# SCM

# **Quick Installation Guide**





#### COPYRIGHT

This manual is proprietary to SAMSUNG Electronics Co., Ltd. and is protected by copyright. No information contained herein may be copied, translated, transcribed or duplicated for any commercial purposes or disclosed to the third party in any form without the prior written consent of SAMSUNG Electronics Co., Ltd.

#### TRADEMARKS

Product names mentioned in this manual may be trademarks and/or registered trademarks of their respective companies.

This manual should be read and used as a guideline for properly installing and operating the product.

All reasonable care has been made to ensure that this document is accurate. If you have any comments on this manual, please contact our documentation centre at the following homepage:

Homepage: http://www.samsungdocs.com

©2013 SAMSUNG Electronics Co., Ltd. All rights reserved.

# INTRODUCTION

### Purpose

This manual describes the quick reference for the system installation.

# **Document Content and Organization**

This manual consists of the following Chapters.

#### **Quick Installation Guide**

Describes the quick guide for each case during the system installation.

#### ABBREVIATION

Describes the acronyms used in this manual.

### Conventions

The following types of paragraphs contain special information that must be carefully read and thoroughly understood. Such information may or may not be enclosed in a rectangular box, separating it from the main text, but is always preceded by an icon and/or a bold title.



#### WARNING

Provides information or instructions that the reader should follow in order to avoid personal injury or fatality.



#### CAUTION

Provides information or instructions that the reader should follow in order to avoid a service failure or damage to the system.



CHECKPOINT

Provides the operator with checkpoints for stable system operation.



NOTE

Indicates additional information as a reference.

# **Console Screen Output**

- The lined box with 'Courier New' font will be used to distinguish between the main content and console output screen text.
- **'Bold Courier New'** font will indicate the value entered by the operator on the console screen.

# **Revision History**

VERSION	DATE OF ISSUE	REMARKS
1.0	10. 2013.	First Version

# SAFETY CONCERNS

The purpose of the Safety Concerns section is to ensure the safety of users and prevent property damage. Please read this document carefully for proper use.

# Symbols



Indication of a general caution



Restriction Indication for prohibiting an action for a product



Instruction

Caution

Indication for commanding a specifically required action

# TABLE OF CONTENTS

INTRO	DUCT	ION	3
	Purp	pose	3
	Docu	ument Content and Organization	3
	Conv	ventions	3
	Cons	sole Screen Output	4
	Revis	sion History	4
SAFE	гү со	NCERNS	5
	Syml	bols	5
Quick	Instal	lation Guide	9
1	Inter	rworking local site desktop phone	9
	1.1	Single Phone User (Server Mode)	9
	1.2	Single Phone User (PNP Mode)	10
	1.3	Multi-Extension Phone (Server Mode)	12
	1.4	Multi-Extension Phone (PNP Mode)	14
2	Inter	rworking local site 3 <sup>rd</sup> party SIP phone	16
3	Inter	rworking home worker desktop phone	18
	3.1	Case of using SBC	18
	3.2	Case without SBC	19
4	Inter	rworking remote site desktop phone	21
	4.1	Same Network Configuration	21
	4.2	Different Network Configuration	21
5	Inter	rworking remote site 3 <sup>rd</sup> party SIP phone	22
	5.1	Same Network Configuration	22
	5.2	Different Network Configuration	22
6	Inter	rworking local gateway	24
	6.1	SCM	24
	6.2	OfficeServ7400	26
	6.3	iBG	
7	Inter	rworking remote site gateway	32

	7.1	SCM	32
	7.2	OfficeServ7400	35
	7.3	iBG	35
8	Interv	vorking FXS	36
	8.1	SCM	
	8.2	OfficeServ7400	37
	8.3	iBG	
9	Interv	working PRI	40
	9.1	SCM	40
	9.2	OfficeServ7400	41
	9.3	iBG	41
10	Interv	vorking FXO	42
	10.1	SCM	42
	10.2	OfficeServ7400	43
	10.3	iBG	44
11	Interv	working SIP trunk	45
	11.1	Making Routes	45
	11.2	Making LCR	48
	11.3	Making Location Based Routing	49
	11.4	Configuring Access Codes	50
	11.5	Configuring DID Routing	51
12	Interv	working SBC	52
	12.1	Media-pool	52
	12.2	Region	53
	12.3	Policy	54
	12.4	Security	56
	12.5	Activating SBC	57
13	NAT/I	Firewall configuration	58
14	Interv	working WE VoIP	60
15	mVol	P	62
16	TLS a	and sRTP configuration	64
	16.1	SCM	64
	16.2	OfficeServ7400	66
	16.3	iBG	67
17	Interv	working mail server	69
18	Confi	iguration of CDRs	72
	18.1	Configuration of Storage option	72

20	Interworking application (SIP, CSTA)	
ABBRE	VIATION	84

#### LIST OF FIGURES

Figure 1. Making Routes	45
Figure 2. Modifying Routes	46

# **Quick Installation Guide**

# 1 Interworking local site desktop phone

Depending on the type of phone can be divided into 'Single Phone User' and 'Multi-Extension Phone'. Depending on the type of interworking can be divided into 'Server Mode' and 'PNP Mode'.

# 1.1 Single Phone User (Server Mode)

#### **License Checking**

Check a license count about Samsung SIP Phones. [CONFIGURATION > Miscellaneous > License]

😹 [DIALOG]License - Detail			
License Key Type	SCM Express - Users 💌	License Key	6RNMFHUB-Z4FC2Y80-GYXQBM9M-USECHYMQ
MAC Address	000C29A9CF9A	License Status	OK 💌
Samsung SIP Phones	100	Samsung Soft Phones	100
Samsung Mobile Phones	100	Samsung PC Attendants	100
3rd Party SIP Phones	100	Analog Phones(Gateway)	100
AA Availability(Master/Slave)	No	High Availability(Active/Standby)	No
Meet-Me Conference Channels		UMS Channels	
Total CSTA Applications		Samsung Operators	
Embeded ACD Agent Links		Communicators(Desktop)	
Other CSTA Applications		SIP Application Channels	
FMS Phones		mVoIP Phones	

#### **Single Phone User Configuration**

Configure the information about Single Phone User. [CONFIGURATION > User > Single Phone User]

😻 [DIALOG] Single Phone User - Create			
User Group	UG1	Service Group	UG1-SG1
Location	UG1-LOC1	Extension Number	6001
Application User ID	6001@ug1,scm,com	Extension Name	6001
Application Password	samsung	PIN Number	0000
Authentication User ID	6001	Phone Verification	None
Authentication Password	0000	MAC Address	
IP Address	165,213,80,252	Private IP Address	165,213,80,252
Profile Login ID	UG16001	Phone Type	Samsung-Desktop-Phone
Profile Login Passcode	0000	Language	Korean
Mobile Phone Number		Use Mobile Phone Number	None
Protocol	UDP 🔽	Media	RTP
TLS Connection	Reuse	Ping Ring Type	None
A-A Primary Node	NODE 0	A-A Dual Registration	Enable
VMS Extension Number		Make Mailbox	Yes
	Create	Close	

- 1) Select the 'Phone Type' to 'Samsung-Desktop-Phone'.
- 2) 'Extension Number', 'Application User ID' and 'Profile Login ID' are not duplicated with the other user's configuration.
- 3) In Active-Active System case, 'A-A Primary Node' must be set.

#### **Phone Configuration**

Select a 'Configure type' to 'Server' in Easy Install menu of phone.

Enter 'Profile Login ID' in Single Phone User menu into 'Login ID' in Easy Install menu of phone.

Enter 'Profile Login Passcode' in Single Phone User menu into 'Password' in Easy Install menu of phone.

Enter 'SCM IP Address' into 'Config Server' in Easy Install menu of phone.

#### **Registration Checking**

You can check a registration status of phone in next menu. [CONFIGURATION > Registration Status > Registration Status]

# **1.2 Single Phone User (PNP Mode)**

#### **License Checking**

Check a license count about Samsung SIP Phone. [CONFIGURATION > Miscellaneous > License]

IDIALOG] Single Phone User - Create					٢.	
User Group	UG1	-	Service Group	UG1-SG1	-	
Location	UG1-LOC1	-	Extension Number	6001		
Application User ID	6001@ug1.scm.com		Extension Name	6001		
Application Password	samsung		PIN Number	0000		
Authentication User ID	6001		Phone Verification	None	-	
Authentication Password	0000		MAC Address			
IP Address	165,213,80,252		Private IP Address	165,213,80,252		
Profile Login ID	UG16001		Phone Type	Samsung-Desktop-Phone	-	
Profile Login Passcode	0000		Language	Korean	-	
Mobile Phone Number			Use Mobile Phone Number	None	-	
Protocol	UDP [	-	Media	RTP	-	
TLS Connection	Reuse [	-	Ping Ring Type	None	•	
A-A Primary Node	NODE 0	•	A-A Dual Registration	Enable	•	
VMS Extension Number			Make Mailbo×	Yes	•	
Create Apply Close						

#### **Single Phone User Configuration**

Configure the information about Single Phone User. [CONFIGURATION > User > Single Phone User]

😻 [DIALOG] Single Phone User - Create					×
User Group	UG1	-	Service Group	UG1-SG1	-
Location	UG1-LOC1	-	Extension Number	6001	
Application User ID	6001@ug1,scm,com		Extension Name	6001	
Application Password	samsung		PIN Number	0000	
Authentication User ID	6001		Phone Verification	MACAddress	-
Authentication Password	0000		MAC Address	11:22:33:44:55:66	
IP Address	165,213,80,252		Private IP Address	165,213,80,252	
Profile Login ID	UG16001		Phone Type	Samsung-Desktop-Phone	-
Profile Login Passcode	0000		Language	English	-
Mobile Phone Number			Use Mobile Phone Number	None	-
Protocol	UDP	-	Media	RTP	-
TLS Connection	Reuse	-	Ping Ring Type	None	-
A-A Primary Node	NODE 0	-	A-A Dual Registration	Enable	-
VMS Extension Number			Make Mailbox	Yes	-
	Create	Ар	ply Close		

- 1) Select the 'Phone Type' to 'Samsung-Desktop-Phone'.
- 2) 'Extension Number', 'Application User ID' and 'Profile Login ID' are not duplicated with the other user's configuration.
- 3) In Active-Active System case, 'A-A Primary Node' must be set.
- 4) Select the 'Phone Verification' to 'MACAddress' and enter the MAC address of phone into 'MAC Address'.

#### **DHCP Server Configuration**

Add the next item to DHCP Server. (Use a SCM IP Address instead of 1.1.1.1)

DHCP Option 43: [A] code: 43 type: string data: sec,tftp://1.1.1.1

#### **Phone Configuration**

Select a 'Configure type' to 'PnP' in Easy Install menu of phone.

#### **Registration Checking**

You can check a registration status of phone in next menu. [CONFIGURATION > Registration Status > Registration Status]

## **1.3 Multi-Extension Phone (Server Mode)**

#### **License Checking**

Check a license count about Samsung SIP Phones. [CONFIGURATION > Miscellaneous > License]

😹 [DIALOG]License - Detail			
License Key Type	SCM Express - Users	License Key	6RNMFHUB-Z4FC2Y80-GYXQBM9M-USECHYMQ
MAC Address	000C29A9CF9A	License Status	ОК
Samsung SIP Phones	100	Samsung Soft Phones	100
Samsung Mobile Phones	100	Samsung PC Attendants	100
3rd Party SIP Phones	100	Analog Phones(Gateway)	100
AA Availability(Master/Slave)	No	High Availability(Active/Standby)	No
Meet-Me Conference Channels		UMS Channels	
Total CSTA Applications		Samsung Operators	
Embeded ACD Agent Links		Communicators(Desktop)	
Other CSTA Applications		SIP Application Channels	
FMS Phones		mVoIP Phones	

#### **Multi-Extension Phone Configuration**

Configure the information about Multi-Extension Phone. [CONFIGURATION > User > Multi-Extension Phone]

Phone Verification IP Address		<b>T</b>	Phone Name	8001a	
IP Address	Nope		MAC Address		
IP AUGIESS	None		MAC Address		
Des file de sele 10			Private IP Address	N1	
Profile Login ID	0000		User Type	Normal	
Profile Login Passcode			Phone Type	Samsung-Desktop-Phone	
Language	English		UHIType	ISIP	
Protocol			DTMF	RFC2833	
Media	RTP		RFC2833 DTMF Payload	101	
Time Zone	Same as System		Accept Login Override	Disable	
Display Option	Normal	-	Send CLI Number		
Off Hook Alarm	Disable	-	Check Registration Protocol	Disable	
TLS Connection	Reuse		MOH SIP Media Mode	Send/Receive	
Phone TX Gain			TLS Key Decryption Password Type	Direct	
'LS Key Decryption Direct Password			TLS Key Decryption Device ID		
TLS Key Decryption Salt			TLS Key Decryption IC	512	
TLS Key Decryption DK	20		NFC Mobile Phone Name		
Line Skipping	None	-	Phone Call History	On	
Primary Extension Number		-	Next Extension Number Selection	Disable	
NFC Auto Login	Disable	-	NFC Auto Login Phone Name		
Use InterProxy	Disable	-	PROXYB Index		
Input Number Display	Display	-	Use mVoIP		
Resume after Transfer-Cancel	No	•	Teinet Access	Disable	
WIFi Access	Enable	•	SIP-PRACK option	Disable	
	No	-	Send RTCP on Hold	No	

- 1) Select the 'Phone Type' to 'Samsung-Desktop-Phone'.
- 2) 'Phone Name' and 'Profile Login ID' are not duplicated with the other user's configuration.
- Depending on the way using phone can be set 'User Type', 'Phone Verification'. (Refer to Operation Manual)

#### **Multi-Phone User Configuration**

Configure the information about Multi- Phone User. [CONFIGURATION > User > Multi-Phone User]

😻 [DIALOG] Multi-Phone User - Create					
User Group	UG1	•	Service Group	UG1-SG1	▼ ▲
Location	UG1-LOC1	•	Extension Number	8001	
Application User ID	8001@ug1,scm,com		Name	M8001	
PIN Number	0000		Mobile Phone Number		
Use Mobile Phone Number		<b>_</b>	Department		-
Position		-	Send CLI Number		
Send CLI Name			Service Group Local Number		
Service Group Local CLI Number	Extension Number	•	Multi Type	Multi Line	-
Call Appearance		-	Extension Lock	None	-
Class of Service		•	Restriction Policy		-
Gateway Name		•	Authentication User ID	8001	
Authentication Password	0000		MOH Announcement ID		-
Account Code Use	None	•	LDAP DN Number		
Auto Answer by Click to Dial	Enable	•	External Ringback Tone Use	None	-
Call Monitoring	Disable	•	Send Extension Number		
Use Virtual Ringback	Disable	•	Multi-Device Conference Join	Disable	-
Caller Ring Type		•	Application Server Service Group		-
Ping Ring Type		•	CMS Monitoring		-
A-A Primary Node		•	A-A Dual Registration		-
VMS Extension Number			Call Recording Method		-
Allow Selective Call		•	Phone Display Name	Extension Number	-
Error Announcement		•	Desk Phone Simultaneous Ring Delay	Disable	-
CLI for Forwarded Call		•	Mobile Number Auto Update	Yes	-
Make Mailbox	Yes	•			
Phone					
[Selected]					
ouura					
		Create Ap	ply Close		

- 1) 'Extension Number' and 'Application User ID' are not duplicated with the other user's configuration.
- 2) Select the phone name to 'Phone' menu among 'Multi-Extension Phone' configured above.
- 3) In Active-Active System case, 'A-A Primary Node' must be set.

#### **Phone Configuration**

Select a 'Configure type' to 'Server' in Easy Install menu of phone.

Enter 'Profile Login ID' in Single Phone User menu into 'Login ID' in Easy Install menu of phone.

Enter 'Profile Login Passcode' in Single Phone User menu into 'Password' in Easy Install menu of phone.

Enter 'SCM IP Address' into 'Config Server' in Easy Install menu of phone.

