



## **Avaya Solution & Interoperability Test Lab**

---

# **Interoperability Application Note for Avaya Aura<sup>®</sup> Session Manager R6.1 and Avaya Aura<sup>®</sup> Communication Manager R6.0.1 with Siemens HiPath 4000 IP Communication Solution via SIP Trunk connection – Issue 1.0**

## **Abstract**

These Application Notes present a sample configuration for Siemens HiPath 4000 to interoperate with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Session Manager. The Siemens HiPath 4000 is an IP based communications solution that also supports traditional circuit-switched communications. The Avaya Aura<sup>®</sup> Session Manager links to the Siemens HiPath 4000 via SIP trunk. The compliance testing focused on basic call and supplementary call feature support between Siemens and Avaya telephony environments.

# Table of Contents

Table of Contents .....	2
1. Introduction.....	3
2. Equipment and Software Validated .....	4
3. Configure Avaya Aura® Communication Manager .....	5
3.1. Verify Avaya Aura® Communication Manager License.....	6
3.2. Administer System Parameter Features .....	7
3.3. Administer IP Node Names.....	7
3.4. Administer IP Network Region and Codec Set.....	8
3.5. Create SIP Signaling Group and Trunk Group .....	10
3.6. Administer Route Pattern .....	13
3.7. Administer Private Numbering .....	13
3.8. Administer Locations .....	14
3.9. Administer Dial Plan and AAR Analysis.....	14
3.10. Create Stations.....	15
3.11. Save Changes.....	16
4. Configure Avaya Aura® Session Manager .....	17
4.1. Log in to Avaya Aura® Session Manager .....	17
4.2. Administer SIP Domain .....	18
4.3. Administer Locations .....	19
4.4. Administer Adaptations.....	21
4.5. Administer SIP Entities.....	22
4.6. Administer SIP Entity Link.....	26
4.7. Administer Time Ranges.....	28
4.8. Administer Routing Policy .....	29
4.9. Administer Dial Pattern.....	31
4.10. Administer Avaya Aura® Session Manager .....	34
4.11. Add Avaya Aura® Communication Manager as an Evolution Server .....	35
4.12. Administer SIP Users .....	40
5. Configure the Siemens HiPath 4000.....	44
5.1. Client PC Preparation.....	44
5.2. HiPath 4000 System Configuration.....	51
5.3. HG 3500 Gateway Configuration .....	61
6. Verification Steps.....	67
6.1. Verify Network Connectivity .....	67
6.2. Verify Avaya Phones .....	68
6.3. Verify Siemens Phones .....	70
6.4. Verify SIP Trunk between Avaya Aura® Session Manager and HiPath SIP Gateway. ....	70
7. Conclusion .....	71
7.1. Issues detected on all Siemens Endpoints.....	71
7.2. Issues detected on Siemens 420S SIP Phone only .....	72
8. Additional References.....	73

The purpose of this interoperability Application Notes is to validate Siemens HiPath 4000 with Avaya Aura® Communication (CM) Evolution Server which are both connected to an Avaya Aura® Session Manager via a separate SIP trunk. A SIP trunk was configured between Avaya Aura® System Manager and Siemens HiPath 4000, and specifically a SIP Entity Link between Avaya Aura® Session Manager and the Siemens HG 3500 SIP Gateway. The Siemens HiPath 4000 Communications Server is the central controlling unit in the Siemens PBX environment. Both H.323 and SIP gateways are linked to Siemens HiPath 4000 via direct ISDN lines and LTU1 and LTU2, detailed in the diagram below. Testing was focused on basic calls and supplementary call feature support between the Avaya and Siemens PBX environments. Testing endpoints included H.323, SIP and TDM; however fax and EC500 test cases were not included.



## 2. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Media Server	Avaya Aura® Communication Manager R6.0.1
Avaya S8800 Media Server	Avaya Aura® System Manager R6.1 6.1.2.0.612004
Avaya S8800 Media Server	Avaya Aura® Session Manager R6.1 6.1.2.0.612004R1.1 (1.1.6.0.113002)
Avaya G650 Media Gateway	TN2312BP HW15FW049 TN2602AP HW08FW049 TN799DP HW01 FW034
Avaya Handset 2420	(Digital) :Firmware : V6.0
Avaya Handset 9650	(H323) Firmware:V3.110b
Avaya Handset 9621G	(9620SIP)Firmware: V6.0
Avaya 1140E (as 9630SIP)	(9630SIP) Firmware : V04.00.04.00
Siemens HiPath 4000	Siemens HiPath 4000 V5 R0.5.28
Siemens SIP Gateway HG3500	L0-T2R.51.000-004 / pzksti40.26.000-004
Siemens SIP RegistrarHG3500	L0-T2R.51.000-004 / pzksti40.26.000-004
Siemens H.323 Gateway HG3500	L0-T2R.51.000-004 / pzksti40.26.000-004
Siemens OptiPoint 500	Firmware: MP02.04
Siemens OpenStage 15T	Firmware; V1 R0.23.0
Siemens OptiPoint 410 Std	Firmware: V5 R6.1.0
Siemens OptiPoint 420Std	Firmware: V5 R6.3.0
Siemens OptiPoint 420 Std S	Firmware: V7 R5.7.0
Siemens OptiPoint OpenStage 20 S	Firmware: V2 R1.21.0
HiPath Expressions Voicemail	V6.01.0.4978

### 3. Configure Avaya Aura® Communication Manager

This section provides details on the configuration of Avaya Aura® Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). This section provides the procedures for configuring Communication Manager on the following areas:

- Verify Avaya Aura® Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec Set
- Administer Signaling Group and Trunk Groups
- Administer Route Pattern
- Administer Private Numbering
- Administer Locations
- Administer Dial Plan and AAR Analysis
- Create Stations
- Saves Changes

The following assumptions have been made as part of this document:

- It is assumed that Communication Manager, System Manager and Session Manager have been installed, configured, licensed. Refer to **Section 8** for documentation regarding these procedures
- Throughout this section, the administration of Communication Manager is performed using a System Access Terminal (SAT). The commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity.
- The user has experience of administering the Avaya system via both SAT and Web Based Management systems.

### 3.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameter customer options** command to compare the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

**Note:** The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

<b>display system-parameters customer-options</b>		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		<b>USED</b>		
Maximum Administered H.323 Trunks:		12000	0	
Maximum Concurrently Registered IP Stations:		18000	1	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		414	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		18000	0	
Maximum Video Capable IP Softphones:		18000	0	
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>10</b>	
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	
Maximum TN2501 VAL Boards:		128	0	
Maximum Media Gateway VAL Sources:		250	0	
Maximum TN2602 Boards with 80 VoIP Channels:		128	0	
Maximum TN2602 Boards with 320 VoIP Channels:		128	1	
Maximum Number of Expanded Meet-me Conference Ports:		300	0	

## 3.2. Administer System Parameter Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from /to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable trunk-to-trunk transfer on a system wide basis.

```
change system-parameters features                               Page 1 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS
                        Self Station Display Enabled? y
                        Trunk-to-Trunk Transfer: all
                        Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
                        Call Park Timeout Interval (minutes): 10
                        Off-Premises Tone Detect Timeout Interval (seconds): 20
                        AAR/ARS Dial Tone Required? y

                        Music (or Silence) on Transferred Trunk Calls? no
                        DID/Tie/ISDN/SIP Intercept Treatment: attd
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                        Automatic Circuit Assurance (ACA) Enabled? n
```

## 3.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for Communication Manager and Session Manager that will be used for connectivity. In the sample network, **clan** and **192.168.81.104** are entered as **Name** and **IP Address** for the CLAN card in Communication Manager running on the Avaya S8800 Server. In addition, **sm100b** and **192.168.81.121** are entered for Session Manager.

```
change node-names ip                                           Page 1 of 2
                        IP NODE NAMES
                        Name      IP Address
clan                    192.168.81.104
default                0.0.0.0
gateway                192.168.81.254
medpro                 192.168.81.105
procr                  192.168.81.102
procr6                 ::
sm100b                 192.168.81.121
```

