boot if "Extension Login" was enabled**	**Fixed**

	SMT-i5210	V1.41 2013.03.07
1	Polish language added	New feature
2	Phone ID and password increased from 4 to a range of 6~8 characters. Requires V4.65 MP	Enhancement
3	Upgrade lock feature	Enhancement
4	When Multicast packet comes into a specific port on SMT phone it will cause the phone to reboot.	Fixed
5	SMT Phone will notify new updated DHCP IP address to the OfficeServ system.	Enhancement
6	The default mode of Headset Key is "Use" mode	Changed
7	Noise suppression value (AEC) changed from 12 to 5 for improved voice quality on the handset.	Enhancement
8	SMDR message for calls from a SMT-i5210 overlaps the date information due to text alignment.	Fixed
9	**Some phones would not boot if "Extension Login" was enabled**	**Fixed**

	SMT-i5230	V1.30 2013.03.11
1	Polish language added	New feature
2	Phone ID and password increased from 4 to a range of 6~8 characters. Requires V4.65 MP	New feature
3	When Multicast packet comes into a specific port on SMT phone it will cause the phone to reboot.	Fixed
4	SMT Phone will notify new updated DHCP IP address to the OfficeServ system.	Enhancement
5	Upgrade lock feature	Enhancement
6	Call log history has been extended from 16 to 32	Enhancement
7	SMDR message for calls from a SMT-i5230 overlaps the date information due to text alignment.	Fixed
8	**The default mode of Headset Key is "Use" mode**	**Changed**

	SMT-i5243	V1.95 2012.12.21
1	Polish language added	New feature
2	Phone ID and password increased from 4 to a range of 6~8 characters. Requires V4.65 MP	New feature
3	The default mode of Headset Key is "Use" mode	Change
4	sRTP service on a video call has been implemented	New feature
5	**MPEG encoding option for interval of "GOP" is set to 100ms and it can be adjusted by engineering menu.**	**New feature**

	SMT-i5264 AOM	V1.26 2012.11.09
1	**Registration fails due to wrong network configuration on SMT-i5264**	**Fixed**

5. DEVICE MANAGER

OfficeServ V4.65 feature package requires new Device Manager 4.65.(DM) In Section 4 of this manual the new fields and programming steps are detailed individually as they relate to each new feature.

This section covers the most important things to know about using new Device Manager 4.65

1. Database Compatibility

- The database of V4.65 is ***not*** compatible with that of a previous version.
- You should download the database of the existing system with DM4.65 before upgrading V4.65 S/W
- After upgrading V4.65 upload the downloaded Database using DM4.65

2. Must use Java 6

- Only Java 6 guarantees normal operation of DM. So you should download Java 6 at the below URL.
  - http://www.java.com/en/download/manual_v6.jsp

3. Change Default Password

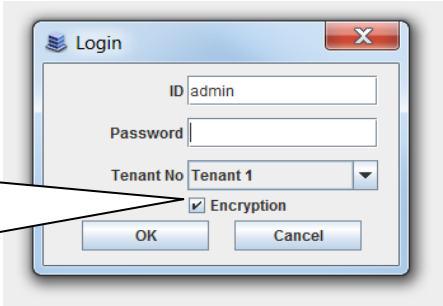
- For increased security DM requires the user to change default password when connecting to the system for the first time. This is covered in section 4.1 of this manual, DM menu 2.1.7 Admin Password for Device Manager Login

4. Encryption

- Security is the major reason for V4.65 Feature Package. Passwords related to accessing the system have been encrypted. DM 4.65 reads the encrypted passwords provided by OS V4.65 software.
- **You should use V4.65 DM when connecting V4.65 system because of encryption.**
- Encryption option is added to DM login menu. Use the check box to select encryption.