#### **Registration Checking**

You can check a registration status of phone in next menu. [CONFIGURATION > Registration Status > Registration Status]

## **1.4 Multi-Extension Phone (PNP Mode)**

#### **License Checking**

Check a license count about Samsung SIP Phones. [CONFIGURATION > Miscellaneous > License]

😻 [DIALOG]License - Detail					
License Key Type	SCM Express - Users	License Key	6RNMFHUB-Z4FC2Y80-GYXQBM9M-USECHYMQ		
MAC Address	000C29A9CF9A	License Status	ОК		
Samsung SIP Phones	100	Samsung Soft Phones	100		
Samsung Mobile Phones	100	Samsung PC Attendants	100		
3rd Party SIP Phones	100	Analog Phones(Gateway)	100		
AA Availability(Master/Slave)	No	High Availability(Active/Standby)	No		
Meet-Me Conference Channels		UMS Channels			
Total CSTA Applications		Samsung Operators			
Embeded ACD Agent Links		Communicators(Desktop)			
Other CSTA Applications		SIP Application Channels			
FMS Phones		mVoIP Phones			

#### **Multi-Extension Phone Configuration**

Configure the information about Multi-Extension Phone. [CONFIGURATION > User > Multi-Extension Phone]

Phone Verification IP Address		-	Phone Name	8001a
IP Address	MACAddress		MAC Address	11:22:33:44:55:66
			Private IP Address	
Profile Login ID	8001a		User Type	Please input 0~9 or a~f, :
Profile Login Passcode	0000		Phone Type	Samsung-Desktop-Phone
Language	English	-	URI Type	SIP
Protocol	UDP	•	DTMF	RFC2833
Media	RTP	•	RFC2833 DTMF Payload	101
Time Zone	GMT +09:00 Asia/Seoul	-	Accept Login Override	Disable
Display Option	Normal	-	Send CLI Number	
Off Hook Alarm	Disable	-	Check Registration Protocol	Disable
TLS Connection	Reuse	-	MOH SIP Media Mode	Send/Receive
Phone TX Gain			TLS Key Decryption Password Type	Direct
LS Key Decryption Direct Password			TLS Key Decryption Device ID	
TLS Key Decryption Salt			TLS Key Decryption IC	512
TLS Key Decryption DK	20		NFC Mobile Phone Name	
Line Skipping	None	-	Phone Call History	On
Primary Extension Number		-	Next Extension Number Selection	Disable
NFC Auto Login	Disable	-	NFC Auto Login Phone Name	
Use InterProxy	Disable	-	PROXYB Index	1
Input Number Display	Display	-	Use mVoIP	No
Resume after Transfer-Cancel	No	-	Telnet Access	Disable
WIFI Access	Enable	-	SIP-PRACK option	Disable
	No	-	Send RTCP on Hold	No

- 1) Select the 'Phone Type' to 'Samsung-Desktop-Phone'.
- 2) 'Phone Name' and 'Profile Login ID' are not duplicated with the other user's configuration.
- 3) Select the 'Phone Verification' to 'MACAddress' and enter the MAC address of phone into 'MAC Address'.
- Depending on the way using phone can be set 'User Type', 'Phone Verification'. (Refer to Operation Manual)

#### **Multi-Phone User Configuration**

Configure the information about Multi- Phone User. [CONFIGURATION > User > Multi-Phone User]

😻 [DIALOG] Multi-Phone User - Create					
User Group	UG1		Service Group	UG1-SG1	<ul> <li>▼</li> </ul>
Location	UG1-LOC1		Extension Number	8001	
Application User ID	8001@ug1,scm,com		Name	M8001	
PIN Number	0000		Mobile Phone Number		
Use Mobile Phone Number			Department		-
Position			Send CLI Number		
Send CLI Name			Service Group Local Number		
Service Group Local CLI Number	Extension Number	-	Multi Type	Multi Line	-
Call Appearance		-	Extension Lock	None	-
Class of Service		-	Restriction Policy		-
Gateway Name		-	Authentication User ID	8001	
Authentication Password	0000		MOH Announcement ID		-
Account Code Use	None	-	LDAP DN Number		
Auto Answer by Click to Dial	Enable	-	External Ringback Tone Use	None	-
Call Monitoring	Disable	-	Send Extension Number		
Use Virtual Ringback	Disable	-	Multi-Device Conference Join	Disable	-
Caller Ring Type		-	Application Server Service Group		-
Ping Ring Type		-	CMS Monitoring		-
A-A Primary Node		-	A-A Dual Registration		-
VMS Extension Number			Call Recording Method		-
Allow Selective Call		-	Phone Display Name	Extension Number	-
Error Announcement		-	Desk Phone Simultaneous Ring Delay	Disable	-
CLI for Forwarded Call		-	Mobile Number Auto Update	Yes	<b>_</b>
Make Mailbo×	Yes	-			
Phone					
[Selected]					
0001a					
		Create Ap	ply Close		

- 1) 'Extension Number' and 'Application User ID' are not duplicated with the other user's configuration.
- 2) Select the phone name to 'Phone' menu among 'Multi-Extension Phone' configured above.
- 3) In Active-Active System case, 'A-A Primary Node' must be set.

#### **DHCP Server Configuration**

Add the next item to DHCP Server. (Use a SCM IP Address instead of 1.1.1.1)

DHCP Option 43: [A] code: 43 type: string data: sec,tftp://1.1.1.1

#### **Phone Configuration**

Select a 'Configure type' to 'PnP' in Easy Install menu of phone.

#### **Registration Checking**

You can check a registration status of phone in next menu. [CONFIGURATION > Registration Status > Registration Status]

# 2 Interworking local site 3<sup>rd</sup> party SIP phone

3rd-party SIP Phone can be used only Sing Phone User type.

#### **License Checking**

Check a license count about 3rd Party SIP Phones. [CONFIGURATION > Miscellaneous > License]

😹 [DIALOG]License - Detail				
License Key Type	SCM Express - Users	-	License Key	6RNMFHUB-Z4FC2Y80-GYXQBM9M-USECHYMQ
MAC Address	000C29A9CF9A		License Status	ОК
Samsung SIP Phones	100		Samsung Soft Phones	100
Samsung Mobile Phones	100		Samsung PC Attendants	100
3rd Party SIP Phones	100		Analog Phones(Gateway)	100
AA Availability(Master/Slave)	No	-	High Availability(Active/Standby)	No
Meet-Me Conference Channels			UMS Channels	
Total CSTA Applications			Samsung Operators	
Embeded ACD Agent Links			Communicators(Desktop)	
Other CSTA Applications			SIP Application Channels	
FMS Phones			mVoIP Phones	

#### **Single Phone User Configuration**

Configure the information about Single Phone User. [CONFIGURATION > User > Single Phone User]

😹 [DIALOG] Single Phone User - Create				
User Group	UG1	Service Group	UG1-SG1	
Location	UG1-LOC1	Extension Number	6001	
Application User ID	6001@ug1,scm,com	Extension Name	6001	
Application Password	samsung	PIN Number	0000	
Authentication User ID	6001	Phone Verification	None	
Authentication Password	0000	MAC Address		
IP Address	165,213,80,252	Private IP Address	165,213,80,252	
Profile Login ID	UG16001	Phone Type	3rd-Party-SIP-Phone	
Profile Login Passcode	0000	Language	English	
Mobile Phone Number		Use Mobile Phone Number	None	
Protocol	UDP	Media.	RTP	
TLS Connection	Reuse	Ping Ring Type	None	
A-A Primary Node	NODE 0	A-A Dual Registration	Enable	
VMS Extension Number		Make Mailbox	Yes 💌	
Create Apply Close				

- 1) Select the 'Phone Type' to '3rd-Party-SIP-Phone'.
- 2) 'Extension Number', 'Application User ID' and 'Profile Login ID' are not duplicated with the other user's configuration.
- 3) Enter the 'Authentication User ID' and 'Authentication Password'.
- 4) In Active-Active System case, 'A-A Primary Node' must be set.

#### **Phone Configuration**

Enter 'SCM IP Address', 'Authentication User ID' and 'Authentication Password' in 3rd Party SIP Phone.

### **Registration Checking**

You can check a registration status of phone in next menu. [CONFIGURATION > Registration Status > Registration Status]

# 3 Interworking home worker desktop phone

Interworking home worker desktop phone is same with interworking local desktop phone basically.

Refer to interworking local desktop phone about basic setting. Additional setting is as follows.

# 3.1 Case of using SBC

#### **SBC Configuration**

Check a license count about Samsung SIP Phones. Next port must be forwarded to SCM in SBC.

- To SIP signaling: UDP (5060), TCP (5060), TCP (5061)
- To RTP packet: RTP port range (40000~40799)

Please refer to '1.12 Interworking SBC' page to detail setting.

#### **Firewall Configuration**

Public IP must be needed to access to SCM from home. Next port must be forwarded to SCM in Firewall for using Public IP.

- To upgrade package of phone: UDP (6000)
- HTTP: TCP (80)
- HTTPS: TCP (443)
- TFTP Server: UDP (69), TCP (69)

Please refer to '1.13 NAT/Firewall configuration' page to detail setting.

#### **Phone Configuration**

Enter 'Public IP Address' of firewall into 'Config Server' in Easy Install menu of phone.

#### **SCM Configuration**

Next configuration is needed in next menu. [CONFIGURATION > Miscellaneous > System Options]

System Options		
Node Name NODE 0	lear Reset	
Name	Value	Node Name
System Public HTTPS Port For Phone Provision	443	NODE 0
System Public IP Address For Admin	none	NODE 0
System Public IP Address For Call	none	NODE 0
System Public IP Address For Phone Provision	none	NODE 0
System SPAM Call Expire Timer (second)	10	NODE 0
System Under NAT	DISABLE	NODE 0
<b>∢ ∢</b> 2/2(132) <b>▶ ▶</b>	Detail Change Excel Att	ach Close

- 1) Enter the Public IP of SBC into 'System Public IP Address For Call'.
- 2) Enter the Public IP of firewall into 'System Public IP For Phone Provision'.

## 3.2 Case without SBC

#### **Firewall Configuration**

Public IP must be needed to access to SCM from home. Next port must be forwarded to SCM in Firewall for using Public IP.

- To SIP signaling: UDP (5060), TCP (5060), TCP (5061)
- To RTP packet: RTP port range (40000~40799)
- To upgrade package of phone: UDP(6000)
- HTTP: TCP (80)
- HTTPS: TCP (443)
- TFTP Server: UDP (69), TCP (69)

Please refer to '1.13 NAT/Firewall configuration' page to detail setting.

#### **Phone Configuration**

Enter 'Public IP Address' of firewall into 'Config Server' in Easy Install menu of phone.

#### **SCM** Configuration

Next configuration is needed in next menu. [CONFIGURATION > Miscellaneous > System Options]

System Options		
Node Name NODE 0	lear Reset	
Name	Value	Node Name
System Public HTTPS Port For Phone Provision	443	NODE 0
System Public IP Address For Admin	none	NODE 0
System Public IP Address For Call	none	NODE 0
System Public IP Address For Phone Provision	none	NODE 0
System SPAM Call Expire Timer (second)	10	NODE 0
System Under NAT	DISABLE	NODE 0
	1	
<b>∢ ∢</b> 2/2(132) <b>▶ )</b>	Detail Change Excel Att	ach Close

- 1) Enter the Public IP of firewall into 'System Public IP Address For Call'.
- 2) Enter the Public IP of firewall into 'System Public IP For Phone Provision'.

# 4 Interworking remote site desktop phone

Interworking remote site desktop phone is divided as follow depend on network configuration.

# 4.1 Same Network Configuration

It is same with interworking local desktop phone basically. Please refer to '1 Interworking local site desktop phone' page.

# 4.2 Different Network Configuration

It is same with interworking home worker desktop phone basically. Please refer to '3 Interworking home worker desktop phone' page.

# 5 Interworking remote site 3<sup>rd</sup> party SIP phone

Interworking remote site 3<sup>rd</sup> party SIP phone is divided as follow depend on network configuration.

# 5.1 Same Network Configuration

It is same with interworking local sire 3<sup>rd</sup> party SIP phone. Please refer to '2 Interworking local site 3<sup>rd</sup> party SIP phone' page.

## 5.2 Different Network Configuration

It is same with interworking local sire 3<sup>rd</sup> party SIP phone basically. Please refer to '2 Interworking local site 3<sup>rd</sup> party SIP phone' page about basic setting. Additional setting is as follows.

### 5.2.1 Case of using SBC

#### **SBC Configuration**

Check a license count about Samsung SIP Phones. Next port must be forwarded to SCM in SBC.

- To SIP signaling: SIP signaling port of 3<sup>rd</sup> Party Phone
- To RTP packet: RTP port range of 3<sup>rd</sup> Party Phone

Please refer to '12 Interworking SBC' page to detail setting.

#### **Phone Configuration**

Enter 'Public IP Address' of SBC into 'Server IP' in 3<sup>rd</sup> party phone.

#### **SCM Configuration**

Next configuration is needed in next menu. [CONFIGURATION > Miscellaneous > System Options]

😻 System Options		
Node Name NODE 0	lear Reset	
Name	Value	Node Name
System Public HTTPS Port For Phone Provision	443	NODE 0
System Public IP Address For Admin	none	NODE 0
System Public IP Address For Call	none	NODE 0
System Public IP Address For Phone Provision	none	NODE 0
System SPAM Call Expire Timer (second)	10	NODE 0
System Under NAT	DISABLE	NODE 0
	1	
<b>4 4</b> 2/2 (132) <b>▶ ▶</b>	Detail Change Excel Att	ach Close

Enter the Public IP of SBC into 'System Public IP Address For Call'.

#### 5.2.2 Case without SBC

#### **Firewall Configuration**

Public IP must be needed to access to SCM from home. Next port must be forwarded to SCM in Firewall for using Public IP.

- To SIP signaling: SIP signaling port of 3<sup>rd</sup> Party Phone
- To RTP packet: RTP port range of 3<sup>rd</sup> Party Phone

Please refer to '13 NAT/Firewall configuration' page to detail setting.

#### **Phone Configuration**

Enter 'Public IP Address' of firewall into 'Server IP' in 3<sup>rd</sup> party phone.

#### **SCM Configuration**

Next configuration is needed in next menu. [CONFIGURATION > Miscellaneous > System Options]

System Options		_ • ×
Node Name NODE 0 • • • • • • • • • • • • • • • • • •	lear Reset	
Name	Value	Node Name
System Public HTTPS Port For Phone Provision	443	NODE 0
System Public IP Address For Admin	none	NODE 0
System Public IP Address For Call	none	NODE 0
System Public IP Address For Phone Provision	none	NODE 0
System SPAM Call Expire Timer (second)	10	NODE 0
System Under NAT	DISABLE	NODE 0
	1	
<b>44 4</b> 2/2 (132) <b>▶ ▶</b>	Detail Change Excel Att	tach Close

Enter the Public IP of firewall into 'System Public IP Address For Call'.

# 6 Interworking local gateway

# 6.1 SCM

SCM configuration is as follows for interworking local gateway.

#### **Route Configuration**

Route must be created for interworking gateway. [CONFIGURATION > Trunk Routing > Route]

Note - Create			
Route Type	User Group 💌	User Group	UG1
Route Name	Gateway	Location	UG1-LOC1
Access Number		Register Type	Receive REGISTER
Proxy Server	165,213,177,248	Port	5060
User Name	GATEWAY	Domain Name	
Authentication User Name	1q2w3e	Authentication Password	1q2w3e
DNS		Outbound CLI Prefix	
DTS Mode	Disable	A-A Primary Node	NODE 0
A-A Dual Registration	Enable		
	Create	Close	

- 1) Select the 'Register Type' to 'Receive REGISTER'.
- 2) Enter the Gateway IP into 'Proxy Server'.
- 3) Enter the 'User Name', 'Authentication User Name' and 'Authentication Password' to refer a gateway setting.
- 4) In Active-Active System case, 'A-A Primary Node' must be set.

#### **Gateway Link Setting**

Create a Gateway Link in next menu. [CONFIGURATION > Gateway > Gateway Link Setting]

😹 [DIALOG]Gateway Link Setting - Cr	reate				- • •
User Group	UG1	-	Name	GATEWAY	<b>▲</b>
Gateway Type	OfficeServ 7400	-			
IP Address(for SIP register)	165,213,177,248		IP Address(for Provision)	165,213,177,248	
NAT	Disable	-	Public IP Address		
MAC Address(0)	11:22:33:44:55:66		MAC Address(1)		
URL					
Login IP Address(MAT)			Login Password(MAT)		
Survivability Users - SIP					
[Selected]			[ AII ]		
			6001		
			6003		
			6004		
			6005		
		•	6006		
			6008		
			6009		
			6010		-
			6011		
1 × ×				Search	
Survivability Users - FXS					
[Selected]			[ AII ]		
		_			
		•			
		*			
	]		<u> </u>		
	Create	Apply	Close		

- 1) Name must be same with 'User Name' in Route.
- 2) Select the 'Gateway Type'.
- 3) Enter the Gateway IP into 'IP Address (for SIP register)'/'IP Address (for Provision)'.
- 4) Select a 'Disable' to 'NAT'.
- 5) Enter the MAC Address of Gateway into 'MAC Address (0)'

#### **Registration Checking**

You can check a registration status of Gateway in next menu. [CONFIGURATION > Registration Status > Registration Status]

## 6.2 OfficeServ7400

#### **IP** setting

On the SIO screen connected to OfficeServ 7000 series, enter the 'ip\_help' command to view a list of available commands.