### 3.4. Administer IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number, to configure the network region being used. In the sample network, ip-network-region 1 is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: mmsil.local
        Name: To ASM61
MEDIA PARAMETERS
    Codec Set: 1
    Intra-region IP-IP Direct Audio: yes
    Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048
    UDP Port Max: 65535
    IP Audio Hairpinning? y
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5
H.323 IP ENDPOINTS
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5
                                                                AUDIO RESOURCE RESERVATION PARAMETERS
                                                                RSVP Enabled? n
```



Use the **change ip-codec-set n** command to configure IP Codec Set parameters where **n** is the IP Codec Set number. In these Application Notes, **IP Codec Set 1** was used as the main default codec set. The standard G.711 codecs and Siemens default G729A codec were selected.

- **Audio Codec** Set for **G.711MU, G.711A, G729** and **G.729A**
- **Silence Suppression:** Retain the default value **n**
- **Frames Per Pkt:** Enter **2**
- **Packet Size (ms):** Enter **20**

Retain the default values for the remaining fields, and submit these changes.

add ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
	<b>Audio</b>	<b>Silence</b>	<b>Frames</b>	<b>Packet</b>		
	<b>Codec</b>	<b>Suppression</b>	<b>Per Pkt</b>	<b>Size(ms)</b>		
1:	G.711A	n	2	20		
2:	G.711MU	n	2	20		
3:	G.729	n	2	20		
4:	G.729A	n	2	20		

## 3.5. Create SIP Signaling Group and Trunk Group

### 3.5.1. SIP Signaling Group

In the test configuration, Communications Manager acts as an Evolution Server. An IMS enabled SIP trunk is not required. The example uses signal group 150 in conjunction with Trunk Group 150 to reach the Session Manager. Use the **add signaling-group n** command where **n** is the signaling group number being added to the system. Use the values defined in **Sections 3.3** and **3.4** for the **Near-end Node name**, **Far-end Node name** and **Far-end Network Region**. The **Far-end Domain** is left blank so that the signaling accepts any authoritative domain. Set **IMS enabled** to **n** and **Peer Detection Enabled** to **y**. Set **Direct IP-IP Audio Connections** to **y** so trunk “shuffling” is on.

add signaling-group 150		Page 1 of 1
SIGNALING GROUP		
Group Number: 150	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: clan	Far-end Node Name: sm100b	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

### 3.5.2. SIP Trunk Group

Use the command **add trunk-group n** to add a corresponding trunk group, where **n** is the trunk group number.

- **Group Number** Set from the **add-trunk-group n** command
- **Group Type** Set as **sip**
- **COR** Set Class of Restriction (default 1)
- **TN** Set Tenant Number (default 1)
- **TAC** Choose integer value, usually set the same as the Trunk Group number
- **Group Name** Choose an appropriate name
- **Outgoing Display** Set to **y**
- **Service Type** Set to **tie**
- **Signaling Group** Enter the corresponding Signaling group number
- **Number of Members** Enter the number of members

```
add trunk-group 150                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 150                                     Group Type: sip          CDR Reports: y
  Group Name: sip tg 150                               COR: 1                 TN: 1                 TAC: 150
    Direction: two-way                                Outgoing Display? y
    Dial Access? n                                     Night Service:
    Queue Length: 0
    Service Type: tie                                  Auth Code? n
                                                    Member Assignment Method: auto
                                                    Signaling Group: 150
                                                    Number of Members: 10
```

Navigate to **Page 3** and set **Numbering Format** to **private**.

```
add trunk-group 150                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none
                                                    Maintenance Tests? y

                                     Numbering Format: private
                                                    UI Treatment: service-provider
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n