Encryption Box

- Before V4.65: Uncheck Encryption box
- V4.65: Check Encryption box



6. APPENDIX

6.1 Software Packages & Compatibility Tables

OfficeServ 7000 series new MP Software release

System	Package name	Description
OS7400 MP40	MP40_V465_20130318.zip	MP S/W for MP40 card
OS7200 MP20	MP20_ V465_20130318.zip	MP S/W for MP20 card
OS7200 MP20S	MP20S_V465_20130318.zip	MP S/W for MP20S card
OS7100 MP10a	MP10a_V465_20130318.zip	MP S/W for MP10a card
OS7030	MP03_V465_20130318.zip	MP S/W for MP03 card

V4.65 Software Compatibility Chart

The following tables list the software compatibility for OfficeServ V4.65 MP Software. Only the version in **RED** changed with the introduction of OfficeServ V4.65.

1. OfficeServ 7400/7200 S/W Version Compatibility table

System	OS7400 (MP40)	OS7200 (MP20)
MP	V4.65 '13.03.18	V4.65 '13.03.18
LP40	V2.02 '13.01.04	N/A
LCP	N/A	V4.32 '12.11.20
TEPRI2 /TEPRIa	V4.28 '10.09.07 V4.29 '11.05.03(STA only)	V4.28 '10.09.07 V4.29 '11.05.03(STA only)
4BRI	V6.03 '10.06.29	V6.03 '10.06.29
MGI16/64	V1.28 '11.12.09	V1.28 '11.12.09
SVMi-20E	V5.4.1.1 '10.12.27	V5.4.1.1 '10.12.27
SVMi-20i	V6.0.0.i '11.12.19	V6.0.0.i '11.12.19

OAS	V2.03 ’11.12.09	V2.03 ’11.12.09
DM	V4.65 ‘13.03.15	V4.65 ‘13.03.15
PWP	V4.60 ‘11.10.24	V4.60 ‘11.10.24
CNF24	V1.02 ’11.11.25	V1.02 ’11.11.25
OS Link	V3.0.0.4	V3.0.0.4
IP-UMS	V1.3.6.10 ’11.10.11	V1.3.6.10 ’11.10.11
SNMP	V1.61 ’11.09.01	V1.61 ’11.09.01-
Bootrom	V1.02 ‘09.02.27 (checksum: u11(8560), u36(0000)	V1.00 ‘08.12.16

2. OfficeServ 7030, MP03 Module version table

System	OS7030 (MP03)
System	V4.65 `13.03.18
MP	V4.65 `13.03.18
SP	V2.61 `13.01.04
VM	V2.83b `13.02.22
MGI	V2.06 `11.12.09
BRM	V4.22g `12.03.08
PRM	-
WEB	V4.12h `10.04.13
MPS	V2.01 `11.12.09
SNMP	V1.61 ’11.09.01
Boot	V4.40 `09.04.21
DM	V4.65 `13.03.15
RTG	V1.00 ’11.12.09

3. OfficeServ 7100 MP10a/ OfficeServ7200 MP20S Module version table.

System	OS7100 (MP10a)	OS7200 (MP20S)
System	V4.65 '13.03.18	V4.65 '13.03.18
MP	V4.65 '13.03.18	V4.65 '13.03.18
SP	V2.61c '13.01.04	V2.61d '13.02.07
VM	V2.83b '13.02.22	V2.83b '13.02.22
MGI	V2.06 '11.12.09	V2.06 '11.12.09
BRM	V4.22g '12.03.08	V4.22g '12.03.08
WEB	V4.12h '10.04.13	V4.12h '10.04.13
MPS	V2.01 '11.12.09	V2.01 '11.12.09
SNMP	V1.61 '11.09.01	V1.61 '11.09.01-
Router	-	-
Boot	V1.07 '09.02.24	V0.30 '09.09.22
DM	V4.65 '13.03.15	V4.65 '13.03.15
PWP	-	V4.60 '11.10.24
RTG	V1.00 '11.12.09	V1.00 '11.12.09

Data Base File

The data base file from previous software version is **not compatible** with v4.65 software. You will need to use new DM 4.65 to download the old data base file to a PC. After upgrading OfficeServ system to v4.65, use DM 4.65 to upload the data base file which was save on the PC to the OfficeServ system.