Set the IP address with the 'ip\_set' command, check the IP address with the 'ip\_config' command, and restart OfficeServ 7000 series with the 'sys\_reset' command.

```
-> ip_help
ip_helpDisplay this help messageip_set "IP","NM","GW"Set IP Address, NetMask, Gatewayip_configShow Info. about Network Interfaces
sys reset
                    System restart
-> ip_set "165.213.89.141", "255.255.255.0", "165.213.89.1"
>>> IP Address = 165.213.89.141
>>> Subnet Mask = 255.255.255.0
>>> Gateway
-> ip config
           <<<<< Network Configuration >>>>
   +-----+
   | No |
           Items
                          Value
                                                     +-----+
   | 0 | MAC Address
                    | 00-00-F0-E8-6F-AA
                                                    | 1 | IP Address | 165.213.89.141
| 2 | Subnet Mask | 255.255.0

        3
        Default Gateway
        165.213.89.1

                                                    -> sys_reset
```

## **Country configuration**

You should use DM from now.

DM 2.1.0 System Selection  $\rightarrow$  System Country  $\rightarrow$  select the country.

•		
IPv4		
165.213.89.141		
165.213.89.1		
255.255.255.0		
Dual		

### **MGI configuration**

DM 2.2.2-configure MGI IP.

2.2.2.MGI Card			
C1-S5			
Item	Value		
Card Type	MGI 16/64		
IP Address	10.254.168.40		
Gateway	10.254.168.1		
Subnet Mask	255.255.255.0		
ІР Туре	Private Only		
MAC Address	00:16:32:C5:A3:03		
Local RTP Port (start)	30000		
Public IP Address 1	0.0.0.0		
Public RTP Port 1	30000		
Public IP Address 2	0.0.0.0		
Public RTP Port 2	30000		
Public IP Address 3	0.0.0.0		
Public RTP Port 3	30000		
	D1 11		

#### **Provisioning Link configuration**

You should configure the Provisioning Link to receive the User Profile data from the SCM Express

DM 5.6.1-set the SCM IP at Master IP address

If SCM is Active-Active configuration, set the Slave SCM IP at Slave IP Address

5.6.1.System I/O Parame	eter	
	Item	Value
MGI Alive Time (sec)		5
COM Expraça Saniar	Master IP Address	165.213.66.93
SOM Express Server	Slave IP Address	255.255.255.255

#### **Connecting to SCM Server**

To have OfficeServ 7000 Series interoperate with SCM, the following items must be configured for SCM and OfficeServ 7000 Series

1) DM 5.2.13 SIP Carrier Options settings

Name	Description
SIP Carrier Name	Set to SCM
SIP server Enable	Enabling SIP server.
Outbound Proxy	Specify the IP address or the domain name of SCM.
Alternative Outbound Proxy	Specify the IP address of Slave SCM on Active-Active configuration.
Proxy Domain Name	Domain Name of SCM User Group.
User Name	Specify the number for the gateway to be registered as an endpoint.
Auth Username	Username of the gateway for authentication.
Auth Password	Password of the gateway for authentication.
Regist. Per User	Set to Per User
Trunk CLI Table	Specify a table containing the called phone number to be used for incoming analog trunk calls. Select one from Tables 1 through 4 in the 'DM 2.4.3 Send CLI Number'
Dual Registration	Set to Enable on Active-Active configuration

SIP Carrier 1				
Item	Value			
SIP Carrier Name	SCM			
SIP Server Enable	Enable			
SIP Service Available	Yes			
Registra Address				
Registra Port	5060			
Outbound Proxy	165.213.66.93			
Alternative Outbound Proxy	0.0.0.0			
Outbound Proxy Port	5060			
Proxy Domain Name	ug1.scm.com			
Local Domain Name				
SMS Domain Name				
DNS Server 1	0.0.0.0			
DNS Server 2	0.0.0.0			
User Name	OS7400			
Auth Username	OS7400			
Auth Password	****			
Regist Per User	PerUser			
Session Timer	None			
Session Expire Time (sec)	1800			
Trunk Reg Expire Time (sec)	1800			
Representative Reg Expire Time (sec)	60			
Alive Notify	None			
Alive Notify Time (sec)	60			
IMS Option	Disable			
P Asserted ID Use	None			
SIP Peering	Disable			
Send CLI Table	1			
Supplementary Type	PBX Managed 2			
302 Response	Disable			
SIP Destination Type	To Header			
Codec Auto Nego	Enable			
URI Type	SIP			
SIP Signal Type	UDP			
PRACK Support	Disable			
Hold Mode	Send Only			
Response to Tag	Кеер			
SIP Connection Reuse	Enable			
SIP Mutual TLS Enable	Enable			
SIP Validate Any TLS Certificate	Enable			
SIP Trunking Codec PR1	G.729			
SIP Trunking Codec PR2	G.711a			
SIP Trunking Codec PR3	G.711u			
SIP Trunking Codec PR4	Disable			
SIP Trunking Use Alias	Disable			
SIP Trunking Max Channel	224			
Outgoing Originator Codec Use	Disable			
Incoming Call Fixed Codec	Disable			
- Anonymous Host Name	Disable			
Dual Registration	Disable			
Trunk Ring Plan CLI Table	1			
Trunk Group Number interworking SCM	805			

#### 2) DM 5.2.14 SIP User settings

Name	Description
User Name	Specify the number for the gateway to be registered as an endpoint.
Auth Username	Username of the gateway for authentication.
Auth Password	Password of the gateway for authentication.
Tel number	Enter the called group number for the trunk. The called group number is the number specified for 'Group Number' in the '4.1.2 Trunk Groups' menu of OfficeServ DM.

5.2.14.SIP Users									
Table No (	1 💌								
Entry No	User Name	Auth User Name	Auth Password	Tel Number	Registration Status	Registration Status 2nd			
1	OS7400	OS7400	*****	805	Yes	No			
2					No	No			
3					No	No			
4					No	No			

### 6.3 iBG

#### IP address & static route configuration

You need to connect to Ubigate iBG via Console with terminal program. Following steps show the way to configure IP address.

```
iBG# configure terminal
iBG/configure# interface ethernet 0/1
iBG/configure/interface/ethernet (0/1)# ip address 10.10.10.100/24
iBG/configure/interface/ethernet (0/1)# exit
iBG/configure# ip route 0.0.0.0/0 10.10.10.1
```

#### **SCM** connection

Following example shows the way to configure voip gateway.

```
iBG# configure terminal
iBG/configure# voip-gateway
// VoIP gateway must be shutdown before setting.
iBG/configure/voip-gateway# shutdown
// setting domain name.
iBG/configure/voip-gateway# host domain-name ugl.scm.com
// setting source interface for SIP and media.
iBG/configure/voip-gateway# bind control interface ethernet 0/1
iBG/configure/voip-gateway# bind media interface ethernet 0/1
iBG/configure/voip-gateway# call-server
```

```
// Setting a SCM server IP Address.
iBG/configure/voip-gateway/call-server# ip-address ipv4:10.10.10.10
iBG/configure/voip-gateway/call-server# ip-address ipv4:10.10.10.11
secondary
\ensuremath{{\prime}}\xspace // Setting gw-uri and Ubigate iBG will register to SCM as an Endpoint.
iBG/configure/voip-gateway/call-server# gw-uri ibg-gw-001
iBG/configure/voip-gateway/call-server# exit
// Setting the username and password for \ensuremath{\mathsf{G}}/\ensuremath{\mathbb{W}} endpoint authentication.
iBG/configure/voip-gateway# sip-ua authentication username ibg-name
password pw1234
// Restarts VoIP gateway.
iBG/configure/voip-gateway# no shutdown
iBG/configure/voip-gateway# exit
iBG/configure# exit
// save current configuration.
iBG# save local
```

# 7 Interworking remote site gateway

## 7.1 SCM

SCM configuration is as follows for interworking remote site gateway.

#### 7.1.1 Same Network Configuration

It is same with interworking local gateway basically. Please refer to '6 Interworking local gateway' page.

#### 7.1.2 Different Network Configuration (Gateway in Public Network)

#### **Route Configuration**

Route must be created for interworking gateway. [CONFIGURATION > Trunk Routing > Route]

😹 [DIALOG] Route - Create			
Route Type	User Group 💌	User Group	UG1 🔽
Route Name	Gateway	Location	UG1-LOC1
Access Number		Register Type	Receive REGISTER
Proxy Server	165,213,177,248	Port	5060
User Name	GATEWAY	Domain Name	
Authentication User Name	1q2w3e	Authentication Password	1q2w3e
DNS		Outbound CLI Prefix	
DTS Mode	Disable	A-A Primary Node	NODE 0
A-A Dual Registration	Enable		
	Create	Close	

- 1) Select the 'Register Type' to 'Receive REGISTER'.
- 2) Enter the Public IP of Gateway into 'Proxy Server'.
- 3) Enter the 'User Name', 'Authentication User Name' and 'Authentication Password' to refer a gateway setting.
- 4) In Active-Active System case, 'A-A Primary Node' must be set.
- 5) If there are NAT instead of SBC between SCM and Gateway, Select a 'Enable' to 'Nat Traversal' Option.

#### **Gateway Link Setting**

Create a Gateway Link in next menu. [CONFIGURATION > Gateway > Gateway Link Setting]

😹 [DIALOG]Gateway Link Setting - Cr	reate					- • ×
User Group	UG1	-	Name	GATEWAY		
Gateway Type	OfficeServ 7400					
IP Address(for SIP register)	165,213,177,248		IP Address(for Provision)	165,213,177,248		
NAT	Disable	-	Public IP Address			
MAC Address(0)	11:22:33:44:55:66		MAC Address(1)			
URL						
Login IP Address(MAT)			Login Password(MAT)			
Survivability Users - SIP						
[Selected]			[ AII ]			
			6001			<b>_</b>
			6002			
		_	6004			
		•	6005			
		•	6006			
			6007			
			6009			
			6010			
			6011			
* *					Search	
Survivability Users - FXS						
[Selected]			[ AII ]			
		_				
		•				
		₩				
		_				
	Create	Apply	Close			

- 1) Name must be same with 'User Name' in Route.
- 2) Select the 'Gateway Type'.
- 3) Enter the Gateway IP into 'IP Address (for SIP register)'/'IP Address (for Provision)'.
- 4) Select a 'Disable' to 'NAT'.
- 5) TCP 8088 port must be forwarded to SCM in Firewall for using Public IP.
- 6) Enter the MAC Address of Gateway into 'MAC Address (0)'

#### **Registration Checking**

You can check a registration status of Gateway in next menu. [CONFIGURATION > Registration Status > Registration Status]

#### 7.1.3 Different Network Configuration (Gateway under NAT)

#### **Route Configuration**

Route must be created for interworking gateway. [CONFIGURATION > Trunk Routing > Route]

😹 [DIALOG] Route - Create				
Route Type	User Group 💌	User Group	UG1	
Route Name	Gateway	Location	UG1-LOC1	-
Access Number		Register Type	Receive REGISTER	-
Proxy Server	165,213,177,248	Port	5060	
User Name	GATEWAY	Domain Name		
Authentication User Name	1q2w3e	Authentication Password	1q2w3e	
DNS		Outbound CLI Prefix		
DTS Mode	Disable	A-A Primary Node	NODE 0	-
A-A Dual Registration	Enable			
	Create Ap	Close		

- 1) Select the 'Register Type' to 'Receive REGISTER'.
- 2) Enter the Public IP of Gateway into 'Proxy Server'.
- 3) Enter the 'User Name', 'Authentication User Name' and 'Authentication Password' to refer a gateway setting.
- 4) In Active-Active System case, 'A-A Primary Node' must be set.
- 5) If there are NAT instead of SBC between SCM and Gateway, Select a 'Enable' to 'Nat Traversal' Option.

#### **Gateway Link Setting**

Create a Gateway Link in next menu. [CONFIGURATION > Gateway > Gateway Link Setting]

😻 [DIALOG]Gateway Link Setting - Cr	eate					• ×	
User Group	UG1	-	Name	GATEWAY		_	
Gateway Type	OfficeServ 7400						
IP Address(for SIP register)	165,213,177,248		IP Address(for Provision)	165,213,177,248			
NAT	Enable	•	Public IP Address	1.2.3.4			
MAC Address(0)	11:22:33:44:55:66		MAC Address(1)				
URL							
Login IP Address(MAT)			Login Password(MAT)				
Survivability Users - SIP							1
[Selected]			[ All ]				
			6001				
			6002				
		_	6004				
		-	6005				
		₩	6006				1
		_	6007				
			6008				
			6010				
			6011				1
± ¥					Search		
					·		1
Survivability Users - FXS			-[ 40 ]				
[ Selected ]			1.801				
		8					
		•					
11							-
	Create	Apply	Close				

- 1) Name must be same with 'User Name' in Route.
- 2) Select the 'Gateway Type'.
- 3) Enter the Gateway real IP into 'IP Address (for SIP register)'/'IP Address (for Provision)'.
- 4) Select a 'Enable' to 'NAT'.
- 5) Enter the Public IP of Gateway into 'Public IP Address'.
- 6) TCP 8088 port must be forwarded to SCM in Firewall for using Public IP.
- 7) Enter the MAC Address of Gateway into 'MAC Address (0)'

#### **Registration Checking**

You can check a registration status of Gateway in next menu. [CONFIGURATION > Registration Status > Registration Status]

# 7.2 OfficeServ7400

It is same configuration with local gateway case except for one setting. If SBC exist between SCM and remote site gateway, SCM IP address must be configured with SBC's IP address.

## 7.3 iBG

It is same configuration with local gateway case except for one setting. If SBC exist between SCM and remote site gateway, call-server IP address must be configured with SBC's IP address.

# 8 Interworking FXS

# 8.1 SCM

Create a user on the phone type set to Analog-FXS-Phone and, if necessary, to operate in survival mode by specifying the gateway will generate.

[DIALOG] Single Phone User - Change				-	X
User Group	UG1	-	Service Group	UG1-SG1	<b>_</b>
Location	UG1-LOC1	-	Extension Number	2004	
Application User ID	2004@ug1,scm,com		Extension Name	2004	
Application Password	*****		PIN Number	****	
Authentication User ID	2004		Phone Verification	None	•
Authentication Password	****		MAC Address		
IP Address			Private IP Address		
Profile Login ID	UG12004		Phone Type	Analog-FXS-Phone	<b>_</b>
Profile Login Passcode	****		Language	Korean	▼
Mobile Phone Number	01020002004		Use Mobile Phone Number	None	<b>T</b>
Protocol	UDP	-	Media	RTP	<b>_</b>
TLS Connection	Reuse		Ping Ring Type	None	
A-A Primary Node	NODE 0		A-A Dual Registration	Disable	
VMS Extension Number			Make Mailbox	Yes	<b>_</b>
URI Type	SIP		DTMF	RFC2833	
RFC2833 DTMF Payload	101		Time Zone	GMT +09:00 Asia/Seoul	<b>_</b>
Department		-	Position		<b>_</b>
Send CLI Number			Service Group Local CLI Number		<b>_</b>
Service Group Local Number			Restriction Policy		<b>_</b>
Class of Service	level5	-	Gateway Name		<b>_</b>
Extension Lock	None	<b>_</b>	LDAP DN Number		
Account Code Use		<b>_</b>	Auto Answer by Click to Dial	Enable	
Accept Login Override	Disable		External Ringback Tone Use	None	
MOH Announcement ID		-	Display Option	Normal	<b>_</b>
Send CLI Name			Call Monitoring	Disable	
Send Extension Number			Use Virtual Ringback	Disable	
Caller Ring Type	None	<b>v</b>	Off Hook Alarm		<b>_</b>
Check Registration Protocol	Disable	-	MOH SIP Media Mode	Send Only	-
Application Server Service Group		-	CMS Monitoring	Disable	
		Change App	ly Close		
## 8.2 OfficeServ7400

### **FXS Settings**

1) DM 5.2.14 SIP User settings

Item	Description
User Name	Specify the number for the extension to be registered as an subscriber.
Auth Username	ID of the extension for authentication.
Auth Password	Password of the extension for authentication.
Tel number	Specify the extension number of '2.8.0 Numbering Plan' of OfficeServ DM

#### ex) FXS 3007 registration

	5.2.14.SIP Users									
	Table No 1									
	Entry No	User Name	Auth User Name	Auth Password	Tel Number	Registration Status	Registration Status 2nd			
1		OS7400	OS7400	*****	805	Yes	No			
2		3007	3007	****	3007	Yes	No			
3						No	No			
4						No	No			

#### 2) DM 2.4.3 Send CLI Number settings

Enter the FXS phone's extension number in the table selected for 'Send CLI Table' in the '5.2.13 SIP Carrier Options' menu of OfficeServ DM.