                                     Modify Tandem Calling Number: no
    Show ANSWERED BY on Display? y
```

Navigate to **Page 4** and enter **97** for the **Telephone Event Payload Type** and **P-Asserted-Identity** for **Identity for Calling Party Display**.

display trunk-group 150	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? y	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
<b>Telephone Event Payload Type: 97</b>	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
<b>Identity for Calling Party Display: P-Asserted-Identity</b>	
Enable Q-SIP? n	

### 3.6. Administer Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the **change route-pattern n** command, where **n** is the route pattern number specified in **Section 3.9**. Configure this route pattern to route calls to **trunk group 150**, as configured in **Section 3.5.2**. Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern, Assign **0** to **No. Del Digits**.

change route-pattern 150										Page	1 of	3
Pattern Number: 150 Pattern Name: To SessMan												
SCCAN? n Secure SIP? n												
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted		DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits		QSIG			
										Intw		
1:	150	0						0	n	user		
2:									n	user		
3:									n	user		
4:									n	user		
5:									n	user		
6:									n	user		
BCC VALUE		TSC	CA-TSC	ITC		BCIE	Service/Feature	PARM	No.	Numbering	LAR	
0 1 2 M 4 W			Request						Dgts	Format		
										Subaddress		
1:	y	y	y	y	y	n	n	unre			none	
2:	y	y	y	y	y	n	n	rest			none	
3:	y	y	y	y	y	n	n	rest			none	
4:	y	y	y	y	y	n	n	rest			none	
5:	y	y	y	y	y	n	n	rest			none	
6:	y	y	y	y	y	n	n	rest			none	

### 3.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling part number to be sent out through the SIP trunk. In the sample network configuration, all calls originating from a **5** digit extension beginning with **23** will result in a **5**-digit calling number. The calling party number will be in the SIP "From" header.

change private-numbering 0										Page	1 of	2
NUMBERING - PRIVATE FORMAT												
Ext	Ext	Trk		Private		Total						
Len	Code	Grp(s)		Prefix		Len						
5	23	150				5	Total Administered: 1					
							Maximum Entries: 540					

### 3.8. Administer Locations

Use the **change locations** command to define the proxy route to use for outgoing calls. In the sample network, the proxy route will be the trunk group defined in **Section 3.5.2**.

change locations					Page 1 of 1	
LOCATIONS						
ARS Prefix 1 Required For 10-Digit NANP Calls? y						
Loc	Name	Timezone	Rule	NPA	Proxy	Sel
No		Offset			Rte	Pat
1:	Main	+ 00:00	0			150

### 3.9. Administer Dial Plan and AAR Analysis

Configure the dial plan for dialing 6-digit extensions beginning with **81** to stations registered with the Siemens. Use the **change dialplan analysis** command to define Dialed String 81 as an **aar** Call Type.

display dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 1			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	3	dac							
230	5	ext							
231	5	ext							
232	5	ext							
233	5	ext							
81	6	aar							
*	2	fac							

Use the **change aar analysis 0** command to configure an **aar** entry for **Dialed String 81** to use **Route Pattern 150**. Add an entry for the SIP phone extensions which begin with **230 or 231**. Use **unku** for call type.

change aar analysis 0						Page	1 of	2
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 1		
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
230		5	5	150	unku		n	
231		5	5	150	unku		n	
3		7	7	999	aar		n	
4		7	7	999	aar		n	
5		7	7	999	aar		n	
6		7	7	999	aar		n	
7		7	7	999	aar		n	
81		6	6	150	unku		n	
9		7	7	999	aar		n	

### 3.10. Create Stations

Create Avaya H.323, SIP and TDM Stations using the command **add station n**, where **n** is the Station extension number.

- **Type** Choose phone type e.g. **9620, 9650, 2420**
- **Name** Choose a suitable name
- **Port** Auto assigned for IP Stations, manually set for TDM Stations
- **Security Code** Set Security Code

#### Example of Avaya H323 Station.

add station 23100		Page	1 of	5
STATION				
Extension: 23100	Lock Messages? n	BCC: 0		
<b>Type: 9650</b>	<b>Security Code: 1234</b>	TN: 1		
<b>Port: S00000</b>	Coverage Path 1:	COR: 1		
<b>Name: AVAYA_H323</b>	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 23100			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english	Button Modules: 0			
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? n			
	IP Video? n			
	Short/Prefixed Registration Allowed: default			
	Customizable Labels? y			

#### Example of Avaya TDM Station.

add station 23000		Page	1 of	5
STATION				
Extension: 23000	Lock Messages? n	BCC: 0		
<b>Type: 2420</b>	<b>Security Code: 1234</b>	TN: 1		
<b>Port: 01A0401</b>	Coverage Path 1:	COR: 1		
<b>Name: Digital Phone</b>	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 2	Personalized Ringing Pattern: 1			
Data Option: none	Message Lamp Ext: 23000			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english	Expansion Module? n			
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? n			
	Remote Office Phone? n			
	IP Video? n			
	Customizable Labels? y			

### Example of Avaya SIP Station.

add station 23200		Page	1 of	6
STATION				
Extension: 23200	Lock Messages? n	BCC: 0		
<b>Type: 9620SIP</b>	<b>Security Code:</b>	TN: 1		
<b>Port: S00001</b>	Coverage Path 1:	COR: 1		
<b>Name: Phone, SIP</b>	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19				
	Message Lamp Ext: 23200			
Display Language: english				
Survivable COR: internal				
Survivable Trunk Dest? y	IP SoftPhone? n			
	IP Video? n			

### Example of Avaya 1140E SIP Station

add station 23300		Page	1 of	6
STATION				
Extension: 23300	Lock Messages? n	BCC: 0		
Type: <b>9630SIP</b>	<b>Security Code:</b>	TN: 1		
Port: <b>S00004</b>	Coverage Path 1:	COR: 1		
Name: <b>NORTEL Phone</b>	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19				
	Message Lamp Ext: 23300			
Display Language: english	Button Modules: 0			
Survivable COR: internal				
Survivable Trunk Dest? y	IP SoftPhone? n			
	IP Video? n			

## 3.11. Save Changes

Use the save translation command to save all changes.

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
<b>Success</b>	<b>0</b>



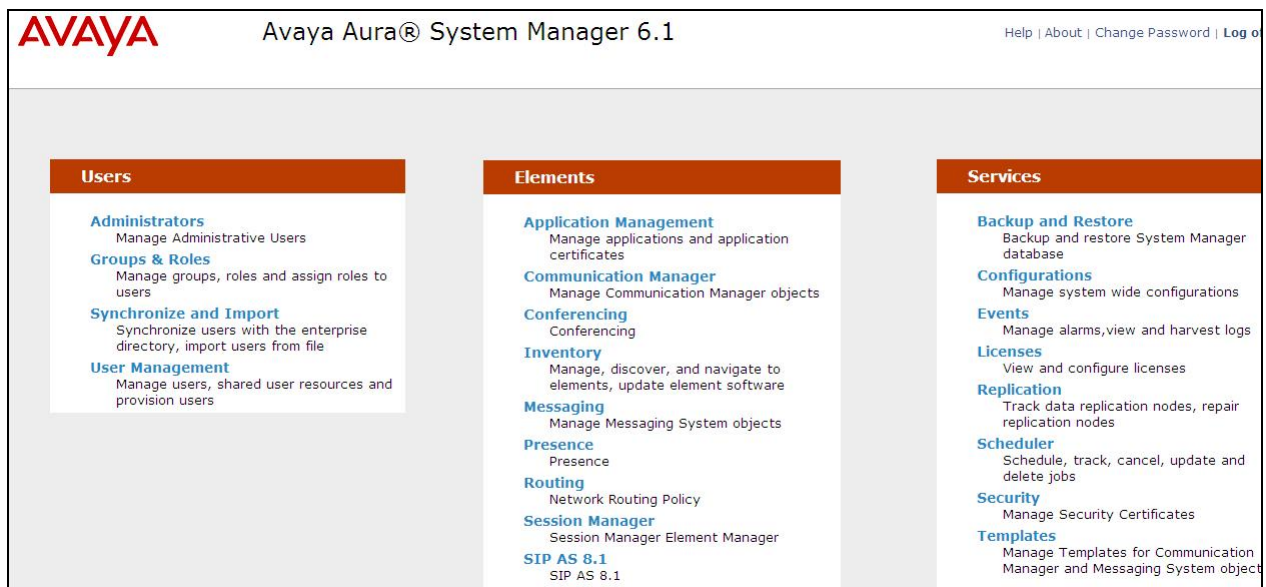
## 4. Configure Avaya Aura® Session Manager

This section provides the procedure for configuring Session Manager. For further reference documents, refer to **Section 8** of this document. The procedures include the following areas:

- Login to Avaya Aura® Session Manager
- Administer SIP Domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Session Manager
- Add Avaya Aura® Communications Manager as an Evolution Server.
- Administer SIP Users

### 4.1. Log in to Avaya Aura® Session Manager

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR** where **<ip-address>** is the IP address of System Manager.



The Home screen is divided into three sections with hyperlinked categories below.