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) DM (Device Manager)

Device Manager works with system software version 4.53b or higher. When using new DM 4.65 to connect to a system **prior to OfficeServ V4.65 you must *uncheck*** the encryption box in the Login Screen. For more information, please refer to section 5 of this document.

When using new DM 4.65 to connect to a system **with OfficeServ V4.65 you must *check*** the encryption box in the Login Screen. For more information, please refer to section 5 of this document.

Remember that DM 4.65 will force the user to change default password (#PBX1357sec.com) the first time after logging in. Only the IP addresses listed in Device Manager Menu **5.13.9 DM IP White** can access Device Manager. See section 4.5 DM White List in this document.

DM has new security measure. ID and password of an 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.

a) 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 V4.65. 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 Java 6 script on your PC. Device manager V4.65 does **not** support Java 7.

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

Device Manager with version 4.65 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 OS7030, 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 tool, Web 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 operating system to perform database conversion.

2) MP20/MP40

The v4.65 software packages cannot be upgraded through DM because the main software file size is over the 20M bytes limitation. You will need to copy v4.65 software to the SD card

3) OS 7030/MP10a/MP20s

For these systems, you can either use DM or SD card to upgrade the system software.

When upgrading system software to v4.65, the embedded voice mail (VM) data base remains 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 v4.6x
   (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 v4.65
   (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.

4) LP 40

- MP40 should be upgraded to V4.65 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.

6.2 Software Upgrade Procedures

1. The OS7400 Upgrade Procedures

Any upgrade to V4.65 will default the database, so doing a backup with DM (Device Manager) V4.65 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 as 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 V4.65 will default the database, so do a backup with Device Manager V4.65 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) Insert the SD Card back into the switch and power cycle the switch.
5) 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.
6) Access MMC 818 and upgrade the LCP Card if this is a two cabinet OS7200 system.
7) Upgrade any MGI-16 and OAS card to be able to use any new features and hardware.
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 815 to the SD card.

10) Upgrade all SMT-I phones.
11) Upgrade Completed.

3. The OS7200S MP20S Upgrade Procedure

Any upgrade to V4.65 will default the database, so doing a backup with Device Manager V4.65 is a must. Start with downloading the DM 4.65 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 V4.65 will default the database, so doing a backup with Device Manager V4.65 is a must. Start with downloading the DM 4.65 program and using it to download the database.

1) Download the database to the PC using the DM 4.65 program.
2) Login with DM and access the FILE CONTROL section.
3) Select the folder with the unzipped version of 4.65 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 V4.65 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 V4.65 will default the database, so doing a backup with Device Manager V4.65 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 DM 4.65 program.
2) Login with DM and access the FILE CONTROL section.
3) Select the folder with the unzipped version of 4.65 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 V4.65 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 and MGI-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) Make sure Telenet IP address is defined in DM menu 5.13.11. See section 4.1 of this manual regarding Management IP White List.
4) Access the START, RUN, CMD to access a telnet session from PC.
5) Type (TELNET XXX.XXX.XXX.XXX) to access the MGI card for programming. XX is the IP address of the MGI.
6) The IP address will be the one in MMC 831 for that card.
7) Login onto the card with user name of mgi and password of mgi12345.
8) Type in (ALLSET)
9) The system will respond with current IP Address which should be the MGI card IP address.

a. Change this address if it needed.