2.4.3.Send CLI Number								
Tal Number		Send CL	l Number		Con			
Ternumber	1	2	3	4	Sen			
2033								
2034								
2035	3007							
2036								
2037								

## 8.3 iBG

#### **MAC address Setting**

Following steps show the way to get system MAC address of iBG.

```
iBG# show mac system
Starting MAC = 00:16:32:xx:xx
```

### Setting the address in following menu. [Gateway > Gateway Link Setting]

	[DIALOG]Gateway Link Setting - Cl	hange				
CONFIGURATION	User Group Gateway Type	UG1 iBG2006	<b>v</b>	Name	gw2006	<b>_</b>
Location	IP Address(for SIP register)	10,254,176,226		IP Address(for Provision)	10,254,176,226	
🗄 User Group	NAT	Disable	<b>v</b>	Public IP Address		
⊞ User	MAC Address(0)			MAC Address(1)		
Trunk Routing				Galeway Reconnect		
Time Schedule	-Survivability Lisers - SID-			LUGIII PASSWUIU(MAT)		
⊞ Service	[Selected]			[ AII ]		
Wireless Enterprise				2000		<u> </u>
<ul> <li>Application</li> </ul>				2001		
Phone Setting				2002		
Announcement				2004		
Miscellaneous			*	2005		_
🗆 Gateway				2007		
Gateway Link Setting				2008		
🗄 Ubigate Slot Setting				2009 2010		<b>_</b>
Ubigate Port Setting	± Ŧ				Searc	sh 🗌
Active/Active Redundan						
Inter-SCM Setting	Survivability Users - FXS					

#### **Slot Setting**

Select a Gateway which you want to configure in the following window, and press **[Change]** button and select change.

Select a Slot Configuration item and choose a card type properly. Slot State indicates actual card equipment state. This state can be updated by receiving information from the gateway.

[Gateway > Ubigate Slot Setting > iBG2006/2016/3026] or [Gateway > Ubigate Slot Setting > iBG1003/1004]

	User Group	Gateway Nam	e Gateway Type	Country	S1(0/0)	S1(0/0) State	S2(0/1)	S2
User	UG1	gw2006	iBG2006	Korea	FXS-4M	FXS-4M	FXO-4M	FXC
Trunk Routing		Change						
Time Schedule	S [DIALOG]/BG2000/2010/5020 -	Change						
Service	User Group	UG1		<b>~</b>	Gate	way Name	gw2006	
Wireless Enterprise	Gateway Type	iBG2006		<b>v</b>	Locate	ed Country	Korea	
	Slot S1(0/0) Configuration	FXS-4M		•	Slot S	1(0/0) State	FXS-4M	
Application	Slot S2(0/1) Configuration	FXO-4M		<b>~</b>	Slot S	2(0/1) State	FXO-4M	
Phone Setting	Slot S3(0/2) Configuration	T1E1-2M		-	Slot S	9(0/2) State	T1E1-2M	
Announcement	Slot S4(0/3) Configuration	None		~	Slot S4	\$(0/3) State		
Miscellaneous	Slot NM1(1) Configuration	None		~	Slot N	v11(1) State		
Gateway	Slot NM2(2) Configuration	None		~	Slot N	vl2(2) State		
Gateway Link Set	FAX Relay	T38 Redun	dancy 3	-	DTM	IF Relay	Inband	
🗆 Ubigate Slot Setti	Media Type	RTP		-	T1/E	1 Select	E1	
iBG2006/2016/3	Use Diversion User Info	Disable		-				
iBG1003/1004				Change Ap	oply Close			

#### **Port Setting**

Select an FXS port which you want to configure in the following window, and press **[Change]** button and select change.

To set extension number of an FXS port, click the 'Extension Number' menu and select a number from listed numbers. To configure this, FXS user must be configured in advance. To remove this port configuration, select the blank instead of the number.

#### [Gateway > Ubigate Port Setting > FXS (Analog Phone)]

one Setting	User (	Froup  Gate	way Name	Slot/Port	Extension Nu	Message Wa	I CID Send	ICID S	ignal Ly	Polarity Reve
nouncement	UG1	gw20	106	0/0/0	3000	Disable	Disable	FSK		Disable
	UG1	gw20	06	0/0/1	3001	Disable	Disable	FSK		Disable
scellaneous	UG1	gw20	06	0/0/2		Disable	Disable	FSK		Disable
iteway	LUC1		ine	0/0/9		Dischlo	Disabla	ECV		Disabla
Gateway Link Settir	[DIALOG]FXS (Analog	Phone) - Cha	nge							l
Ubigate Slot Settins	User Grou	p	UG1		- (	ateway Name	[	gw2006		
iBG2006/2016/30:	Slot/Port		0/0/0		<ul> <li>Extension Number</li> </ul>		[	3000		
iBG1003/1004	Message Waiting	ndication	Disable			-	CID Send	[	Disable	
Ubigate Port Settin:	CID Signal T	уре	FSK		2	<ul> <li>Polar</li> </ul>	ity Reverse Signal	[	Disable	
PBI Trunk	Loop Open Re	lease	Disable			🖌 Ca	l Progress Tone	[	System Def	ault
EYO (Apalog Tr	Media Dial T	one	None			-				
TAO (Analog III					Change A	DDIV CI	ose			
FXS (Analog Ph					<u> </u>					

## 9 Interworking PRI

## 9.1 SCM

#### **Creating Route**

Route must be created for interworking gateway. [CONFIGURATION > Trunk Routing > Route]

😹 [DIALOG] Route - Create			
Route Type	User Group 💌	User Group	UG1 🔽
Route Name	Gateway	Location	UG1-LOC1
Access Number		Register Type	Receive REGISTER
Proxy Server	165,213,177,248	Port	5060
User Name	GATEWAY	Domain Name	
Authentication User Name	1q2w3e	Authentication Password	1q2w3e
DNS		Outbound CLI Prefix	
DTS Mode	Disable	A-A Primary Node	NODE 0
A-A Dual Registration	Enable		
	Create	ply Close	

- 1) Select the 'Register Type' to 'Receive REGISTER'.
- 2) Enter the Public IP of Gateway into 'Proxy Server'.
- 3) Enter the 'User Name', 'Authentication User Name' and 'Authentication Password' to refer a gateway setting.
- 4) In Active-Active System case, 'A-A Primary Node' must be set.
- 5) Fill out Access Number to select The PRI trunk

#### Selecting Access Code Type and Setting DID number

#### [CONFIGURATION > Trunk Routing > Route > Access Code]

If you want to send number with access code, select the internal number type. Normal Type make number to send without access number.

IDIALOG]Access Code - Create			
User Group	UG1	Access Number	9
Number Type	Normal	Location Based Routing Name	RPar_9
Minimum Digit Length	2	Maximum Digit Length	40
	Create	ly Close	

#### [CONFIGURATION > Trunk Routing > Route > DID Routing]

If you want receive call from PRI, you must configure DID number.

## 9.2 OfficeServ7400

#### **PRI settings**

DM 5.2.14 SIP User setting

ltem	Description
User Name	Specify the name for the PRI trunk group to be registered as an endpoint.
Auth Username	ID of the endpoint for authentication.
Auth Password	Password of the endpoint for authentication.
Tel number	Enter the called group number for the PRI trunk. The called group number
	is the number specified for 'Group Number' in the '4.1.2 Trunk Groups'
	menu of OfficeServ DM.

#### ex) PRI registration (OS7400\_pri)

	5.2.14.SIP Users									
	Table No 1									
	Entry No	User Name	Auth User Name	Auth Password	Tel Number	Registration Status	Registration Status 2nd			
1		OS7400	OS7400	*****	805	Yes	No			
2		OS7400_pri	OS7400_pri	*****	806	Yes	No			
3						No	No			
4						No	No			

## 9.3 iBG

#### **Slot setting**

Refer to Interworking FXS for slot setting. T1E1 card is required for PRI.

#### **Port setting**

Select an ISDN-PRI trunk which you want to configure in the following window, and press **[Change]** button and select change. Change configurations of the ISDN-PRI trunk, in this window you can change items.

To select name of an ISDN-PRI trunk, click 'Route Name' menu and select a route name from listed names. Route must be configured in advance. To remove this port configuration, select the blank instead of the name.

#### [Gateway > Ubigate Port Setting > PRI Trunk]

he	Setting	Use	r Group	Gateway Name	Slot/Port	Route Name	Sending Com,	PRI	Trunk Type	Switch Type	Use Channels
bu	uncement	UG1		gw2006	0/2/0		Disable	TE		NI2	30
.e	IDIALOG]PRI Trunk - Change	-		And and a second	-		-	-		-	
31	User Group		UG1		[	- G	ateway Name		gw2006		
3	Slot/Port		0/2/0		[	-	Route Name				
Л	Sending Complete		Disable		[	- P	RI Trunk Type		TE		-
I	Switch Type		NI2		[	<b>-</b> ι	lse Channels		30		
l					Change /	Apply Clo	se				
JE	hgate i ort octania	_						-			
	PRI Trunk										

## 10 Interworking FXO

## 10.1 SCM

Route must be created for interworking gateway. [CONFIGURATION > Trunk Routing > Route]

😹 [DIALOG] Route - Create			
Route Type	User Group 💌	User Group	UG1
Route Name	Gateway	Location	UG1-LOC1
Access Number		Register Type	Receive REGISTER
Proxy Server	165,213,177,248	Port	5060
User Name	GATEWAY	Domain Name	
Authentication User Name	1q2w3e	Authentication Password	1q2w3e
DNS		Outbound CLI Prefix	
DTS Mode	Disable	A-A Primary Node	NODE 0
A-A Dual Registration	Enable		
	Create Ap	ply Close	

- 1) Select the 'Register Type' to 'Receive REGISTER'.
- 2) Enter the Public IP of Gateway into 'Proxy Server'.
- 3) Enter the 'User Name', 'Authentication User Name' and 'Authentication Password' to refer a gateway setting.
- 4) In Active-Active System case, 'A-A Primary Node' must be set.
- 5) Fill out Access Number to select The FXO trunk

## 10.2 OfficeServ7400

### **FXO settings**

1) DM 5.2.14 SIP User settings

ltem	Description
User Name	Specify the name for the FXO trunk group to be registered as an endpoint.
Auth Username	ID of the endpoint for authentication.
Auth Password	Password of the endpoint for authentication.
Tel number	Enter the called group number for the FXO trunk. The called group number is the number specified for 'Group Number' in the '4.1.2 Trunk Groups' menu of OfficeServ DM.

### ex) FXO registration (OS7400\_fxo)

5.2.14.SIP Users	3					
Table No 1	-					
Entry No	User Name	Auth User Name	Auth Password	Tel Number	Registration Status	Registration Status 2nd
1	OS7400	OS7400	*******	805	Yes	No
2	OS7400_fxo	OS7400_fxo	*****	8	Yes	No
3					No	No
4					No	No

#### 2) DM 2.4.3 Send CLI Number setting

Enter the called phone number to use for incoming FXO trunk calls in the table selected for 'Trunk CLI Table' in the '5.2.13 SIP Carrier Options' menu of OfficeServ DM

2.4.3.Send CLI Number							
Tel Number		Send CLI Number					
Ternumber	1	2	3	4	Senu S		
7001			3010				
7002							
7003							
7004							

## 10.3 iBG

#### **Slot setting**

Refer to Interworking FXS for slot setting.

#### Port setting

Select an FXO trunk which you want to configure in the following window, and press **[Change]** button and select change. Change configurations of the FXO trunk, in this window you can change items.

To select name of an FXO trunk, click 'Route Name' menu and select a route name from listed names. Route must be configured in advance. To remove this port configuration, select the blank instead of the name.

#### [Gateway > Ubigate Port Setting > FXO (Analog Trunk)]

ne Se	tting	User Gro	up  Gateway Nam	e Slot/Port	Route Name	Destination N	CID Recei	ve  CID Signal T	yPolarity Reve
ounce	ment	UG1	gw2006	0/1/0			Disable	FSK	Disconnect
		UG1	gw2006	0/1/1			Disable	FSK	Disconnect
eway	😻 [DIALOG]FXO (Analog Tru	unk) - Change		-					
Gatev	User Group	U	G1		<b>v</b>	Gateway Name	gw	2006	
Ubiga	Slot/Port	0,	/1/1		-	Route Name			
iPi	Destination Number	er 🗌				CID Receive	Dis	able	
	CID Signal Type	F	SK		Pol	arity Reverse Sign	al Dis	connect	
IBI	Loop Open Releas	se D	isable		<b>–</b> C	all Progress Tone	Sy	stem Default	
Ubiga PF				Change	Apply	Close			
FX	O (Analog Trunk)								

## 11 Interworking SIP trunk

This section describes a process of creating information for trunks. The information shown below are the mandatory requirements for trunk calls, listed in the required order of creation.

- 1) Route information: This is the trunk port information for external connection to ITSP SIP servers, gateways, and other entities that interoperate with SCM.
- 2) LCR information: Specifying the preferred routes that are connected to the endpoint allows automatic selection of alternative routes and other factors.
- 3) LCR by location table information: You can specify different call routes according to the caller's location.
- 4) Access code information: This is the access code used for selecting trunk call routes.

## 11.1 Making Routes

A route means a conceptual path connected to an SIP server, a gateway, and other entities interoperating with SCM. The route includes information on the handling method for outgoing/incoming calls from each external connection endpoint as well as the number translation policy information.

You can create routes using the **[CONFIGURATION > Trunk Routing > Route]** menu. The blue text items are mandatory.

F			
[DIALOG] Route - Create			
Route Type	User Group	User Group	<b>_</b>
Route Name		Location	<b></b>
Access Number		Register Type	Send REGISTER
Proxy Server		Port	5060
User Name		Domain Name	
Authentication User Name		Authentication Password	
DNS		Outbound CLI Prefix	
DTS Mode	<b></b>	A-A Primary Node	
A-A Dual Registration	<b></b>		
	Create	Close	

#### Figure 1. Making Routes

ltem	Description
Route Type	<ul> <li>Specify whether the route is used for one particular user group or shared by all user groups.</li> <li>Common: Can be used by all user groups. If used for incoming calls only, additional settings are required, as number analysis is necessary to identify the user group being called.</li> <li>User Group: Can be used only by one particular user group.</li> </ul>
User Group	Select a user group to which the route belongs. If route type is set to Common, the user group also must be set to Common.
Location	Specify a location to which the endpoint belongs.

Item	Description
Register Type	Specify a registration method for the endpoint.
	- Receive REGISTER: REGISTER is received from the endpoint for
	registering the endpoint.
	- Send REGISTER: SCM sends REGISTER to the endpoint for registration.
	- None: No registration is performed between the endpoint and SCM.
Proxy Server	Specify the primary proxy server address for the endpoint.
Port	Specify a port number for the endpoint.
User Name	Specify the user name to use in user info of SIP URI.
DTS Mode	Specify the trunk option to use DTS Service
A-A Primary Node	Specify a node to use primary node.
	When trunk sends registration message, it sends to first selected node.
A-A Dual Registration	Specify the dual-registration.
	If register type is send trunk, this option must set 'disable'.
Access Code	Enter an access code to use when making calls to trunks instead of
	extension numbers.
	If you set this option in this step, Priority Routing, Location Based Routing
	and Access Code are created automatically.

When creating a route, you didn't input data that saved default. If you want changing data then you can change data.