## 4.2. Administer SIP Domain

SIP domains are created as part of the Avaya Aura® System Manager (ASM) basic configuration. There will be at least one which the ASM is the authoritative SIP controller. In these sample notes it is **mmsil.local**. The ASM can also deal with traffic from other domains, so multiple SIP domain entries may be listed.

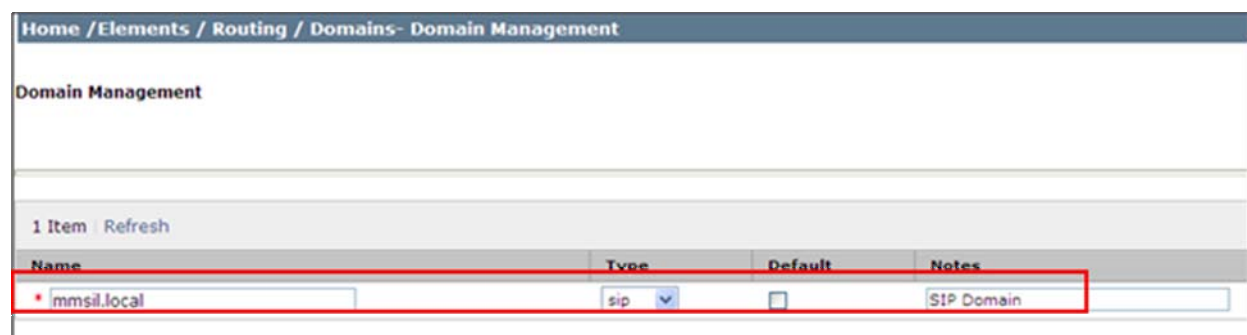


The location of where you are currently in the system is listed at the top of the screen Underneath will be listed the domain(s) available in the system.

To create a new SIP Domain, from the **Home** (first screen available upon successful logon) select the following; **Home → Elements → Routing → Domains → Domain Management** and click **New**.

- **Name** Add a descriptive name,
- **Type** Set to **SIP**
- **Notes**, Add a brief description in the **Notes** field.

Click **Commit** to save (button not shown).



Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are any dial patterns administered for specific locations. Locations are also used to limit the number of calls coming out of or going into a physical locations. This is useful for those locations where the network bandwidth is limited. For this sample configuration, one **Location** has been created which will reference the both the ASM location and the Siemens HiPath location. Navigate to **Home → Elements → Routing → Locations**. To create a new Location, click **New**.

- **Name** Add a descriptive name.
- **Notes** add a brief description.

General

\* Name: Galway

Notes: Galway Lab Siemens\_Avaya

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

\* Default Audio Bandwidth: 80 Kbit/sec

Continue scrolling down the screen until **Location Pattern** is displayed as shown below. In the **Location Pattern** section, under **IP Address Pattern** enter ip addresses used to logically identify the location(s). Under **Notes** add a brief description. Click **Commit** to save.

**Location Pattern**

3 Items | [Refresh](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*X.X.99.*	IP Phone addresses
<input type="checkbox"/>	*X.X.81.*	LabEnv_IP Addresses.*
<input type="checkbox"/>	*X.X.9.*	Lab_DNS

Select : All, None

In the example above, ip addresses have been entered with a (\*) wildcard to indicate a range.

## 4.4. Administer Adaptations

Adaptations are used to manipulate digits in the SIP URI strings of incoming and outgoing calls. For this sample configuration, an Adaptation was created for calls to and from the Siemens HiPath PBX. Any calls from the Siemens HiPath PBX will have the leading digit **6** removed from the destination SIP URI, before that are routed to destination. Any calls going to Siemens HiPath PBX, with leading digits **23**, will have **6** appended to the start. This was configured to match dial out from Siemens.

The screenshot shows the 'Adaptations' configuration page. On the left is a navigation menu with options: Routing, Domains, Locations, Adaptations (selected), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail: Home / Elements / Routing / Adaptations- Adaptations. Below this is a table of adaptations. There is one item listed: 'SiemensHiPath4K' with module name 'DigitConversionAdapter'. Above the table are buttons for Edit, New, Duplicate, Delete, and More Actions. Below the table is a 'Select : All, None' option.

Name	Module name
SiemensHiPath4K	DigitConversionAdapter

To create new Adaptation, browse to **Home→Elements→Routing→Adaptations**. Click **New**. In the **General** section, under **Adaptation Name** add a descriptive name. Select the **Module name** from the drop down list, **DigitConversionAdapter**. Add the **Digit Conversion** as required, for the incoming and outgoing calls. Click **Commit** to save.

The screenshot shows the 'General' configuration page for an adaptation. It includes fields for 'Adaptation name' (SiemensHiPath4K), 'Module name' (DigitConversionAdapter), 'Module parameter', 'Egress URI Parameters', and 'Notes'. Below these are two sections for digit conversion: 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM'. Each section has an 'Add' and 'Remove' button and a table of conversion rules. The 'Incoming Calls' table has one rule: Matching Pattern \*6, Min \*6, Max \*6, Delete Digits \*1, Address to modify destination, Notes remove 6 from incoming no. The 'Outgoing Calls' table has one rule: Matching Pattern \*2, Min \*5, Max \*5, Delete Digits \*0, Insert Digits 6, Address to modify origination, Notes insert 6 to outgoing no.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
*6	*6	*6		*1		destination	remove 6 from incoming no.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
*2	*5	*5		*0	6	origination	insert 6 to outgoing no.

In the example above, Siemens will dial 6-2XXXX, where 2XXXX is the extension number on Avaya. Conversely, the identity of the Avaya extension will have 6 inserted in front of its identity as it dials an extension on the Siemens and this will be presented on the Siemens display.

## 4.5. Administer SIP Entities

Each SIP device (other than Avaya SIP Phones) that communicates with the ASM requires a SIP Entity configuration. This section details the steps to create SIP Entities for the Siemens HiPath SIP Gateway, Session Manager and Communication Manager Evolution Server.

Home / Elements / Routing / SIP Entities- SIP Entities			
<b>SIP Entities</b>			
<div>EditNewDuplicateDeleteMore Actions ▾</div>			
3 Items   Refresh			
<input type="checkbox"/>	Name	FQDN or IP Address	Type
<input type="checkbox"/>	<a href="#">CM EvolutionServer</a>	192.168.81.104	CM
<input type="checkbox"/>	<a href="#">Session Manager</a>	192.168.81.121	Session Manager
<input type="checkbox"/>	<a href="#">SiemensHipath</a>	192.168.81.6	SIP Trunk

To create a SIP Entity for the **Siemens HiPath**, browse to **Home → Elements → Routing → SIP Entities** and click **New**.

### SIP Entity Details

#### General

\* Name:

SiemensHipath

\* FQDN or IP Address:

192.168.81.6

Type:

SIP Trunk

Notes:

SiemensHipathentity

Adaptation:

SiemensHiPath4K

Location:

Galway

Time Zone:

Etc/GMT

Override Port & Transport with DNS SRV:

☐

\* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

egress

#### SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

In the **General** section,

- **Name** add a descriptive name
- **FQDN or IP Address** add the IP Address of the target entity (Siemens SIP Gateway card)
- **Type**, select **SIP Trunk**
- **Notes** add a brief description
- **Adaptation**, click on the drop down arrow and select **SiemensHiPath** (created in **Section 4.4**)
- **Location**, click on the drop down arrow select **SiemensHiPath**. (created in **Section 4.3**)
- **Time Zone** Select the appropriate **Time Zone**
- **SIP Link Monitoring** Set to **Use Session Manager Configuration**