10) The next prompt will be the SUBNET MASK which is 255.255.255.000
11) The next prompt will be the GATWAY. Put in your gateway.
12) The next prompt will be the I/O Server which is the **PC IP address**.
13) When the system responds, 20 seconds later, type in (REBOOT) to reboot the card.
14) 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.
15) After a few minutes, access DM 2.2.0 (MMC 727) and verify the software load and date is correct.
16) 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) Make sure Telenet IP address is defined in DM menu 5.13.11. See section 4.1 of this manual regarding Management IP White List.
4) Access the START, RUN, CMD to access a telnet session from PC.
5) Type (TELNET XXX.XXX.XXX.XXX) to access the OAS card for programming. XX is the IP address of OAS card.
6) The IP address will be the one in DM 2.2.2 (MMC 831) for that card.
7) Login onto the card with user name of mgi and password of mgi12345.
8) Type in (ALLSET)
9) The system will respond with current IP Address which is the MGI card IP address. Change this address if it needed.
10) The next prompt will be the SUBNET MASK which is 255.255.255.000
11) The next prompt will be the GATWAY which is 105.52.21.1. Put in your gateway.
12) The next prompt will be the I/O Server which is the PC IP address.
13) When the system responds, 20 seconds later, type in (REBOOT) to reboot the card.
14) 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.
15) After a few minutes, access MMC 727 and verify the software load and date is correct.
16) Upgrade Complete.

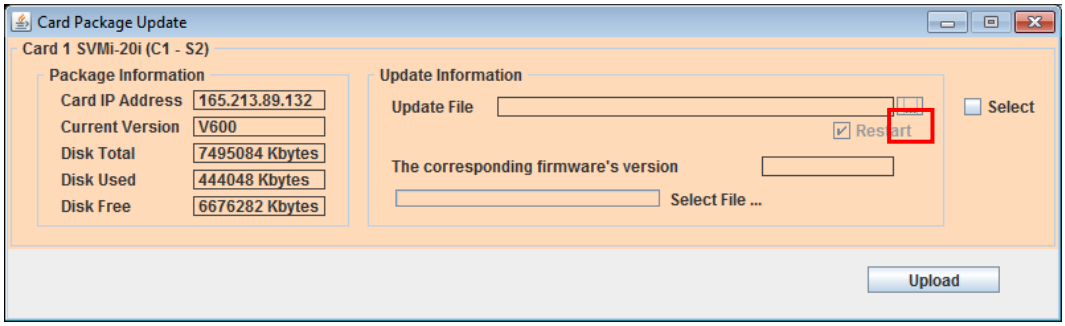
8. CNF-24 Upgrade Procedure

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.

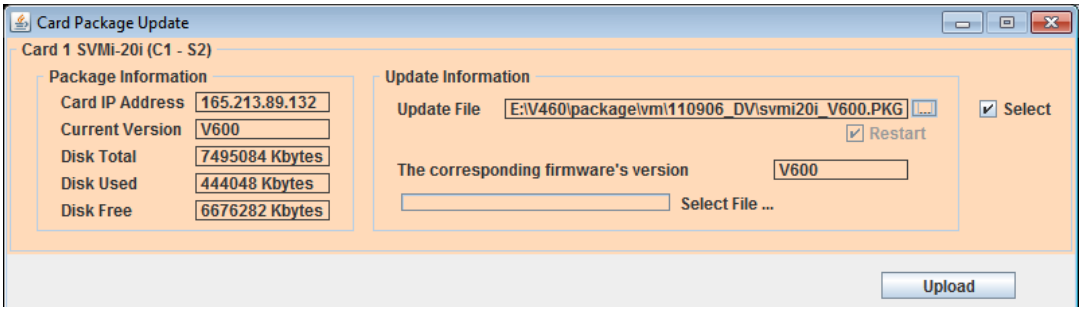
9. SVMi-20i Upgrade Procedure

1) The SVMi-20i software package does not need to be unzipped.
2) Login onto the switch using the latest DM program. System IP needs to be set first in MMC 830.
3) Set an IP address and gateway for the SVMi-20i in DM 2.2.17 or MMC 873
4) The PC needs to be in the same subnet as the system