😻 [DIALOG] Route - Change					
Route Type	User Group	-	User Group	UG1	▼ ▲
Route Name	RTE_IBG		Location	UG1-LOC1	•
Register Type	None	-	Proxy Server	165,213,176,xxx	
Port	5060		User Name	pri	
Domain Name	ibg2006,com		Authentication User Name		
Authentication Password			DNS		
Outbound CLI Prefix					
Forced Send CLI Number	None	-	Send CLI Name for User	User Name	•
Send CLI Name for Inbound Call	None	-	CLI for Forwarded Call	Originator	•
Transfer Caller ID	Transfer Party Number	-	Anonymous URI	Anonymous Invalid	<b>_</b>
Anonymous Call Reject	None	-	Route Lock	None	
NAT Traversal	Disable	-	TIE Trunk	Normal	•
URI Type	SIP	-	FXO(Loop Trunk) Destination		
Protocol Type	UDP	-	Register Expires(sec)		
Registrar Address			Maximum Register Retry	1	
Register Retry Interval(sec)			Call Authentication		-
Use Request URI User Info	Disable	-	Keep Alive	Enable	-
Keep Alive Interval(sec)	35		Maximum Keep Alive Retry	1	
Keep Alive Retry Interval(sec)	35		Keep Alive User Info	Disable	•
SIP P-Asserted-ID Type	Primary	-	MOH SIP Media Mode	Send/Receive	<b>_</b>
Indifu E 164 Format	Ma		Outbound Error Announcement	Epoblo	
C Selected 1					
		¥ 4			
*				Search	
	Ch	ange App	Close		

Figure 2. Modifying Routes

Item	Description
Domain Name	Enter a domain to use as the host of SIP URI.
Authentication User Name	Enter the user authentication name used for registration.
Authentication Password	Enter the authentication user password used for registration.
DNS	Enter the IP address of DNS server.
Outbound CLI Prefix	If there is no configuration of 'Send CLI Number' in a user and there is only extension number, when the user make a call through this route and there is prefix, add this prefix to the extension number and send it as calling number.
Forced Send CLI Number	<ul> <li>When make a call to outbound, select the caller ID below:</li> <li>None: Follow the system priority. It is same as the order listed below.</li> <li>Phone CLI Number: Send 'Phone CLI Number' as caller ID.</li> <li>User CLI Number: Send 'User CLI Number' as caller ID.</li> <li>Service Group CLI Number: Send 'Service Group CLI Number' as caller ID.</li> <li>User Group CLI Number: Send 'User Group CLI Number' as caller ID.</li> <li>Outbound CLI Prefix + Extension Number: Send 'Outbound CLI prefix' with 'Extension Number' as caller ID.</li> <li>Extension Number: Send 'Extension Number' as caller ID.</li> </ul>
Send CLI Name for	When make a call to outbound, select the caller Name below:
User	<ul> <li>User Name: send 'User Name' as caller name.</li> <li>Send CLI Name: Send 'Send CLI Name' as caller name.</li> </ul>
Send CLI Name for Inbound Call	If there is no caller name for inbound call, use below options. - None: not used. - Receive CLI Number: use caller number as caller name.
URI TYPE	Select SIPS if the protocol is TLS. Select SIP in other cases.
Protocol Type	Select UDP, TCP, or TLS as the protocol to use.
Register Expires (sec)	This is the expiration period for registration. SCM must retry registration within this period.
Register Retry Interval (sec)	Enter the interval for resending the REGISTER message.
Keep Alive	It is used to verify the connection using SIP OPTION message.
Keep Alive Interval (sec)	Specify an interval (seconds) for exchanging Keep Alive Messages
SIP P-Asserted-ID Type	<ul> <li>Select a type of representative number.</li> <li>Primary: The P-Asserted-Identity header contains the Primary number and the From header contains residential number.</li> <li>Secondary: The P-Asserted-Identity header contains the residential number and the From header contains Primary number.</li> </ul>
Modify E.164 Format	Specify whether to use E.164 format for calling number or called number for outgoing call through this route.
DNS SRV Query	Select whether to use of DNS SRV.
TLS Connection	Specify the TLS connection type:

Item	Description
	- Normal: use TLS Full handshaking method.
	- Reuse: reuses the existing TLS connection established by initial Message.
	- Resume: use simplified handshaking method using TLS Session ID.

## 11.2 Making LCR

A Least Cost Route (LCR) is a method of selecting a route when processing outgoing trunk calls. There are three different types of LCR, as shown below.

#### **Priority Routing**

A priority routing allows automatic selection of alternative routes when the default outgoing path becomes unavailable. Priority is assigned to the direct route and alternative routes. When calls going out through the high-priority route fail, they can be retried through the low-priority routes.

You can create route sequences in the [CONFIGURATION > Trunk Routing > Priority Routing] menu. This menu is used for creating route sequences.

Item	Description
User Group	Specify a user group to which the route sequence belongs.
Name	Specify a name for the route sequence. Pay special attention to choosing the name, as it is used as an identifier when selecting the route sequence in other menus and cannot be changed.
Route Priority	<ul> <li>Assign priority to the route.</li> <li>Direct Route: Specify the top priority route.</li> <li>Alternative Route1 to Alternative Route8: Select the routes according to their priority levels.</li> </ul>
Route Name	Select a route for the route priority level.
Outbound DOD Delete Length	Specifies the length of digits to delete from the first position of the called number for outbound call.
Outbound DOD Insert Digits	Specifies the digits to insert from the first position of the called number for outbound call.
Outbound CLI Delete Length	Specifies the length of digits to delete from the first position of the calling number for outbound call.
Outbound CLI Insert Digits	Specifies the digits to insert from the first position of the calling number for outbound call.
Outbound MCN	Specify MCN rules for outbound call.

#### **Time-based Routing**

A time-based routing sequence contains time conditions so that each service group can use different route sequences according to the conditions.

#### Load-balanced Routing

A load-balanced routing allows use of the selected routes in a specified ratio. Calls are distributed between the routes identified as available for calls, and therefore there is no need for configuring alternative routes.

Among the three types of LCRs, the route sequence type is used by default. For more information on LCRs, including the setup method and route selection, see the 'Least Cost Route (LCR) Policy' section of System Features.

## 11.3 Making Location Based Routing

A location based routing allows each location to use its own LCR. Since each location is set with its own LCR, if you have created multiple locations, you must set an LCR for each of the locations. If no LCR is set for a particular location, the location is not allowed to make trunk calls.

You can create route partitions in the **[CONFIGURATION > Routing > Location Based Routing]** menu. This menu is used for creating Location Based Routing.

ltem	Description
User Group	Select a user group to which the Location Based Routing belongs.
Location Based Routing Name	Enter a name for the Location Based Routing. Pay special attention to choosing the name, as it is used as an identifier when selecting the route partition in other menus and cannot be changed.
Location select	Select whether to use the 'Location'. If Location selects use 'disable', all location can use this Location Based Routing.
Location	Select a location to set the routes.
Routing Type	Select a type of LCR for the location. - Time-Based Routing: Select to use a Time-Based Routing. - Priority Routing: Select to use a Priority Routing. - Load Balance Routing: Select to use a Load Balance Routing.

## 11.4 Configuring Access Codes

Access codes are number to be used for dialing a directly outgoing call. They are also used for analyzing the destination numbers to determine which location-based routes to be used for outgoing trunk calls.

You can create access codes using the [CONFIGURATION > Routing > Access Code] menu. The following items are mandatory.

ltem	Description
User Group	Select a user group to which the access code belongs.
Access Code	Enter an access code to use when making calls to trunks instead of extension numbers. Pay special attention to choosing the code, as it is used as an identifier when selecting the access code in other menus and cannot be changed.
Number Type	<ul> <li>Select a type of access code.</li> <li>The access code can be the beginning portion of the external destination number, or an internal code is used within the boundary of the SIP servers or gateways.</li> <li>Normal: When the calling number for an outgoing trunk call is analyzed, the digit corresponding to the access code is deleted from the number dialed by the user, and then the call is made to the trunk.</li> <li>Internal: When the calling number for an outgoing trunk call is analyzed, the digit corresponding to the access code is not deleted from the number dialed by the user and the call is made to the trunk as is.</li> <li>Emergency: When the calling number for an outgoing trunk call is analyzed, only the digit corresponding to the access code from the number dialed by the user is used as the destination number, and then the call is made to the trunk.</li> <li>Pattern: When analyzing the calling numbers for outgoing trunk calls, a wild card (expressed as X) is used to denote the length. The call is made to the trunk without deleting the digit corresponding to the access code from the number dialed by the user.</li> <li>DTS: When the calling number for an outgoing trunk call is analyzed, the digit corresponding to the access code is not deleted from the number dialed by the user.</li> </ul>
Location Based Routing Name	Select a Location Based Routing to use with this access code.

## 11.5 Configuring DID Routing

Destination of incoming trunk calls depend on the DID number. When entering a DID number, you can use wild cards (entered by \*) to enter multiple numbers at a time. If the called number is set to 'B', a translated DID number is used as the called number.

Also the called number is set to 'E', a translated DID number is used as the called number. Digit differences allow tandem call or not.

You can specify different called numbers for different times of the day. Time periods are defined by ring plans.

For more information on DID number translation and assigning called numbers by ring plans, see the 'DID Routing' section of System Features. Also, for more information on ring plans, see the 'Ring Plan' section of System Features.

You can assign routes by DID number using the [CONFIGURATION > Routing > DID Routing] menu. The following items are mandatory.

Item	Description
User Group	Select a user group to which the calls are directed.
DID Number	Enter a DID number for incoming trunk calls.
Default Destination	Specify a called number to which the incoming calls with the selected DID number are directed. The default called number is used if the current ring plan is not RP1 through RP10.

## 12 Interworking SBC

This section describes a way to set iBG-SBC as sequence of installation. This section includes commands used generally for quick installation. Some setup method for setting network (for example, IP address, default gateway or TLS key) are not described here. You can see them in other sections for 'iBG' in this document. Note that this document contains commands for quick installation only. You can get more information for setup in 'configuration guide for iBG-SBC'.

### 12.1 Media-pool

You can setup a media-pool in iBG-SBC to pass media packets between public network and local network.

#### <Mandatory>

- 1) Set IP address to be used when media packets are passed.
- 2) Set port range to be used when media packets are passed.

#### <Setup method>

 Create or delete media-pool: You can create or delete media-pool with command 'media-pool'. A name 'mpublic' below is just example. A name of media-pool is designated by operator.

```
SBC# configure terminal
SBC/configure# session-router
SBC/configure/session-router# media-pool mpublic (creation)
SBC/configure/session-router# no media-pool mpublic (deletion)
```

2) Setup IP address: You can set IP address to be used when media packets are passed with command 'ip-address'. A IP address '211.123.123.123' below is just example.

```
SBC/configure/session-router/media-pool mpublic# ip-address
211.123.123.123
```

3) Setup port range: You can set port range to be used when media packets are passed with command 'media-port'. First parameter (40000 in below) means starting value of port. Second parameter (512 in below) means range to be used. Range '40000-40512' in below is just example.

SBC/configure/session-router/media-pool mpublic# media-port 40000 512

## 12.2 Region

In iBG-SBC, logical network zone for classifying local and public side is called with 'region'. You can set physical network interface to region with commands below.

#### <Mandatory>

- 1) Designate media-pool to be used in region.
- 2) Designate ethernet interface to be used in region.

#### <Main option>

- NAT option in region.
   (You should set it if there are SIP entities maintained behind NAT)
- Set whether or not iBG-SBC manages SIP registration. (You should set it if there are SIP entities registering via iBG-SBC)
- Change signaling port number to be used in region. (If you don't set it, iBG-SBC will use default port number, UDP-5060, TCP-5060 and TLS-5061)

#### <Setup method>

 Create or delete region: You can create or delete region with command 'region'. A name 'public' below is just example. A name of region is designated by operator.

```
SBC# configure terminal
SBC/configure# session-router
SBC/configure/session-router# region public (creation)
SBC/configure/session-router# no region public (deletion)
```

 Designate media-pool: You can designate media-pool to be used in region with command 'media-pool'. You should designate local media-pool to local region and public media-pool to public region.

SBC/configure/session-router/region public# media-pool mpublic

 Designate network interface: You can designate network interface to be used in region with command 'bind-interface'. A interface 'ethernet 0/1' below is just example. You should designate interface you select.

```
SBC/configure/session-router/region public# bind-interface ethernet
0/1
```

 Set NAT option: You can set NAT option in region with command 'nat-traversal'. If you set NAT option with 'always', iBG-SBC detects SIP entities managed behind NAT with SIP message and handle it properly. If you set NAT option with 'none', iBG-SBC doesn't care information for NAT. If there are SIP entities managed behind NAT, you should set this option with 'always'.

```
SBC/configure/session-router/region public# sip-interface
SBC/configure/session-router/region public/sip-interface# nat-
traversal always
```

5) Set SIP registrar option: You can set SIP registrar option in region with command 'route-to-registrar'. If you set this command, iBG-SBC records username and IP address with SIP 'REGISTER' message and preferentially uses this list to route SIP call.

```
SBC/configure/session-router/region public# sip-interface
SBC/configure/session-router/region public/sip-interface# registrar
SBC/configure/session-router/region public/sip-interface/registrar#
route-to-registrar
```

6) Change signaling port: You can change SIP signaling port in region with command 'local-port'. If you don't set it, iBG-SBC will use SIP default port (UDP=5060, TCP=5060, TLS=5061). If there is no customer's request about it, you don't need to change these ports.

```
SBC/configure/session-router/region public# sip-interface
SBC/configure/session-router/region public/sip-interface#
local-port udp 25060 tcp 25060 tls 25061
```

## 12.3 Policy

iBG-SBC has policy list to be used for routing SIP call. A policy is consist of condition and target. If SIP call corresponds with condition of certain policy, the call will be routed to target of that policy. Each policy has priority. iBG-SBC preferentially searches policy having high priority. If you set route-to-route to region, iBG-SBC will search SIP entities registered with SIP 'REGISTER' before searching policy list.

#### <Mandatory>

- 1) Set condition about source region.
- 2) Set target region.
- 3) Set target address (It can be IP or DNS address).

#### <Main option>

- Set condition about source IP address.
   (Set this option, if you want to accept special IP addresses)
- 2) Set priority.(You can set searching sequence with this)

#### <Setup method>

 Create or delete policy: You can create or delete policy with command 'policy'. A name 'loc2pub' below is just example. A name of policy is designated by operator.

```
SBC# configure terminal
SBC/configure# session-router
SBC/configure/session-router# policy loc2pub (creation)
SBC/configure/session-router# no policy loc2pub (deletion)
```

 Set condition about source region: You can set condition of policy about source region with command 'source-region'. If you don't set it, policy will be out from searching list.

SBC/configure/session-router/policy loc2pub# source-region local

3) Set target region: You can set target region of policy with command 'destinationregion'. If a SIP call corresponds with condition, the call will be route to this region.

```
SBC/configure/session-router/policy loc2pub# routing-policy
SBC/configure/session-router/policy loc2pub/routing-policy#
destination-region public
```

 Set target address: You can set target address of policy with command 'next-hop'. It can be IP or DNS address. A IP and DNS addresses below is just example. Additionally, you can set target port with this command too.

```
SBC/configure/session-router/policy loc2pub# routing-policy
SBC/configure/session-router/policy loc2pub/routing-policy#
next-hop ipv4:128.123.123.123
next-hop ipv4:128.123.123.123:7080
next-hop dns:sec.sip-server.com
next-hop dns:sec.sip-server.com:6070
```

5) Set condition about source IP address: You can set condition about source IP addresses of policy with command 'source-address'. If you don't set it, iBG-SBC doesn't care source IP address. You can set it with subnet-type and range-type. See examples below.

```
SBC/configure/session-router/policy loc2pub#
source-address 211.34.34.0/24
source-address 112.45.45.45/32
source-address 120.30.30.1-120.30.30.100
```

6) Set priority: You can set searching priority of policy with command 'priority'. It can be set from 0 to 99. default value is 50. A smaller one has higher priority.

SBC/configure/session-router/policy loc2pub# priority 30

## 12.4 Security

iBG-SBC supports security function to protect SIP entities don't have permission. iBG-SBC can check permission with IP address and stations. iBG-SBC has 'station' list. In iBG-SBC, stations mean SIP entities that try to register via iBG-SBC and receive '200 OK' response for it. You can set permission for security to call message (INVITE) and normal message (non-INVITE) separately.

#### <Mandatory>

- 1) Create peer-group.
- 2) Set permission.

#### <Setup method>

 Create or delete peer-group: You can create or delete peer-group with command 'peergroup'. A name 'pg\_good' below is just example. A name is designated by operator. Peer-group has IP (or IP range) list with command 'add'. You can use 'no add' command to delete IP (range) from peer-group. You can set IP, IP range and port to peer-group. See below examples.

<Create or delete peer-group >

```
SBC# configure terminal
SBC/configure# session-router
SBC/configure/session-router# peer-group pg_good (creation)
SBC/configure/session-router# no peer-group pg_good (deletion)
```

<Add or delete IP addresses>

```
SBC/configure/session-router/peer-group pg_good#
add 2.3.4.5
add 2.3.4.5-2.3.4.10
add 2.3.4.5:1000-2.3.4.5:3000 (adding IP)
SBC/configure/session-router#
no add 2.3.4.5 (deleting IP)
```

2) Set permission: You can set permission with commands call-permission and message-permission in policy. A call-permission is used to set permission about call (INVITE message) and a message-permission is used to set permission about normal message (non-INVITE message). Subjects of permission can be peer-group or stations.