Click **Commit** to save. A message will appear advising that “**Entity Links** can be added to the record once the Entity has been saved”. **Section 4.6** advises how to create Entity Links. To create a **SIP Entity** for the **Session Manager** and **Communications Manager**, repeat the above process. Screenshots are on the next page showing sample data for creating SIP Entities for Session Manager and CM Evolution Server.

Screen shot for Session Manager SIP entity. Change the **Type** to **Session Manager** when programming the **SIP Entity** for **Session Manager**.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. The page is divided into two main sections: 'General' and 'SIP Link Monitoring'. In the 'General' section, a red box highlights the 'Name' field (set to 'Session Manager'), the 'FQDN or IP Address' field (set to '192.168.81.121'), the 'Type' dropdown menu (set to 'Session Manager'), and the 'Notes' field (containing 'entity for Avaya Sess Manager (8'). Below these, the 'Location' dropdown is set to 'Galway', 'Outbound Proxy' is empty, 'Time Zone' is set to 'Etc/GMT', and 'Credential name' is empty. In the 'SIP Link Monitoring' section, a red box highlights the 'SIP Link Monitoring' dropdown menu, which is set to 'Use Session Manager Configuration'.

Home / Elements / Routing / SIP Entities- SIP Entity Details

**SIP Entity Details**

**General**

\* Name: Session Manager

\* FQDN or IP Address: 192.168.81.121

Type: Session Manager

Notes: entity for Avaya Sess Manager (8

Location: Galway

Outbound Proxy:

Time Zone: Etc/GMT

Credential name:

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration



Below is the screenshot for SIP Entity for CM\_Evolution Server. Change the **Type** to **CM** when programming the SIP Entity for Communications Manager.

The screenshot shows the 'SIP Entity Details' configuration page for 'CM\_EvolutionServer'. The 'General' tab is selected. The 'Type' dropdown menu is highlighted with a red rectangle and is set to 'CM'. Other fields include 'Name' (CM\_EvolutionServer), 'FQDN or IP Address' (192.168.81.104), 'Notes' (CM\_EvolutionServer/AvayaPBX), 'Adaptation' (empty), 'Location' (Galway), 'Time Zone' (Etc/GMT), 'Override Port & Transport with DNS SRV' (unchecked), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), and 'Call Detail Recording' (none).

Home / Elements / Routing / SIP Entities- SIP Entity Details	
SIP Entity Details	
General	
* Name:	CM_EvolutionServer
* FQDN or IP Address:	192.168.81.104
Type:	CM
Notes:	CM_EvolutionServer/AvayaPBX
Adaptation:	
Location:	Galway
Time Zone:	Etc/GMT
Override Port & Transport with DNS SRV:	<input type="checkbox"/>
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

## 4.6. Administer SIP Entity Link

A SIP Trunk between a Session Manager and a telephony system is described by an Entity Link. The next step is to create SIP Entity Links, which included the transport parameters to be used for communications between the ASM and external SIP devices.



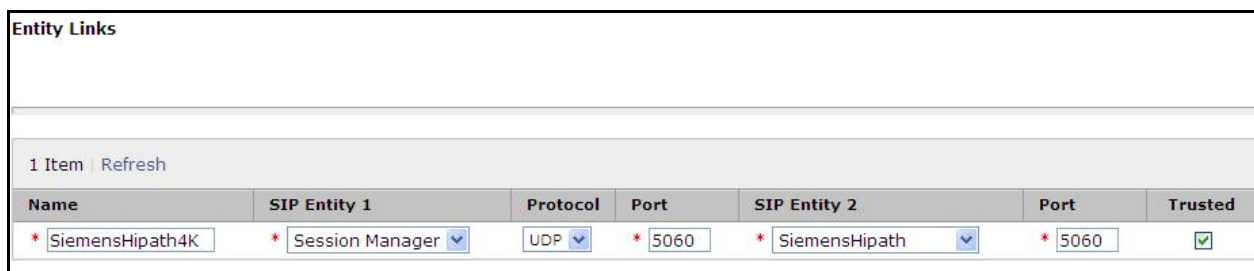
Home / Elements / Routing / Entity Links- Entity Links								
Entity Links								
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/>								
2 Items Refresh Filter: E								
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	CM-ES	Session Manager	TCP	5060	CM_EvolutionServer	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SiemensHipath4K	Session Manager	UDP	5060	SiemensHipath	5060	<input checked="" type="checkbox"/>	Entity for SessMan to Siemens

Create a SIP Entity Link for Siemens HiPath. Browse to **Home → Elements → Routing → Entity Links**. Click **New**.

- **Name** Enter a suitable identifier e.g. **SiemensHiPath4K**
- **SIP Entity 1** Drop-down and select the appropriate **Session Manager**
- **Protocol** Drop down and select **UDP**
- **Port** Enter **5060**
- **SIP Entity 2** Drop-down select the SIP Entity added previously, i.e. **SiemensHipath**
- **Port** Enter **5060**
- **Trusted** Set the field as ticked
- **Notes** Add a brief description

Click **Commit** to save.

**Note:** Some of the parameters are not visible in the screenshot below.



Entity Links							
1 Item Refresh							
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	
* SiemensHipath4K	* Session Manager	UDP	* 5060	* SiemensHipath	* 5060	<input checked="" type="checkbox"/>	

Create a SIP Entity Link for CM\_EvolutionServer. Browse to **Home → Elements → Routing → Entity Links**. Click **New**.

- **Name** Enter a suitable identifier e.g. **CM-ES**
- **SIP Entity 1** Drop-down select the appropriate **Session Manager**
- **Protocol** Dropdown select **TCP**
- **Port** Enter **5060**
- **SIP Entity 2** Drop-down and select the SIP Entity added previously, i.e. **CM\_EvolutionServer**
- **Port** enter **5060**
- **Trusted** Tick the field
- **Notes** Add a brief description

Click **Commit** to save (not shown).

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* CM-ES	* Session Manager	TCP	* 5060	* CM_EvolutionServer	* 5060	<input checked="" type="checkbox"/>

SIP Entities of type "Session Manager"

\* Input Required

Once the Entity Links have been created, return to the SIP Entities and check to see if the Entity Links have been assigned to the SIP Entities.

### Entity Links assigned to SIP Entity Siemens HiPath.

**Entity Links**  
Add Remove

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	Session Manager	UDP	* 5060	SiemensHiPath	* 5060	<input checked="" type="checkbox"/>

Select : All, None

\* Input Required

Commit Cancel

If the Entity Links have not been added to the SIP Entity automatically, click **Add** and assign the Entity Link manually.

## Entity Links and Ports assigned to SIP Entity CM\_EvolutionServer.

**Entity Links**  
Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	Session Manager	TCP	* 5060	CM_EvolutionServer	* 5060	<input checked="" type="checkbox"/>

Select : All, None

\* Input Required Commit Cancel

## Entity Links and Ports assigned to SIP Entity Session Manager.

**Entity Links**  
Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	Session Manager	TCP	* 5060	CM_EvolutionServer	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Session Manager	UDP	* 5060	SiemensHipath	* 5060	<input checked="" type="checkbox"/>

Select : All, None

**Port**  
Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	mmsil.local	
<input type="checkbox"/>	5060	TCP	mmsil.local	
<input type="checkbox"/>	5061	TLS	mmsil.local	

Select : All, None

\* Input Required Commit Cancel

## 4.7. Administer Time Ranges

Create a Time Range for LCR routing which defines policies will be active. To create a Time Range, browse to **Home → Elements → Routing → Time Ranges**. Click **New**. Under **Name** enter a suitable identified. Select which **Days** are to be included in the Range. Set a suitable **Start Time** and **End Time**. This will be used in configuring the **Dial Plan**. In Session Manager, a default policy (24/7) is available that would allow routing to occur anytime. This was used in the example network.