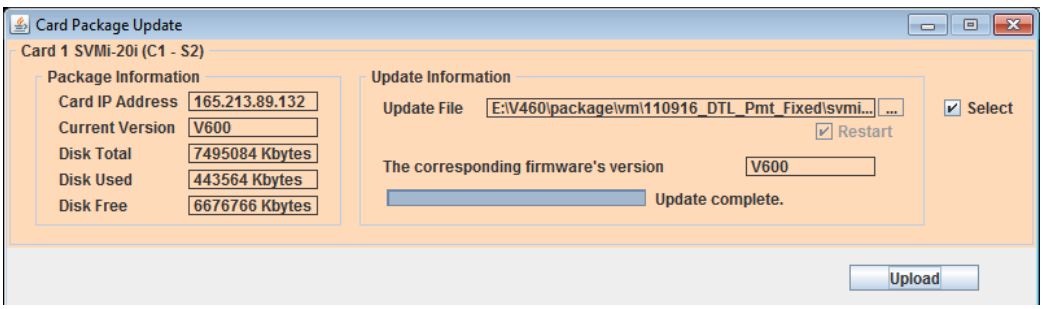
5) Select Package Update.
   In order to upgrade the SVMi-20i's firmware, select 'Package Update' in Util tab of the Device Manager. Then, the following window will pop up.



6) Select the file to update.
   Click **[...]** and select the file to update. If the file is selected, 'firmware's version' will be displayed in File Information.



7) Upload the package.
   Click **[Upload]** button to start to upload the file. To apply the uploaded file, the SVMi-20i card will be restarted automatically.



8) Upgrade Completed.

10. 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.

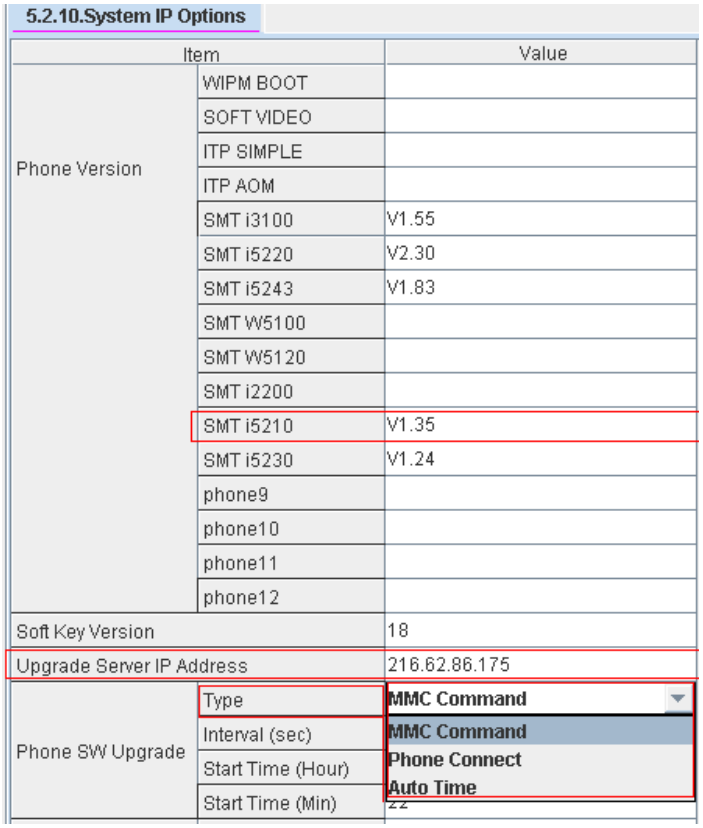
11. SMT-I Phone Upgrade Procedure

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.


5.2.10.System IP Options
Item
Value
Phone Version
WIPM BOOT
SOFT VIDEO
ITP SIMPLE
ITP AOM
SMT i3100
V1.55
SMT i5220
V2.30
SMT i5243
V1.83
SMT W5100
SMT W5120
SMT i2200
SMT i5210
V1.35
SMT i5230
V1.24
phone9
phone10
phone11
phone12
Soft Key Version
18
Upgrade Server IP Address
216.62.86.175
Phone SW Upgrade
Type
MMC Command
Interval (sec)
Start Time (Hour)
Start Time (Min)
MMC Command
Phone Connect
Auto Time

6.3 Product Bulletins

Product Bulletin 249_Software_v4.65-Release: Software Version 4.65 Availability.