<Set call-permission>

```
SBC/configure/session-router# policy pub2loc
SBC/configure/session-router/policy pub2loc# call-permission
SBC/configure/session-router/policy pub2loc/call-permission#
permission allow station
permission allow peer-group pg_good
permission reject peer-group pg bad
```

<Set message-permission>

```
SBC/configure/session-router# policy pub2loc
SBC/configure/session-router/policy pub2loc# message-permission
SBC/configure/session-router/policy pub2loc/message-permission#
permission allow peer-group pg_good
permission reject peer-group pg_bad
```

## 12.5 Activating SBC

You can activate and deactivate SBC function with command 'shutdown'. All iBG-SBC's configuration items, except 'features', can be set when SBC function is deactivated only.

#### <Setup method>

1) Activate SBC: You can activate SBC function in iBG with command 'no shutdown'.

```
SBC# configure terminal
SBC/configure# session-router
SBC/configure/session-router# no shutdown
```

2) Deactivate SBC: You can deactivate SBC function in iBG with command 'shutdown'.

```
SBC# configure terminal
SBC/configure# session-router
SBC/configure/session-router# shutdown
```

## **13 NAT/Firewall configuration**

When recognizing that there is a network-aware application program behind the NAT device, the NAT traversal feature obtains the external IP address and performs port mapping in order to transfer the data from the external port of the NAT device to the internal port used by the application program. All this is done automatically. There is no need for the user to manually perform port mapping or use any other mechanism.

To facilitate use of this technology in Internet telephony, SCM provides the media proxy feature for securing communication paths between the IP phones on the NAT network and the systems and phones on the public IP network.

As such, when it is difficult for SCM to obtain a public IP address, it can use the port mapping configuration of the existing NAT system to obtain a private IP address for SCM itself and provide a reliable Internet telephony service with IP phones on the public IP network or IP phones on another NAT network.

To implement this technology, the port information below must be set to open for the NAT system, and port mapping must be configured for the NAT system.

Service	TCP Port	UDP Port	Description
General	20, 21	-	FTP Server
	22		Secure Shell
	23	-	Telnet
	80, 443	-	HTTP Web Server
	389		LDAP Server
	123	123	NTP
Provisioning	69	-	TFTP Server
	8088	-	Gateway Provisioning
-		6000	Phone upgrade from Proprietary to SIP
NMS	-	161	SNMP Agent
Personal	8080, 9500	-	Personal Assistant for Call Service
Management	4002, 4003, 4004	-	Single Sign-On, PWP for UMS/Conference
System Management	20001, 20002, 20003, 20005, 20006	-	SCM Administrator
	5432	-	PostGRE DBMS connection
Call	5060, 5061	5060	SIP signaling
UMS	5080, 8624	5080	Call signaling for UMS

Following is a list of ports must be open when the SCM is located under NAT.

Service	TCP Port	UDP Port	Description
	-	14002~14130	RTP path for UMS
	25, 143, 993	-	Signaling for E-mail Server
3681, 3683, 2001, 22001		-	Signaling for Outlook client
	2200	-	UMS File Server
Conference	3333	5090, 5098	Call signaling for Conference
	-	44000~49998	RTP path for Conference
МОН	-	35000~35999	RTP path for MOH/Announcement
MPS	-	40000~40799	RTP path for MPS (Media Proxy Service)
Others	6000~6127 -		CSTA link for each user group
	9050, 9052	-	PMS link
	9090, 9092,9094	-	Proprietary Application server link
	9000, 9002,5110	-	Voice Monitoring server link
	9010,9011	-	MVS client link
	18124,18126	-	mySingle link
	10306, 2300	-	CDR (Call Data Record)
	-	1812,1813	Radius server
	1122	-	Active-Active node TCP port

## 14 Interworking WE VoIP

### **Creating User**

Create a user on the phone type set to Samsung-Mobile-Phone. Fill in the mobile number and select the using type of mobile phone number.

[CONFIGURATION > User > Single Phone User]

E [DIALOG] Single Phone User - Change			10 A A A		- • ×
User Group	UG1		Service Group	UG1-SG1	▼▲
Location	UG1-LOC1	-	Extension Number	2001	
Application User ID	2001@ug1,scm,com		Extension Name	2001	
Application Password	*****		PIN Number	****	
Authentication User ID	2001		Phone Verification	None	<b>v</b>
Authentication Password	****		MAC Address		
IP Address	10,251,191,164		Private IP Address	10,251,191,164	
Profile Login ID	UG12001		Phone Type	Samsung-Mobile-Phone	•
Profile Login Passcode	****		Language	Korean	<b>v</b>
Mobile Phone Number			Use Mobile Phone Number	None	<b>_</b>
Protocol	UDP	▼	Media	RTP	-
TLS Connection	Reuse	-	Ping Ring Type	None	<b>_</b>
A-A Primary Node	NODE 0	<b>v</b>	A-A Dual Registration	Enable	
VMS Extension Number			Make Mailbo×	Yes	<b>_</b>
URI Type	SIP	-	DTMF	RFC2833	<b>_</b>
RFC2833 DTMF Payload	101		Time Zone	GMT +09:00 Asia/Seoul	<b>_</b>
Department		-	Position		-
Send CLI Number			Service Group Local CLI Number		<b>_</b>
Service Group Local Number			Restriction Policy		<b>_</b>
Class of Service		-	Gateway Name		-
Extension Lock	None	-	LDAP DN Number		
Account Code Use		•	Auto Answer by Click to Dial	Enable	<b>_</b>
Accept Login Override	Disable	<b>v</b>	External Ringback Tone Use	None	<b>v</b>
MOH Announcement ID		-	Display Option	Normal	-
Send CLI Name			Call Monitoring	Disable	-
Send Extension Number			Use Virtual Ringback	Disable	<b>_</b>
Caller Ring Type	None	<b>_</b>	Off Hook Alarm		-
Check Registration Protocol	Disable	<b>_</b>	MOH SIP Media Mode	Send Only	<b>_</b>
Application Server Service Group		-	CMS Monitoring	Disable	
		Change App	ly Close		

#### **Configuration Mobile Service Option**

Set the SSID of the WiFi SSID and the device WiFi must be the same. [CONFIGURATION > Wireless Enterprise > Mobile Service Options]

[DIALOG]Mobile Service Options - Change						
User Group	UG1		SSID			
Remote Dial Public IP Address			Remote Dial Public Port			
Mobile DISA Number			Mobile DISA Code			
Mobile VMS DISA Number			]			
WE Work Server IP Address			WE Work Server Port	80		
WE Work Server Public IP Address			WE Work Server Public Port	80		
WE VoIP CID Server IP Address			WE VoIP CID Server Port	80		
WE VoIP CID Server Public IP			WE VoIP CID Server Public Port	80		
WE Work Server Protocol	НТТР	-	WE VoIP CID Server Protocol	HTTP	<b>~</b>	
WE VoIP CID Server Public Protocol	НТТР	-				
Wait Call, Later Call	False		WiFi Band	Auto	•	
Auto Answer CLI Number			Auto Answer Profile Number			
Use 3G Call Only	No	-	3G Call Prefix			
Logo File Path			]			
24G Channel List						
	ПСНЕ		Пснз	Псна		
И сн э	CH 10			CH 12		
CH 13						
					Selected All	
-5G Channel List						
✓ CH 36	V CH 40		✓ CH 44	🗹 CH 48		
CH 149	V CH 153		✓ CH 157	V CH 161		
					Selected All	
		Change Ap	close			

#### **Configuration Phone Upgrade**

Specify Server Address to upgrade Phone. [CONFIGURATION > Wireless Enterprise > Upgrade Mobile Software]

😻 [DIALOG]Upgrade Mobile Software -	Change					
User Group	UG1 💌					
Download Server 1 - IP Address		Download Server 1 - File Folder				
Download Server 2 - IP Address		Download Server 2 - File Folder				
Download Server 3 - IP Address		Download Server 3 - File Folder				
Download Server 4 - IP Address		Download Server 4 - File Folder				
Download Server 5 - IP Address		Download Server 5 - File Folder				
Change Apply Close						

#### **Configuration Mobile Phone Profile**

[CONFIGURATION > Wireless Enterprise > Mobile Phone Profile]

[DIALOG]Mobile Phone Profile - Char	nge		
User Group	<b></b>	Extension Number	
Mobile Phone Number	<b></b>	User Agent Info	
Select Download Server		Version	
Roaming Trigger		Roaming Delta	
Roaming Scan Period		Noise Supression RX	Image:
Noise Supression TX		AECM	
Echo Suppression	<b></b>	Enable Swing Free RX	▼
Enable Swing Free TX	<b></b>	Enable CNG	Image:
Media Start Port		Media End Port	
Multiframe Enable		Multicast Enable	
TOS Media Value(DSCP)		TOS Control Value(DSCP)	
JBC Threshold			
	Change Ap	ply Close	

## 15 mVoIP

## **Creating User**

Create a user on the phone type set to Samsung-Mobile-Phone and set Use mVoIP option to Enable.

IDIALOG Single Phone User - Change							
Class of Service		-	Gateway Name		-		
Extension Lock	None	-	LDAP DN Number				
Account Code Use		-	Auto Answer by Click to Dial	Enable	•		
Accept Login Override	Disable	-	External Ringback Tone Use	None	•		
MOH Announcement ID		-	Display Option	Normal	•		
Send CLI Name			Call Monitoring	Disable	•		
Send Extension Number			Use Virtual Ringback	Disable	-		
Caller Ring Type	None	-	Off Hook Alarm		•		
Check Registration Protocol	Disable	-	MOH SIP Media Mode	Send Only	-		
Application Server Service Group		-	CMS Monitoring	Disable	•		
FMS Zone Name		-	User Account Code				
Call Recording Method		-	Phone TX Gain				
TLS Key Decryption Password Type	Direct	-	TLS Key Decryption Direct Password				
TLS Key Decryption Device ID			TLS Key Decryption Salt				
TLS Key Decryption IC	512		TLS Key Decryption DK	20			
NFC Mobile Phone Name		-	Phone Call History	On	•		
NFC Auto Login	Disable	-	Allow Selective Call		-		
Phone Display Name	Extension Number	-	Use InterProxy	Disable	•		
PROXYB Index	3		Input Number Display		-		
Change to Multi Type		-	Call Appearance		•		
User Type		-	Error Announcement		•		
Desk Phone Simultaneous Ring Delay	Disable	-	CLI for Forwarded Call		-		
Use mVoIP	Yes		Resume after Transfer-Cancel	No	•		
Telnet Access	Disable	-	WiFi Access	Enable	•		
SIP-PRACK option	Disable	-	Comfort Noise	No	•		
Mobile Number Auto Update	Yes	-	Send RTCP on Hold	No	•		
Change Apply Close							

## **Network Configuration**

Specify Public IP for mVoIP

SCM Administrator		X			
File Tool Tab Dialog Help	🔚 Server16521380.63 💄 User	root 目 Level 1,Engineer			
scм Administrator	📕 🎘 🖳 🖼 🎽				
CONFIGURATION	System Options Upgrade Mobile Software Mobile Phone Profile Mobile Service	Options Lice ( )			
	Node Name NODE 0				
E Service	Search Clear Reset				
Wireless Enterprise	Name Value	Node Name			
Application	Statistic DB Keep Up Lifetime (day) 30	NODE 0			
Phone Setting	Switch Over by CPU Overload DISABLE	NODE 0			
Announcement	System Loop Back Test DISABLE	NODE 0			
<ul> <li>Miscellaneous</li> </ul>	System Private IP Address For Call none	NODE 0			
Licepse	System Public HTTP Port For Phone Provision 80	NODE 0			
Ductor Time	System Public HTTPS Port For Phone Provision 443	NODE 0			
System Time	System Public IP Address For Admin none NODE 0				
NTP Server	System Public IP Address For Call 162/138063 NODE 0				
DNS Server	System Public IP Address For Phone Provision 1652138063	NODE 0			
System Options	System Span Car Expire Timer (second)	NODE 0			
System Capacity	Upsolicited Notify ENABLE	NODE 0			
System IP Information	WiMAX 111 Interface Enable DISABLE	NODE 0			
System Information	WiMAX U1 Interface IP Address none	NODE 0			
Vendor Dependant	XML Server Data Syncronization Hour ( 0 ~ 23 hour) 03	NODE 0			
SNMP Config	XML Server Prefix Number none	NODE 0			
Internal Proxy Config	Hete         2/2 (131)         >>>>           Detail         Change         Excel         Detach         Close				
System Viewer	Event Viewer				
System: [MINE] scme-vmc-61	Level Type Date/Time Node Name System Name Descr	ription			
Status: [MASTER] Active Alone	STATUS 2013-09-03 16:07/25 NODE 1 Scme-vmc-62 DATABASE BACKUP (	COMPLETE : PATH[/u			
Alarm: CRI(0) MAJ(0) MIN(0)	STATUS 2013-09-03 16:07:29 NODE 1 SOME-VMC-61 DATABASE BACKUP (	SUMPLETE : PATH[/U_			
CPU Memory File	Memory File				
Clear Detach Close					
Message [Search] Completion (Total : 31 / 131) [2013-09-03 17:29:27] 2013-09-03 17:29:39					

## 16 TLS and sRTP configuration

## 16.1 SCM

#### **TLS configuration**

#### **Configure TLS Version**

SCM supports TLS V1.0 and V1.2. You can select one of them. [CONFIGURATION  $\rightarrow$  Miscellaneous  $\rightarrow$  System Option  $\rightarrow$  SIP TLS Version]

#### **Configure TLS Use**

- You can enable TLS of a Single Phone User by setting Protocol to TLS in the [CONFIGURATION > User > Single Phone User] menu.
- You can enable TLS of a Multi-Extension Phone by setting Protocol to TLS in the [CONFIGURATION > User > Multi-Extension Phone] menu.
- You can enable TLS for endpoints by setting Protocol to TLS in the [CONFIGURATION > Trunk Routing > Route] menu.

#### **TLS Certification**

You can be issued from Certificate Authority for SCM, phone, gateway and the issued Certifications should be located specific directory.

- 1) Directory Path /DI/BASE/data/COM
- 2) SCM Certification Type and name format
  - ① root\_caCert.pem: Root CA certification
  - ② caCert.pem: CA certification
  - ③ myCert.pem: PBX certification
  - ④ myPrvKey.pem: PBX private key

When install SCM, the basic three certifications-caCert.pem, myCert.pem, myPrvKey.pem are built-in.

If you get from external Certificate Authority, you must change name to above type. If the private key is encrypted, you enable the option in following menu

# [CONFIGURATION $\rightarrow$ Miscellaneous $\rightarrow$ System Option $\rightarrow$ SIP TLS Private Key Decryption $\rightarrow$ Enable].

To apply new certification, it is necessary to restart SCM.

3) Phone Certification

Phone can download own certification from SCM, if the certification is located in SCM specific directory and Use TLS Certification options is enabled.
[CONFIGURATION > Phone Setting > SIP Options > Use TLS Certification > Enable]

Phone Certification Directory Path /tftpboot/sec\_cert

#### Phone Certification Type and name format

- {MAC}.der.pem: Phone certification
- {MAC}.key.pem: Phone private key
- example: phone's MAC is 00214c9c8eef certification: 00214c9c8eef.der.pem private key: 00214c9c8eef.key.pem

#### SRTP

The media encryption feature provides encryption for the voice data exchanged between the caller and the called party for calls established with signaling encryption. SCM supports media encryption for calls with phones, SCM's built-in conference system, SCM's built-in voice mail system, endpoints, and SCM's built-in MOH system. SCM supports AES and ARIA as media encryption algorithms.

You can enable media encryption for a Single Phone User by setting 'Media' in the **[CONFIGURATION > User > Single Phone User]** menu. You can enable media encryption for a Multi-Extension Phone by setting 'Media' in the **[CONFIGURATION > User > Multi-Extension Phone]** menu.

- RTP: No media encryption.
- sRTP (AES/ARIA128): Encrypts media into the ARIA128 or AES protocol, and uses AES first.
- sRTP (ARIA128/AES): Encrypts media into the ARIA128 or AES protocol, and uses ARIA128 first.
- sRTP (AES/ARIA192): Encrypts media into the ARIA192 or AES protocol, and uses AES first.
- sRTP (ARIA192/AES): Encrypts media into the ARIA192 or AES protocol, and uses ARIA192 first.
- sRTP (AES): Encrypts media into the AES protocol.
- sRTP (ARIA128): Encrypts media into the ARIA128 protocol.
- sRTP (ARIA192): Encrypts media into the ARIA192 protocol.

Media encryption is not used for calls between phones or endpoints enabled with encryption and phones or endpoints not enabled with encryption.