**Time Ranges** Commit

1 Item Refresh Filter: E

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* 24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	* 00:00	* 23:59	

## 4.8. Administer Routing Policy

To complete the routing configuration, a Routing Policy is created. Routing policies direct how calls will be routed to a system. Two routing policies must be created, one for the Communications Manager and the second for the Siemens HiPath 4000. These are to be associated with the Dial Patterns which will be created in the next step. To create a Routing Policy to route traffic to Siemens HiPath, browse to **Home → Elements → Routing → Routing Policies**. Click **New**. Under **Name** enter a suitable identifier. Under **Notes** enter suitable description. Under **SIP Entity as Destination** click on **Select**. Choose the appropriate SIP Entity that is to be the call destination. Under **Time of Day**, assign a suitable time range if more than one is programmed, click on **Add**. Click **Commit** to save.

**Routing Policy Details**

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Not
------	--------------------	------	-----

**Time of Day**

1 Item Refresh

<input type="checkbox"/>	Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00

Select : All, None

A Routing Policy is also created for the CM\_Evolution Server.

**Routing Policy Details**

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
CM_EvolutionServer	192.168.81.104	CM	CM_EvolutionServer/AvayaPBX

**Time of Day**

1 Item | [Refresh](#)

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00

Select : [All](#), [None](#)

At this stage the records are missing the **Dial Pattern** which will be created next.(Section 4.9).

## 4.9. Administer Dial Pattern

As one of its main functions, ASM routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate system. In the sample network, 5 digit extensions beginning 230 or 231 are designated as Avaya handsets (Digital and H.323), whilst 6 digit extension starting 81 are Siemens handsets. To create a Dial Pattern for calls to the Siemens HiPath, browse to **Home → Elements → Routing → Dial Patterns**. Click **New**. Under **Pattern** enter a dial string pattern e.g. **81xxxx**. (all calls with 6 digit ext beginning with **81** will be routed to Siemens HiPath). Under **SIP Domains** drop-down select **All**. Under **Notes** enter a suitable description.

**Dial Pattern Details**

**General**

\* Pattern: 81

\* Min: 6

\* Max: 6

Emergency Call: ☐

SIP Domain: -ALL-

Notes: SiemensExt

**Originating Locations and Routing Policies**

**Add** **Remove**

1 Item | Refresh

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	-ALL-	Any Locations	SiemensHiPath4K	0	<input type="checkbox"/>	SiemensHipath

Select : All, None

To add the **Originating Locations** and **Routing Policies**, previously created, click **Add**.

In the **Originating Location** section (created in **Section 4.3**), select **Apply the Selected Routing Policies to All Originating Locations**. In the **Routing Policies** (created in **Section 4.8**), select the **Routing Policy** to be applied. Click **Commit** to save.

**Originating Location**

☒ Apply The Selected Routing Policies to All Originating Locations

1 Item | Refresh

<input checked="" type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Galway	Galway Lab Siemens_Avaya

Select : All, None

**Routing Policies**

2 Items | Refresh

<input type="checkbox"/>	Name	Disabled	Destination
<input type="checkbox"/>	CM_EvoServer	<input type="checkbox"/>	CM_EvolutionServer
<input checked="" type="checkbox"/>	SiemensHiPath4K	<input type="checkbox"/>	SiemensHipath

Dial Patterns should also be created for the Avaya Digital and H.323 handsets. Screenshots for these are on the next page.



Dial Patterns should also be entered for Avaya extensions beginning **230** (Digital) and **231** (H.323) and set the **Originating Location and Routing Policies**, choosing the relevant Routing Policy for the CM\_Evolution Server.

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

General

\* Pattern: 230

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes: 230\_Digital

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	-ALL-	Any Locations	CM_EvoServer	0	<input type="checkbox"/>	CM_EvolutionServer

## 4.10. Administer Avaya Aura® Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between the System Manager and Session Manager. On the System Manager management screen, under **Elements** select **Session Manager** or from the Home screen, browse to **Home → Elements → Session Manager → Session Manager Administration**. On the right hand side, under **Session Manager Instances**, click on **New**.

Under **General**:

- **SIP Entity name** Select the names of the SIP entity added for Session Manager
- **Description** Descriptive Comment
- **Management Access Point Host Name/IP**  
Enter the IP address of the Session Manager management interface

Under **Security Module**

- **Network Mask** Enter the network mask corresponding to the IP address of the Session Manager
- **Default Gateway** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields.

**Edit Session Manager**

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Conn  
Expand All | Collapse All

**General**

SIP Entity Name: Session Manager

Description: SM100

\* Management Access Point Host Name/IP: 192.168.81.120

\* Direct Routing to Endpoints: Enable

**Security Module**

SIP Entity IP Address: 192.168.81.121

\* Network Mask: 255.255.255.0

\* Default Gateway: 192.168.81.254

\* Call Control PHB: 46

\* QOS Priority: 6

\* Speed & Duplex: Auto

VLAN ID:

## 4.11. Add Avaya Aura® Communication Manager as an Evolution Server

In order for Communication Manager to provide configuration and Evolution Server support to SIP Phones when they register to Session Manager, Communication Manager must be added as an application.

### 4.11.1. Create a Avaya Aura® Communication Manager Instance

On the System Manager Managements screen under **Elements**, select **Inventory**. Alternatively, browse to **Home → Elements → Inventory → Manage Elements**. Click **New**. Click on the **Application Tab** and enter detail in the following fields.

- **Name** Enter a Descriptive Name
- **Type** Set to **CM**
- **Description** Free text entry
- **Node** Set to IP Address for CM SAT Access

All other fields may be left with default settings.

**Edit CM: CM**

**Application \*** **Attributes \***

Application ▼

\* **Name** CM

\* **Type** CM ▼

**Description** CM Instance

\* **Node** 192.168.81.102

Click on the **Attributes Tab** and enter detail in the following fields.

- **Login** Login used for SAT access
- **Password** Password used for SAT access
- **Confirm Password** Password used for SAT access
- **Node** Set to IP Address for CM SAT Access

All other fields may be left with default settings.

**Edit CM: CM**

Application \* **Attributes \***

SNMP Attributes ▾