### 16.2 OfficeServ7400

#### **TLS configuration**

#### **Configure TLS Version**

SCM supports TLS V1.0 and V1.2. You can select one of them. [DM 5.2.12 SIP Stack/Ext/Trunk Opionts  $\rightarrow$  SIP Trunk Configuration  $\rightarrow$  TLS Version] select V1.0 or V1.2

**Configure TLS Use** 

[DM 5.2.13 SIP Carrier Options → SIP Signal Type] set to TLS

#### **TLS Certification**

You can be issued from Certificate Authority for SCM, phone, gateway and the issued Certifications should be located specific directory.

- 1) Directory Path Located on SD card /certification/sip
- 2) OS7400 certificate type and name format
  - ① root\_caCert.pem: Root CA certification
  - ② caCert.pem: CA certification
  - ③ myCert.pem: PBX certification
  - ④ myPrvKey.pem: PBX private key

OS7400 package involves the default certificates (rootCaCert.pem, caCert.pem, myCert.pem, myPrvKey.pem)

If you get from external Certificate Authority, you must change name to above type. After changing the certificate, **[DM 5.2.13 SIP Server Enable]** Disable  $\rightarrow$  Enable should be done.

#### SRTP

OS7400 supports AES and ARIA of SRTP encryption algorithm. You can set for this in the DM.

[DM 2.1.5 System Options  $\rightarrow$  sRTP Algorithm] select encryption algorithm [DM 5.2.16 MGI Options  $\rightarrow$  USE sRTP] set to Enable

## 16.3 iBG

#### **TLS configuration**

You need to connect to Ubigate iBG via Console with terminal program. First of all, You must shutdown the voip gateway.

```
iBG# configure terminal
iBG/configure/voip-gateway# shutdown
```

If you have to use certification for TLS, you need to upload certification file to CF card of iBG. After that, set the certification file.

In case of RootCA+CA+EndSystem

```
iBG# configure terminal
iBG/configure# voice service sip tls-option load-3cert r c e k
```

In case of RootCA+EndSystem

```
iBG# configure terminal
iBG/configure# voice service sip tls-option load-cert r e k
```

Change the transport option for TLS, and restart voip gateway.

```
iBG# configure terminal
iBG/configure# voice service sip transport tls
iBG/configure# voip-gateway
iBG/configure/voip-gateway# shutdown
iBG/configure/voip-gateway# no shutdown
```

#### **SRTP configuration**

Select the media type for SRTP configuration. This configuration will affect system globally. It is not possible to configure media type for individual FXS user or trunk. [Gateway > Ubigate Slot Setting > iBG2006/2016/3026] or [Gateway > Ubigate Slot Setting > iBG1003/1004]

User	User Group UG1	Gateway Name gw2006	Gateway Type iBG2006	Country Korea	S1(0/0) FXS-4M	S1(0/0) State FXS-4M	52(0/1) FXO-4M	S2 FXC
Trunk Routing	M (DIALOC)/RC2006/2016/2026	Change						
Time Schedule	S [DIALOG]IBG2000/2010/5020	- Change			1			
Service	User Group	UG1			Gater	way Name	gw2006	
Wireless Enterprise	Gateway Type	IBG2006		·	Locate	ed Country	Korea	
Application	Slot S1(0/0) Configuration	FXS-4M			Slot S	1(0/0) State	F×S-4M	
Application	Slot S2(0/1) Configuration	FXO-4M			Slot S	2(0/1) State	FXO-4M	
Phone Setting	Slot S3(0/2) Configuration	T1E1-2M		<b>v</b>	Slot S	3(0/2) State	T1E1-2M	
Announcement	Slot S4(0/3) Configuration	None			] Slot S4	4(0/3) State		
Miscellaneous	Slot NM1(1) Configuration	None		<b>v</b>	Slot N	M1(1) State		
Gateway	Slot NM2(2) Configuration	None		<b>v</b>	Slot N	M2(2) State		
Gateway Link Set	FAX Relay	T38 Redund	lancy 3		) DTN	IF Relay	Inband	
🖃 Ubigate Slot Setti	Media Type	RTP			] T1/E	1 Select	E1	
iBG2006/2016/3	Use Diversion User Info	Disable			]			
iBG1003/1004				Change Ap	ply Close			

## 17 Interworking mail server

### E-mail Delivery and Notification for VM

SCM can send e-mail for voide message. You can configure your email server in the **[VM/AA > Open Block Table > Mailbox Class > SMTP Server]** 

MClass Block(Standard)	81 10	
Previous Next		Copy Refer
SMTP Server Host ID port SMTP User ID Password Domain	192,168,172,211       25	
Delivery Controls Attempts Retry interval	3	
Message Retention Contro Adjust message retention Message retention to use		

Item	Description		
Host ID	Enter the IP address of the Host Mail Server used by the users assigned this MClass.		
PORT	The default (recommended) port to use is: 25. Most Mail Servers look at port 25 for receiving and sending Mail		
STMP USER ID (OPTIONAL)	This is the User ID the SCME VM will use to log on to the Mail Server and Identify itself as a Client associated with sending Mail (Mail Servers that are on a local LAN and that do not have Public IP addresses often do not require authentication)		
PASSWORD (OPTIONAL)	This is the password associated with the SCME VM's User ID for logging into the Mail Server verifying it is the Client it said it was. (Mail Servers that are on a local LAN and that do not have Public IP addresses often do not require authentication.)		
DOMAIN (OPTIONAL)	The Domain is used as part of the authentication process between the SCME and the Mail server. Based on the Local Domain Name and Domain ID the mail server can validate that it is accepting mail from this Client. (Mail Servers that are ona local LAN and that do not have Public IP addresses often do not require authentication.)		
ATTEMPTS	How many times to do you want the SCME VM to attempt to deliver the E-Mail Message if it fails? The Default value is: 3.		
RETRY INTERVAL	This is how long the SCME VM will wait between failure attempts before trying to deliver the e-mail message again		

ltem	Description
ADJUST MESSAGE	'N' is the default setting. This means SCME VM will leave the original
RETENTION	Save the Voice Message via the Subscriber can than go in and Delete or Save the Voice Message via the telephone interface at any time up to the number of days specified in the Message Retention timer set on page one of the MCLass. 'Y' means the SCME VM will follow the 'Message Retention to use:' value set below in place of the Message Retention set on page one
MESSAGE RETENTION TO USE	Sets the number of days to retain the Voice Message as New after it sends it to the Mail server. A value of '0' means delete the original voice message immediately after it is packed up and sent to the Mail Server. 'Adjust Message Retention:' must be set to 'Y' for this parameter to take effect. The selected range is from 0 to 999

#### **E-mail Notification Setup**

SCM can send e-mail to notify Alarm/Fault/Status information or making conference reservation. You can configure your email server settings in the [**PERFORMANCE** > **Fault** > **E-mail Notification Setup**] menu.

ltem	Description		
SMTP Server: Host ID	IP address or host name of the e-mail server.		
SMTP Server: Port	Port number of the e-mail server		
	- Support SMTP or TLS (Start TLS) only		
	- SMTP usually 25, TLS usually 587		
	* It can be different from e-mail server.		
SMTP Server: Domain	Domain name of the e-mail server (optional)		
Auth Login: User ID,	User ID and password required for user authentication by the e-mail		
Password	server		
	- In case Basic Authentication is set to ON in e-mail server, User ID		
	and Password should be set.		
	- In case Basic Authentication is set to OFF, User ID and Password		
	should not be set. (For SCM Administrator not to try authentication)		
Address: From	Sender's e-mail address		
Address: To	Recipient's e-mail address		
	* It's specified for notifying alarm/fault/status.		
	* You can configure recipient's e-mail address for notifying conference		
	reservation in [Configuration > User > User Profile].		

#### Notifying Alarm/Fault/Status message

The alarm, fault and status information generated in SCM can be notified to the administrator by e-mail. You can set **[E-mail Flag]** to Enable in **[Perfomance > Fault > Setting > Setting-Alarm, Setting-Fault, Setting-Status]** by item.

#### **Notifying Meet Me Conference Reservation**

The invitation letters for Meet Me Conference Reservation can be sent to the members. You can check [Send Invitation letters] in [Conference > Conference Management > Meet Me Reservation].

## **18 Configuration of CDRs**

## 18.1 Configuration of Storage option

The SCM creates and stores CDRs according to the specified configuration at CDR Storage Option in **[CONFIGURATION > User Group > Change User Group > Information]**. There are 7 CDR Storage options as below.

[DIALOG]Information - Change					×
User Group	UG1	-	CDR Storage Options	None	
Host	ug1,scm,com		Authentication Method		
MOH ID	1100	-	MOH Enable	None	
Transfer Ringback Tone	1115	-	User Group Code	ETP	
CLI Number			QOP(Quality of Protection)	RADIUS	
Realm	ug1,scm,com		Algorithm	TCP	
LDAP Root Directory			Restriction Policy	TCP_SMDR	
Default Access Code			Min Digit (Default Access Code		
Service Call Access Code		-	Media Option		•
SRTP Mline offer Option			External Cooperation ID		
Restriction User Group					
		•			
¥ ¥				Se	arch
		Change Ap	ply Close		

#### NONE

The CDRs are not created.

#### Local

The CDRs are stored at the local disk of the SCM. For detailed configuration for 'Local', configure the following item. [MANAGEMENT > CDR Storage Options > Local]

Name	Description			
CDR Local Backup Interval (hour)	When configuring CDR files to be backed up in the hard disk, specify the backup interval. All CDR files generated are moved to the backup directory and the files in the local directory are deleted at this interval. Only the CDR files not saved in the backup directory will be left in the local directory.			
CDR Local Backup Lifetime (day)	When configuring CDR files to be backed up in the hard disk, specify the number of days for which the backed up CDR files will be kept in the hard disk. At midnight everyday, the system automatically deletes any backed up CDR files which have passed the specified date.			
CDR Local Backup Used	Specify whether to back up the generated CDR files in the hard			
Name	Description			
------------------------------------	--	--	--	--
	disk. If enabled, the files are backed up in the /DI/CM/data/cdr/ local/Backup directory.			
CDR Local create Interval (min)	Specify the interval in minutes at which the CDR data files will be generated. New CDR files are generated at this interval. No CDR file will be generated if there is no CDR information for this period. The CDR files generated are saved in the /DI/CM/data/cdr/local directory.			

### FTP

The CDRs are sent to the CDR server via FTP. For detailed configuration for 'FTP', configure the following item [MANAGEMENT > CDR Storage Options > FTP Send]

Attribute	Description
CDR FTP Backup Lifetime (day)	When interoperating with the accounting system over FTP, the CDR files generated can be backed up in SCM even after they have been transferred by FTP. Specify the number of days for which the backed up CDR files will be kept. At midnight everyday, the system automatically deletes any backed up CDR files which have passed the specified date.
CDR FTP Backup Used	When interoperating with the accounting system over FTP, the CDR files generated can be backed up in SCM even after they have been transferred by FTP. If enabled, the CDR files are backed up in the /scm_data/cdr/ftp/Backup directory in SCM.
CDR FTP Create Interval (min)	When interoperating with the accounting system over FTP, specify the interval at which the CDR files are generated. New CDR files are generated at this interval. No CDR file will be generated if there is no CDR information for this period. The CDR files generated are saved in the /DI/CM/data/cdr/ftp directory.
CDR FTP Directory	Specify the name of the directory in the FTP server where the files will be saved when transferring CDR files over FTP.
CDR FTP IP	Specify the IP address of the FTP server when transferring CDR files over FTP.
CDR FTP Login Name	Specify the login name of the FTP server when transferring CDR files over FTP.
CDR FTP Password	Specify the password of the FTP server when transferring CDR files over FTP.
CDR FTP Port	Specify the port number of the FTP server when transferring CDR files over FTP.
CDR FTP Secure	Specify whether to use Secure-FTP when transferring CDR files over FTP.

Attribute	Description
CDR FTP Transfer Interval	When interoperating with the accounting system over FTP,
(min)	specify the interval (in minutes) at which the CDR files are
	transferred. All CDR files generated are transferred over FTP
	and the successfully transferred files are moved to the backup
	directory at this interval. Only the CDR files not transferred over
	FTP will be left in the local directory.

### RADIUS

The CDRs are sent to the CDR server via RADIUS protocol. For detailed configuration for 'RADIUS', configure the following item [MANAGEMENT > CDR Storage Options > RADIUS Send]

Attribute	Description
CDR RADIUS Backup Lifetime (day)	When interoperating with the accounting system over RADIUS and backing up CDR files in SCM, the CDR files generated can be backed up in SCM even after they have been transferred to the RADIUS server. Specify the number of days for which the backed up CDR files will be kept. At midnight everyday, the system automatically deletes any backed up CDR files which have passed the specified date.
CDR RADIUS Backup Used	When interoperating with the accounting system over RADIUS, the CDR files can be backed up in SCM even after they have been transferred to the RADIUS server. If enabled, the CDR files are backed up in the /DI/CM/data/cdr/radius/Backup directory in SCM.
CDR RADIUS Create Interval (hour)	When interoperating with the accounting system over RADIUS and backing up CDR files in SCM, specify the interval (in minutes) at which the CDR files to be backed up are generated. The CDR files generated are moved to the backup directory, the files in the local directory are deleted, and CDR files with new names are generated at this interval. No CDR file will be generated if there is no CDR information for this period. The CDR files generated are saved in the /DI/CM/data/cdr/radius directory. Only the CDR files not saved in the backup directory will be left in this directory.
RADIUS Account Server IP	Specify the IP address of the RADIUS server when interoperating with the accounting system over RADIUS.
RADIUS Account Server Port	Specify the port number of the RADIUS server when interoperating with the accounting system over RADIUS.
RADIUS Account Used	Specify whether the CDR data will be sent to the RADIUS server when interoperating with the accounting system over RADIUS.

### **CDR TCP**

The CDRs are sent to the CDR server via TCP protocol.

For detailed configuration for 'TCP', configure the following item [MANAGEMENT > CDR Storage Options > TCP Send]

Attribute	Description
CDR TCP Backup Lifetime (day)	When interoperating with the accounting system over TCP and backing up CDR files in SCM, the number of days for which the backed up CDR files will be kept in SCM. At midnight everyday, the system automatically deletes any backed up CDR files which have passed the specified date.
CDR TCP Create Interval (min)	When interoperating with the accounting system over TCP and backing up CDR files in SCM, specify the interval (in minutes) at which the CDR files to be backed up are generated. New CDR files are generated at this interval. No CDR file will be generated if there is no CDR information for this period. The CDR files generated are saved in the /DI/CM/data/cdr/tcp directory.
CDR TCP Link1 IP	Specify the IP address of the first of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.
CDR TCP Link1 Used	Specify whether to transfer the CDR data to the first of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.
CDR TCP Link2 IP	Specify the IP address of the second of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.
CDR TCP Link2 Used	Specify whether to transfer the CDR data to the second of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.
CDR TCP Link3 IP	Specify whether to transfer the CDR data to the third of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.
CDR TCP Link3 Used	Specify whether to transfer the CDR data to the third of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.
CDR TCP Link4 IP	Specify the IP address of the fourth of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.
CDR TCP Link4 Used	Specify whether to transfer the CDR data to the fourth of the four TCP servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP.

### TCP\_SMDR

Basically same as TCP options but the data is the format of SMDR. For detailed configuration for 'TCP\_SMDR', configure the following item [MANAGEMENT > CDR Storage Options > Old SMDR Send]

Attribute	Description
SMDR TCP Backup Lifetime (day)	When interoperating with the accounting system over TCP, send SMDR data and backing up CDR files in SCM, the number of days for which the backed up CDR files will be kept in SCM. At midnight everyday, the system automatically deletes any backed up CDR files which have passed the specified date.
SMDR TCP Create Interval (min)	When interoperating with the accounting system over TCP, send SMDR data and backing up CDR files in SCM, specify the interval (in minutes) at which the CDR files to be backed up are generated. New CDR files are generated at this interval. No CDR file will be generated if there is no CDR information for this period. The CDR files generated are saved in the /DI/CM/data/cdr/tcpSMDR directory.
SMDR TCP Link1 IP	Specify the IP address of the first of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.
SMDR TCP Link1 Used	Specify whether to transfer the SMDR data to the first of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.
SMDR TCP Link2 IP	Specify the IP address of the second of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.
SMDR TCP Link2 Used	Specify whether to transfer the SMDR data to the second of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.
SMDR TCP Link3 IP	Specify the IP address of the third of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.
SMDR TCP Link3 Used	Specify whether to transfer the SMDR data to the third of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.
SMDR TCP Link4 IP	Specify the IP address of the fourth of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.
SMDR TCP Link4 Used	Specify whether to transfer the SMDR data to the fourth of the four TCP servers, to which the SMDR data can be transferred when interoperating with the accounting system over TCP.

### TCP\_Ack

Basically same as TCP options but the CDRs are sent to the TCP\_ACK CDR server via proprietary TCP protocol.

For detailed configuration for 'TCP\_ACK', configure the following item [MANAGEMENT > CDR Storage Options > TCPACK Send]

Name	Description
CDR TCP Ack Link1 IP	Specify the IP address of the first of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.
CDR TCP Ack Link1 Used	Specify whether to transfer the CDR data to the first of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.
CDR TCP Ack Link2 IP	Specify the IP address of the second of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.
CDR TCP Ack Link2 Used	Specify whether to transfer the CDR data to the second of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.
CDR TCP Ack Link3 IP	Specify the IP address of the third of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.
CDR TCP Ack Link3 Used	Specify whether to transfer the CDR data to the third of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.
CDR TCP Ack Link4 IP	Specify the IP address of the fourth of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.
CDR TCP Ack Link4 Used	Specify whether to transfer the CDR data to the fourth of the four TCP ACK servers, to which the CDR data can be transferred when interoperating with the accounting system over TCP ACK.

### **Set Billing Output**

This is a function that the CDR data is created by call types. To use this function, you should set the item whose 'use billing output' is 'ENABLE ' in the [MANAGEMENT > CDR Storage Options > CDR Option] menu. And you should set items in the [MANAGEMENT > CDR Storage Options > Set Billing Output] menu.

Name	Description
App Server Call Billing Output [App Server]	The CDR is created if Calling type (4) is application and Called Type is application (4)
App Server Call Billing Output [Service]	The CDR is created if Calling Type (4) is Application and Called Type is Service (2)
App Server Call Billing Output [Subscriber]	The CDR is created if Calling Type (4) is Application and Called Type is Subscriber (1)
All Call Billing Ouput Set	The CDR is created about all calls
Incoming Call Billing Output[Normal]	The CDR is created if the trunk is a normal type and call is a outgoing call
Incoming Call Billing Output[TIE]	The CDR is created if the trunk is a TIE type and is call is a outgoing call
Outgoing Call Billing Output[Normal]	The CDR is created if the trunk is a normal type and call is a incoming call
Outgoing Call Billing Output[TIE]	The CDR is created if the trunk is a TIE type and call is a incoming call
Service Call Billing Output[App Server]	The CDR is created if Calling Type is Service (2) and Called Type is application (4)
Service Call Billing Output[Service]	The CDR is created if Calling Type is Service (2) and Called Type is Service (2)
Service Call Billing Output[Subscriber]	The CDR is created if Calling Type is Service (2) and Called Type is Subscriber (1)
Subscriber Call Billing Output[App Server]	The CDR is created if Calling Type is Service (1) and Called Type is application (4)
Subscriber Call Billing Output[Service]	The CDR is created if Calling Type is Service (1) and Called Type is Service (2)
Subscriber Call Billing Output[Subscriber]	The CDR is created if Calling Type is Subscriber (1) and Called Type is Subscriber (1)

### Length of Bill Delete

This is a function that deletes access code of trunk in the 'connect number' of CDR. To use this function, you should set 'Length of Bill Delete' in the [Configuration > Trunk Routing > Route] menu

### 19 OfficeServ phone upgrade

How to Upgrade the OfficeServ PKG phone to SCME PKG can be divided into upgrade from SCME System and upgrade from the menu on the terminal itself.

### Upgrade method from the terminal menu.

- Excute the HTTP Server or TFTP Server on the PC.
- Enter the IP address of the PC and Upgrade Type from the S/W Upgrade menu of the administrator menu of the terminal and press OK button, then Upgrade will be progressed.

### Upgrade method from SCME System

Uploading SCME PKG of terminal to the SCME system using the SCME Admin .

File Upload	
Phone Image File	i5220S_SCME_V02,44_20130913,tar,gz Search
Phone Info	SMT-i5220S/D Send
	File Upload
	File_Uploads] i5220S_SCME_V02;44_20130913;tar 55%
	4014080 / 7255976
	Cancel
	Detach Close

- PNP Mode Upgrade After terminal is completed booting, upgrade to SCME PKG by referring to the SCME IP information received from the DHCP Server.
- Static IP/DHCP Mode Upgrade
   Enter the necessary information of the terminal IP, Server IP (SCME IP), User ID,
   Password, through easy installation menu of the terminal, and then reboot the terminal.
   It will proceed to upgrade SCME PKG from SCME system.

### 20 Interworking application (SIP, CSTA)

### **CSTA License**

CSTA license defines the capability to use CSTA application. Operators should input CSTA licenses in the [SCM Administrator/CONFIGURATION/Miscellaneous/License] menu to integrate with CSTA applications such as Samsung Operator, Embedded ACD Agent, Communicator, ACD Server, SC Plus and other CSTA Applications.

When an external license key is issued, Samsung Operator, Embedded ACD Agent and Communicator can be set the number of CSTA application channels for the each corresponding entries. But this cannot exceed the number of Total CSTA applications entry. ACD Server and SC Plus do not need licenses. Because SCM provides 10 license for ACD server and SC Plus. Every CSTA applications without previously mentioned uses the channels specified in **[Other CSTA Applications]**.

The number specified in **[Total CSTA Applications]** entry means total available number that can be assigned to CSTA applications. It is including 10 licenses that SCM basically provides for ACD server and SC Plus.

Although only ACD server or SC Plus that does not need to input licenses is used, operator should input External Application License.

[DIALOG]License - Detail			
License Key Type	SCM Express - External Application	License Key	Time: 2011/11/07 14:18:22, Elapsed Time: 8205(hr)
MAC Address		License Status	Using time expired (30days)
Samsung SIP Phones		Samsung Soft Phones	
Samsung Mobile Phones		Samsung PC Attendants	
3rd Party SIP Phones		Analog Phones(Gateway)	
AA Availability(Master/Slave)	<b>_</b>	High Availability(Active/Standby)	<b>_</b>
Meet-Me Conference Channels		UMS Channels	
Total CSTA Applications	60	Samsung Operators	2
Embeded ACD Agent Links	30	Communicators(Desktop)	10
Other CSTA Applications	8	SIP Application Channels	100
FMS Phones		MVS Phones	

### **CSTA Configuration**

As a client, CSTA application makes TCP connection to SCM with SCM IP address and CSTA port.

Each User Group has separate connection with a different CSTA port, which is determined according to the User Group. Therefore, ACD Group/Agent/IVR is controlled depending on the User Group. CSTA port for each user group is shown in the [SCM Administrator/ CONFIGURATION/User Group/Change User Group/Options] menu.

When several SCM is installed in a site, unique CSTA Call Id is available by setting CSTA Node Code in the [SCM Administrator/CONFIGURATION/User Group/Change User Group/Options] menu. Each SCM should have different CSTA Node Code. If just one SCM is installed in a site, CSTA Node Code has no meaning.

[DIALOG]Options - Detail					
User Group	UG1	<b>v</b>	Transfer RingBack Tone	мон	-
Operator Recall	Disable	<b>v</b>	Auto Answer Attention Tone	Bellcore 1	-
Auto Answer Tone Count	0	<b>v</b>	Chain Forwarding	First Callee	
Call Authentication	Disable	<b>v</b>	CSTA Port	6001	
Maximum Call Forward Count	3		Long Duration Call Auto Release	Disable	
Park Announcement ID	1100	<b>v</b>	Wake-Up Announcement ID	1049	
Wake-Up Announcement Iteration	3		Wake-Up No Answer Retry Count	3	
Wake-Up Ring Type	None	<b>v</b>	Callback Ring Type	None	<b>~</b>
Recall Ring Type	None	<b>v</b>	Paging On Answer Ring Type	None	
Dispatch Conf, Ring Type	Siren 1	<b>v</b>	Predefined Conf, Ring Type	Siren 1	-
Line Seize Option	None	<b>v</b>	Transfer Recall	Enable All	-
Application Server Service Group	UG1-APPGRP1	<b>v</b>	Node1's App Server Service Group	UG1-APPGRP2	-
Missed Call by Multi-Device	Display Disable	<b>v</b>	Missed Call by Hunt Answer	Display Disable	-
Missed Call by Multiring Answer	Display Disable	Y	Missed Call for Pickup	Display Disable	-
System Speed Dial Display	Speed Number	<b>v</b>	Transfer Target Display for Recall	Enable Operator Only	-
CSTA Node Code	0				

### **SIP Application License**

SCM License scheme defines SIP application channel capabilities. Operators can insert the external license key issued by a license server using **[SCM Administrator**/

**CONFIGURATION/Miscellaneous/License]** menu. In order to integrate with application servers such as Voice Mail, Recording, Auto Attendant, Conference and External Ringback Tone server, the **[SIP Application Channels]** of External License should be assigned. The **[SIP Application Channels]** defines SIP application channel capabilities.

Each application needs to set SIP channels in each application menu. The number of each application license cannot exceed the total number of SIP application channel capacity. Total SIP application channels are be shown as below.

😻 [DIALOG]License - Detail				_ <b>_</b> X
License Key Type	SCM Express - External Application	-	License Key	-3HUYJTZ3-02WQX6R4-SH90OSBQ-7QYXALMT
MAC Address	000C2958BD9E		License Status	ОК
Samsung SIP Phones			Samsung Soft Phones	
Samsung Mobile Phones			Samsung PC Attendants	
3rd Party SIP Phones			Analog Phones(Gateway)	
AA Availability(Master/Slave)		-	High Availability(Active/Standby)	<b></b>
Meet-Me Conference Channels			UMS Channels	
Total CSTA Applications	50		Samsung Operators	
Embeded ACD Agent Links	10		Communicators(Desktop)	10
Other CSTA Applications			SIP Application Channels	10
FMS Phones			MVS Phones	

### **Creating Application Server**

Create Application Server
 [CONFIGURATION > Application]

CONFIGURATION					
🗄 Location 🖉					
🗄 User Group	I				
🕀 User	I				
∃ Trunk Routing	I				
🗄 Time Schedule	I				
🕀 Wireless Enterprise					
Application	I				
⊞ ACD	I				
VM/AA Server	I				
Conference Server	I				
Messenger Server	I				
Other Application Server					
Application Server Group					
⊕ Phone Setting					

2) Create Application Server Group
 When creating Server Group, Each Service must be set by Application Server.
 [CONFIGURATION > Application > Application Server Group]

🔊 [DIALOG]Application Server Group - Change					
User Group	UG1	-	Name	UG1-APPGRP1	<b>v</b>
Voice Mail Server	UG1,UMS	-	Call Recording Server	UG1,UMS	<b>~</b>
Paging Conference Server	UG1,CONF	▼	Meet-Me Conference Server	UG1,CONF	<b>T</b>
One-Step Conference Server	UG1,CONF	-	Add-On Conference Server	UG1,CONF	-
External Ringback Tone Server		-	Gateway MOH Server		-
Change Apply Close					

3) Set Application Server Group to User Group, Service Group, User [CONFIGURATION > User Group > Change User > Options]

[DIALOG] Options - Change		Care of the Advantage			
User Group	UG1	-	Transfer RingBack Tone	мон	-
Operator Recall	Disable	-	Auto Answer Attention Tone	Bellcore 1	-
Auto Answer Tone Count	0	-	Chain Forwarding	First Callee	
Call Authentication	Disable	-	CSTA Port	6001	
Maximum Call Forward Count	3		Long Duration Call Auto Release	Disable	-
Park Announcement ID	1100	-	Wake-Up Announcement ID	1049	-
Wake-Up Announcement Iteration	3		Wake-Up No Answer Retry Count	3	
Wake-Up Ring Type	None	-	Callback Ring Type	None	<b>•</b>
Recall Ring Type	None	-	Paging On Answer Ring Type	None	-
Dispatch Conf, Ring Type	Siren 1	-	Predefined Conf, Ring Type	Siren 1	-
Line Seize Option	None	-	Transfer Recall	Enable All	
Application Server Service Group	UG1-APPGRP1		Node1 App Server Service Group		
Missed Call by Multi-Device	Display Disable	-	Missed Call by Hunt Answer	Display Disable	<b>~</b>
Missed Call by Multiring Answer	Display Disable	-	Missed Call for Pickup	Display Disable	-
System Speed Dial Display	Speed Number	-	Transfer Target Display for Recall	Enable Operator Only	-
CSTA Node Code	0		No Ring for Multi-Device	Disable	-
Minimum Number Translation Length	10		Hunt Group Member Service	Disable	-
Smart Routing Service	Enable	-	Use Default Access Code Use List	No	-
Change Apply Close					

### [CONFIGURATION > User Group > Service Group]

IDIALOG]Service Group - Change			
User Group	UG1 💌	Name	UG1-SG1
Service Group Code		CLI Number	
Class of Service	v	Restriction Policy	Image:
Dial Tone	<b></b>	Dial Plan	
Application Server Service Group	<b>•</b>	Node1 App Server Service Group	
Call Recording Method	Conference Recording	Auto Attendant Ring Plan Schedule	
CFUR Service Schedule			
	Change Ap	ply Close	

[CONFIGURATION > User > Single Phone User]

User Group	UG1	<b>v</b>	Service Group	UG1-SG1	
Location	UG1-LOC1	-	Extension Number	2001	
Application User ID	2001@ug1,scm,com		Extension Name	2001	
Application Password	*****		PIN Number	****	
Authentication User ID	2001		Phone Verification	None	
Authentication Password	****		MAC Address		
IP Address	10,251,191,164		Private IP Address	10,251,191,164	
Profile Login ID	UG12001		Phone Type	Samsung-Desktop-Phone	
Profile Login Passcode	****		Language	Korean	
Mobile Phone Number			Use Mobile Phone Number	None	
Protocol	UDP		Media	RTP	
TLS Connection	Reuse	<b></b>	Ping Ring Type	None	
A-A Primary Node	NODE 0	-	A-A Dual Registration	Enable	
VMS Extension Number			Make Mailbox	Yes	
URI Type	SIP	<b>_</b>	DTMF	RFC2833	
RFC2833 DTMF Payload	101		Time Zone	GMT +09:00 Asia/Seoul	
Department		<b>_</b>	Position		
Send CLI Number			Service Group Local CLI Number		
Service Group Local Number			Restriction Policy		
Class of Service		-	Gateway Name		
Extension Lock	None	<b>_</b>	LDAP DN Number		
Account Code Use		-	Auto Answer by Click to Dial	Enable	
Accept Login Override	Disable	-	External Ringback Tone Use	None	
MOH Announcement ID		-	Display Option	Normal	
Send CLI Name			Call Monitoring	Disable	
Send Extension Number			Use Virtual Ringback	Disable	
Caller Ring Type	None	-	Off Hook Alarm		
Check Registration Protocol	Disable	-	MOH SIP Media Mode	Send Only	
pplication Server Service Group		-	CMS Monitoring	Disable	

# ABBREVIATION

#### Α AA Auto Attendant AAR Automatic Alternative Routing ACD Automatic Call Distribution AR Alternative Route B BHCA **Busy Hour Call Attempt** BLF **Busy Lamp Field** С CAC Call Admission Control CDR Call Detailed Record CLI Calling Line Identification CLIR Calling Line Identification Restriction COS **Class of Service** CPS Call Per Second Computer Supported Telephony Application CSTA **Computer Telephony Interface** CTI D DID **Direct Inward Dial** DISA **Direct Inward System Access** DN **Directory Number** DND Do Not Disturb DOD **Direct Outward Dial** DR **Direct Route** DTMF **Dual Tone Multi-Frequency** F

Fixed Mobile Convergence

© SAMSUNG Electronics Co., Ltd.

FMC

I		
	ITSP IVR	Internet Telephony Service Provider Interactive Voice Response
L	LDAP	Lightweight Directory Access Protocol
М		
	MCS MOH	Multimedia Conference System Music On Hold
	MWI	Message Waiting Indication
Ν		
	NMS	Network Management System
Ρ		
	PBX PSTN	Private Branch eXchange Public Switched Telephone Network
R		
	RADIUS RFC RTP	Remote Authentication Dial In User Service Request For Comments Realtime Transport Protocol
S		
	SBC SCM SIP SNMP	Session Border Controller Samsung Communication Manager Session Initiation Protocol Simple Network Management Protocol
т		
	TLS	Transport Layer Security
U		
	UMS	Unified Messaging System
V		
	VMS VoIP	Voice Mailing System Voice over IP

## W

WE

Wireless Enterprise

### scm Quick Installation Guide

©2013 Samsung Electronics Co., Ltd.

All rights reserved.

Information in this manual is proprietary to SAMSUNG Electronics Co., Ltd.

No information contained here may be copied, translated, transcribed or duplicated by any form without the prior written consent of SAMSUNG.

Information in this manual is subject to change without notice.