\* Version ☒ None ☐ V1 ☐ V3

Attributes ▾

\* Login

Password

Confirm Password

Is SSH Connection ☒

\* Port

#### 4.11.2. Create an Evolution Server Application

For Evolution Server support, further configuration of the Session Manager is required. Once complete the Session Manager will support Avaya SIP phone registration. Users are created through the Session Manager **User Management** screens. Session Manager creates corresponding stations on the Evolution Server. Configuration of the Evolution Server Application via Session Manager is a two stage sequence, with the Application being created first, followed by the Application Sequence. To configure browse to: **Home → Elements → Session Manager → Application Configuration → Applications**. Click **New**. Under **Name** enter a suitable identifier. Under **SIP Entity** drop-down select the SIP Entity of the Feature Server. Under **Description** enter a suitable description. Click **Commit** to save.

**Home / Elements / Session Manager / Application Configuration / Applications- Applications**

**Application Editor**

Application

\* Name

CM-ES

\* SIP Entity

CM\_EvolutionServer ▼

\* CM System for SIP Entity

CM ▼

Refresh

[View/Add CM Systems](#)

Description

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

To configure the Application Sequences Configuration. Browse to: **Home → -Elements → -Session Manager → Application Configuration → Applications Sequences**. Click **New**. Under **Name** enter a suitable identifier. Under **Description** enter a suitable description. From the **Available Applications** section, select the **+** sign beside the **Application** that is to be added to this sequence. Verify that the **Application in this Sequence** is updated correctly Click **Commit** to save.

**Application Sequence Editor**

Application Sequence

\*Name

Description

**Applications in this Sequence**

Move First Move Last Remove

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory
<input type="checkbox"/>		CM-ES	CM_EvolutionServer	<input checked="" type="checkbox"/>

Select : All, None

**Available Applications**

1 Item Refresh

	Name	SIP Entity	Description
+	CM-ES	CM_EvolutionServer	

At this point the configuration of ASM is complete. To add users for Avaya SIP endpoints refer to **Section 8 Reference [1]**.

### 4.11.3. Synchronize Avaya Aura® Communication Manager Data

On the System Manager management screen under **Elements**, select **Inventory** or browse to **Home → Elements → Inventory → Synchronization → Communication System**. Select the appropriate **Element Name** and the select **Initialize data for selected devices**. Then click on **Now**.

**Note:** This Process can take some time.

Home / Elements / Inventory / Synchronization / Communication System- Synchronize CM Data and Configure Optic

### Synchronize CM Data and Configure Options

Synchronize CM Data/Launch Element Cut Through | Configuration Options |  
Expand All | Collapse All

Synchronize CM Data/Launch Element Cut Through ▾

1 Item | Refresh | Show ALL ▾

<input checked="" type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status
<input checked="" type="checkbox"/>	CM	192.168.81.102	May 27, 2011 12:00:27 AM +01:00	10:00 pm THU MAY 26, 2011	Incremental	Completed

Select : All, None

☒ Initialize data for selected devices  
☐ Incremental Sync data for selected devices  
☐ Save Translations for selected devices

## 4.12. Administer SIP Users

SIP Users must be added via Session Manager and the details will be updated on Communication Manager. On the System Manager management screen under the **Users** Column, select **User Management** or browse to **Home → Users → User Management → Manage Users**. Click **New**. On the **Identity** tab enter the following information and use defaults for other fields.

- **Last Name** Enter a last name
- **First Name** Enter a first name
- **Login Name** Enter the desired phone [extension@domain.com](#) where the domain was defined in **Section 4.2**
- **Password** Password for the user to log into System Manager (SMGR)

The screenshot shows the 'New User Profile' form with the 'Identity' tab selected. The form contains the following fields and values:

- Last Name:** Phone\_2
- First Name:** SIP
- Middle Name:** (empty)
- Description:** 2nd SIP Phone
- Login Name:** 23400@mmsil.local
- Authentication Type:** Basic
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Localized Display Name:** (empty)
- Endpoint Display Name:** (empty)
- Honorific:** (empty)
- Language Preference:** (dropdown menu)
- Time Zone:** (dropdown menu)



Next click on the **Communication Profile** tab.

- **Last Name** a desired last name
- **First Name** a desired first name
- **Login Name** the desired phone [extension@domain.com](#) where the domain was defined in **Section 4.2**
- **Password** Password for the user to log into System Manager (SMGR)
- **Communication Profile Password** Password entered by user when logging into a phone
- **Confirm Password** Repeat of the above password

Expand **Communication Address** and click **New**.

- **Type** Set to Avaya SIP
- **Fully Qualified Address** Enter the extension number and set the Domain.

Communication Profile ▾

Communication Profile Password:

Confirm Password:

Name
Primary

Select : None

\* Name:

Default : ☒

Communication Address ▾

Type	Handle	Domain
No Records found		

Type:

Fully Qualified Address:  @

Next, navigate down the screen to **Session Manager Profile** and **Endpoint Profile**.



The screenshot shows a configuration window with a 'Fully Qualified Address' field containing '244000' and a dropdown menu set to 'mmsf.local'. Below this, there are three profile selection options, each with a checkbox and an asterisk: 'Session Manager Profile', 'Endpoint Profile', and 'Messaging Profile'. A red rectangular box highlights the 'Session Manager Profile' and 'Endpoint Profile' options.

Select the appropriate Session Manager server for **Primary Session Manager**. For **Origination Application Sequence** select the Application Sequence created in **Section 4.11.3**. Choose **Home Location** created in **Section 4.3**. Click on **Endpoint Profile** to expand that section. Enter the following fields and use defaults for the remaining fields.

- **System** Select the CM Entity
- **Extension** Enter a desired extension number
- **Template** Select a telephone type template
- **Port** Select **IP**

Click on **Commit** to save changes.

☒ Session Manager Profile

\* Primary Session Manager

Session Manager

Secondary Session Manager

(None)

Origination Application Sequence

CM-ES

Termination Application Sequence

CM-ES

Survivability Server

(None)

\* Home Location

Galway

Primary	Secondary	Maximum
4	0	4

Primary	Secondary	Maximum

☒ Endpoint Profile

\* System

CM

\* Profile Type

Endpoint

Use Existing Endpoints

☐

\* Extension

24400

Endpoint Editor

\* Template

DEFAULT\_9620SIP\_CM\_6\_0

Set Type

9620SIP

Security Code

\* Port

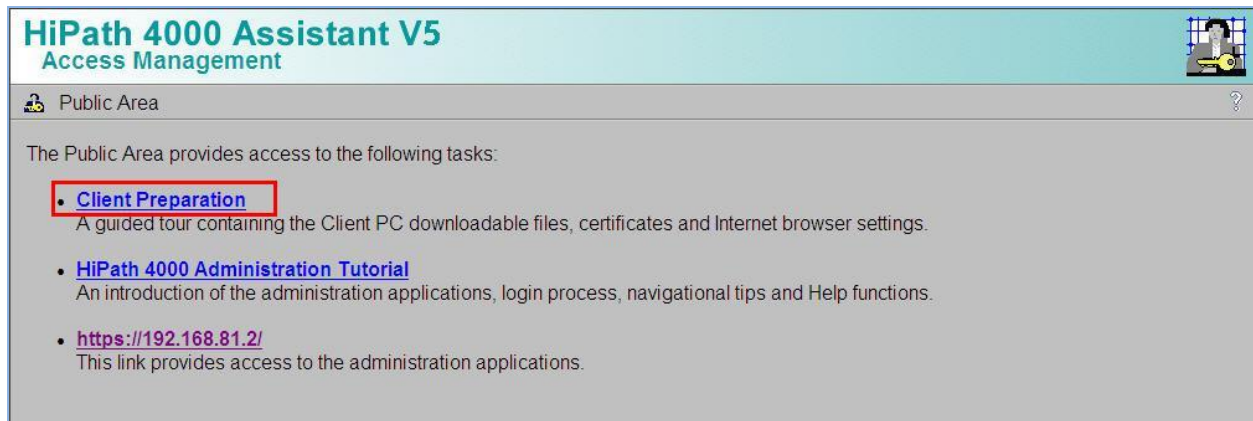
IP

## 5. Configure the Siemens HiPath 4000

The Siemens HiPath configuration was verified using the web interface HiPath 4000 Assistant V5. Before the web interface can be used, the Client PC must be prepared. To access the web interface use internet explorer [http://IPAddress\\_of\\_HiPath/](http://IPAddress_of_HiPath/).

### 5.1. Client PC Preparation

To access the HiPath 4000 Assistant via internet browser, the user must prepare the client machine. Click on **Client Preparation**.



The following page is displayed, listing the steps to prepare the Client PC. Click on **Next**.



Click **Next**.

If an error is displayed for the version of Internet Browser detected, follow the steps listed under **Installation** to install a correct level of Browser. Otherwise click on **Next**.

## HiPath 4000 Assistant V5

PreviousCancelNext

### Installation of the Internet Browser [1/6]


#### Information

The following Internet browsers are supported:

- Microsoft Internet Explorer 5.5, 6.0, 7.0

#### Diagnosis

Result of the automatic browser check:

**INFO:**  
Proper Internet browser (Internet Explorer 7.0) installed.

- If a green check (✓) appears, you are using a supported Internet browser version and you may proceed with the next preparation step.
- If a yellow warning triangle (⚠) or a red stop sign (⛔) appears, you are using an unsupported Internet browser version. There is no information available whether this version works. To be sure install a supported version of an Internet browser.

#### Installation

1. Download your favorite Internet browser straight from the manufacturer:
  - [Microsoft Internet Explorer](#)
2. Quit your currently running Internet browser.
3. Install the downloaded Internet browser according the installation instructions of the manufacturer.
4. Start the newly installed Internet browser, return to this page and continue with the client preparation.

PreviousCancelNext



Verify that the Client PC has a suitable version of Java Runtime Environment Plug-in. In the image below, a warning is displayed. Although you can ignore this warning if you have a newer version of Java, should you experience problems with loading HiPath Assistant screens, please return to this preparation process and install a recommended version of Java, having first uninstalled any previous versions of Java, Java Plug-in v1.6.0\_17 works fine. Click **Next**.

## HiPath 4000 Assistant V5

PreviousCancelNext


### Installation of the Java™ Runtime Environment (Java Plug-in) [2/6]

#### Information

The installation of the Java™ Runtime Environment (Java Plug-in) is required for HiPath 4000 administration clients.

#### Diagnosis

Installation status of the Java™ Runtime Environment (Java Plug-in):



**WARNING:**  
Installed version (v1.6.0\_17) is not explicitly approved.

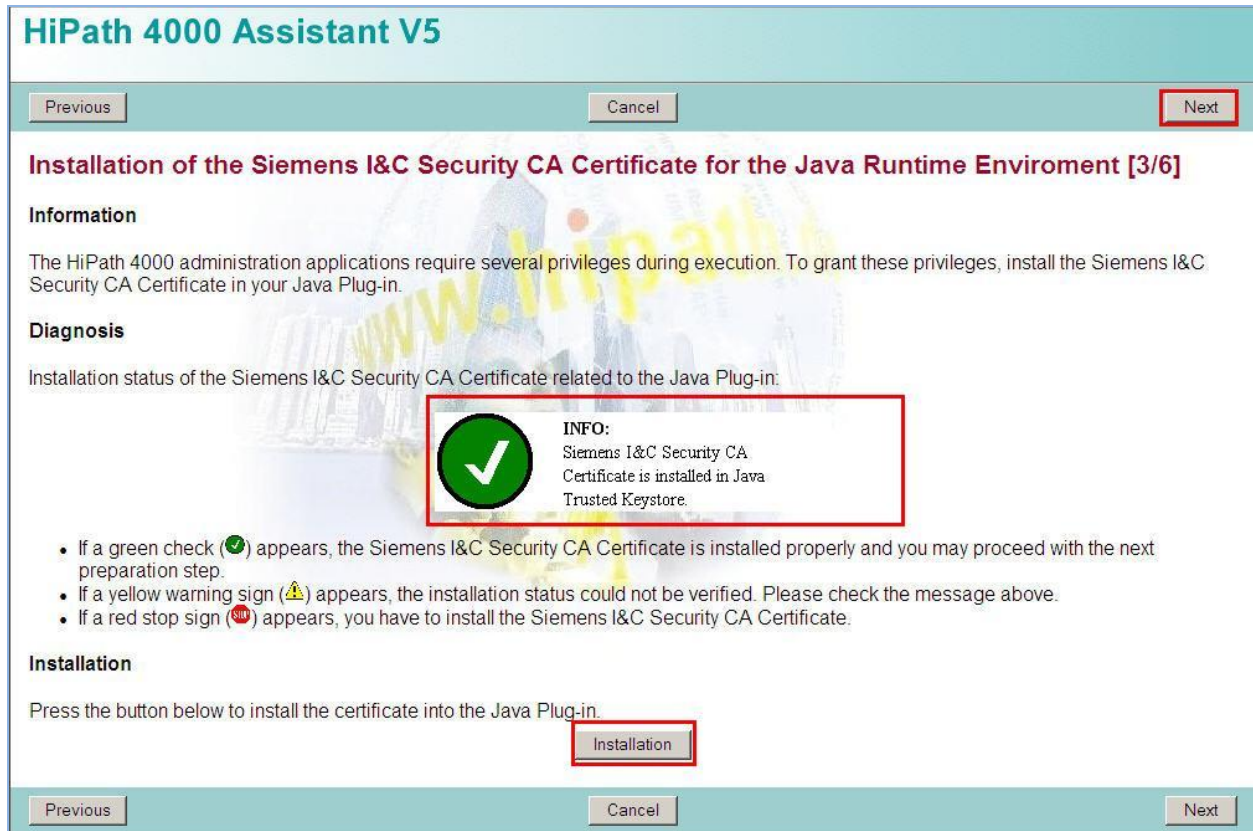
- If a green check (✓) appears, a correct version of the Java™ Runtime Environment is already installed and you may proceed with the next step.
- If a yellow warning triangle (⚠) appears, you have a version of the Java™ Runtime Environment installed that is not explicitly approved. There is no information available whether this version works. Install the version provided below.
- If a red stop sign (⛔) appears, install the provided version of the Java™ Runtime Environment and/or enable Active-X controls and plug-ins. If you are not sure whether you have already installed Java™ Runtime Environment, it is safer to install it again.
- If the automatic diagnosis fails (🔧 / 📄), install the provided version of the Java™ Runtime Environment.

#### Installation

1. Select JRE according to your operating system:
  - Download JRE 6 Update 11  
[jre-6u11-windows-i586-p.exe](#), suitable for operating system [Microsoft Windows™ 2000 / XP / 2003 / Vista](#).
  - Download JRE 5.0 Update 17  
[jre-1\\_5\\_0\\_17-windows-i586-p.exe](#), suitable for operating systee [Microsoft Windows™ 98 / ME / 2000 / XP / 2003 / Vista](#).
  - Download JRE 1.4.2 Update 19  
[j2re-1\\_4\\_2\\_19-windows-i586-p.exe](#), suitable for operating systees [Microsoft Windows™ 95 / 98 / ME / NT4.0 / 2000 / XP / 2003 / Vista](#).
2. Quit and exit your Internet browser.
3. Install the downloaded JRE on your PC by double clicking the executable.
4. You may delete this executable after successful installation.
5. Restart your Internet browser, return to this Web page and continue with the client preparation.

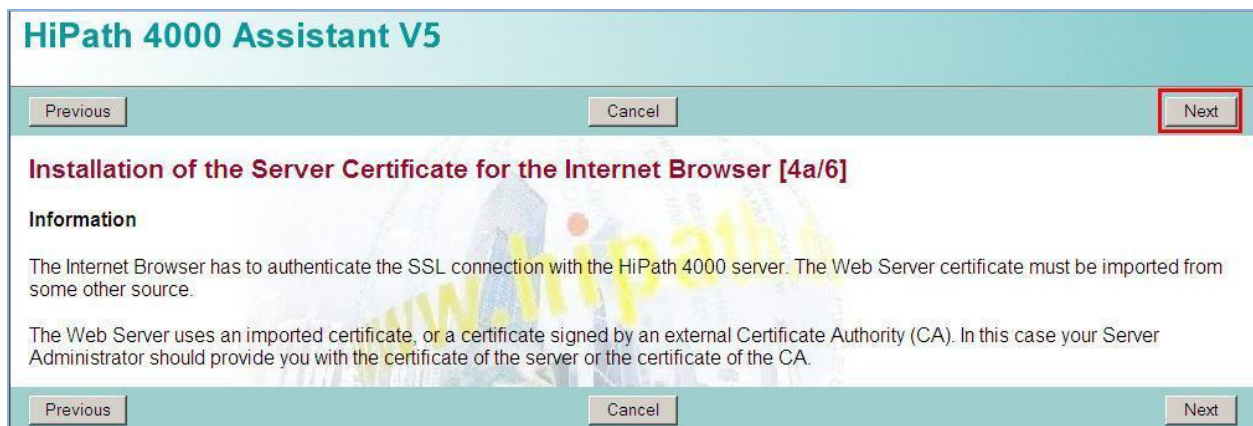
PreviousCancelNext

Verify Siemens I&C Security CA Certificate. If an error message is displayed, click on **Installation** to install the Security Certificate. Click **Next**.



**Notes:** It is strongly recommended that you close Internet Explorer and re-open it after certificate installation.

The next three screens are information level notices. Click **Next** to proceed.



Click **Next**.

**HiPath 4000 Assistant V5**

Previous Cancel **Next**

**Installation of the Server Certificate into the Java Runtime Environment [4b/6]**

**Information**

The Internet Browser has to authenticate the SSL connection with the HiPath 4000 server. The Web Server certificate must be imported from some other source.

The Web Server uses an imported certificate, or a certificate signed by an external Certificate Authority (CA). In this case your Server Administrator should provide you with the certificate of the server or the certificate of the CA.

Previous Cancel Next

Click **Next**.

**HiPath 4000 Assistant V5**

Previous Cancel **Next**

**Configuration of the Internet Browser [5/6]**

**Information**

The HiPath 4000 administration applications require your Internet browser be properly configured. Details about the required configuration are found by pressing the *Information* button below.

**Information**

Please note: Changing your browser configuration may affect the access to other sites and the security of your system. Ask your system administrator if you are not sure about these issues.

**Diagnosis**

To check the configuration of your Internet browser press the *Diagnosis* button below.

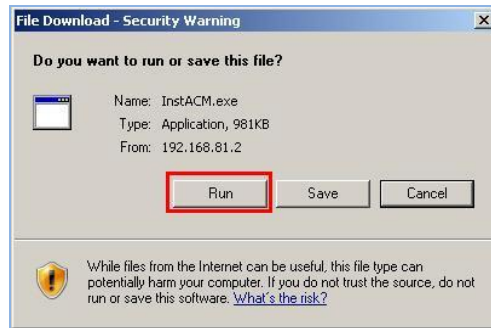
**Diagnosis**

Please note: the diagnosis does not cover all required and optional parameters.  
For a detailed list of these parameters for manual configuration see chapter *Information* above.

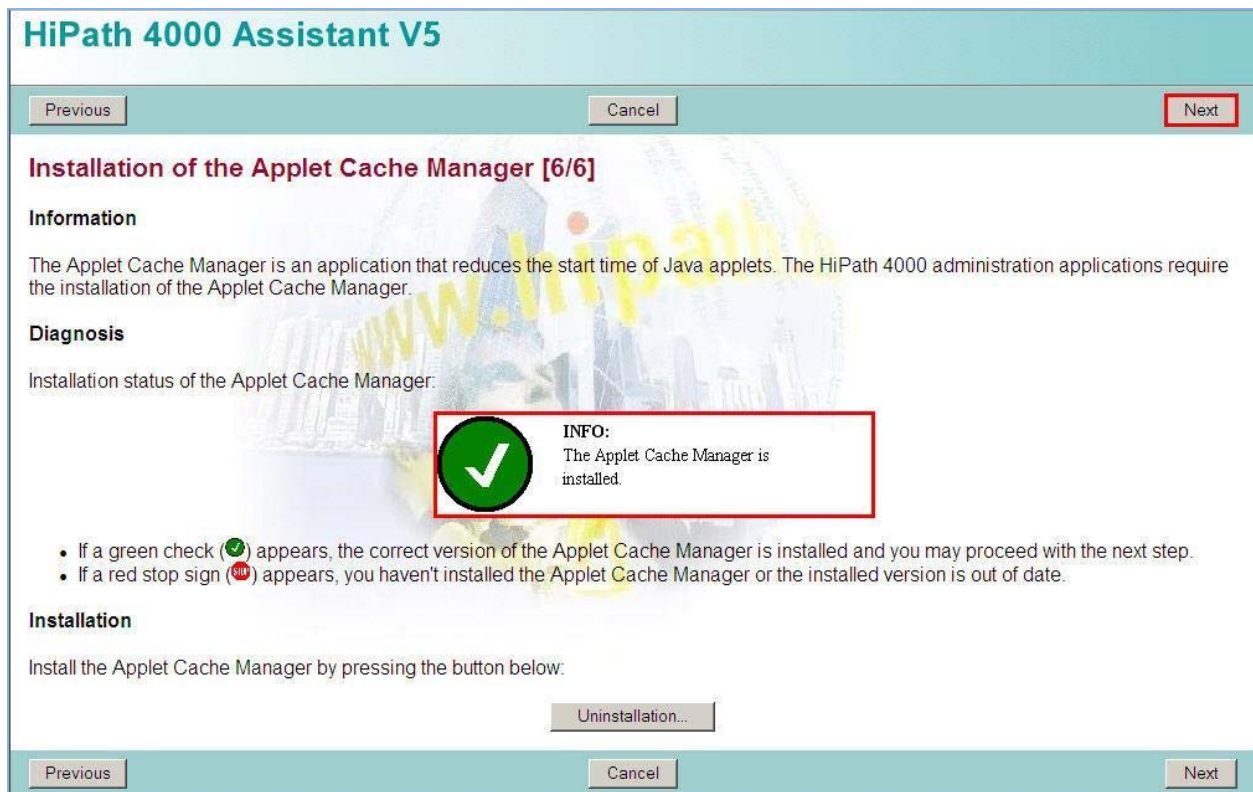
Previous Cancel Next



The Client PC will be prompted to install **InstACM.exe**. This is an Applet Cache Manager plug-in which is required to run HiPath 4000 Assistant web interface. Click on **Run**.



The browser may need to be restarted, proceed to step 6 of the web installation. Verify that the Applet Cache Manager is installed. Click on **Next**.

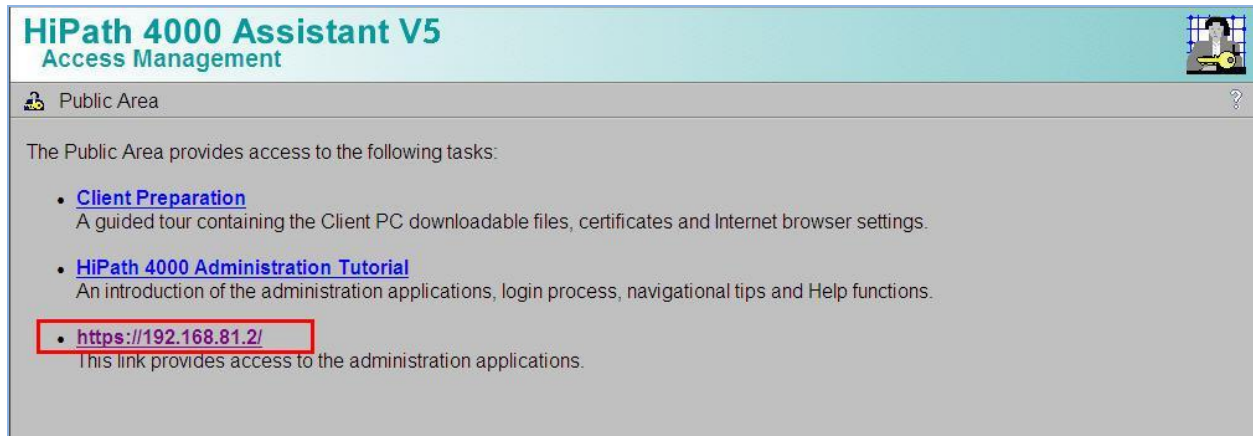


Client Preparation finished. Click **Logon**.



## 5.2. HiPath 4000 System Configuration

Once the Client PC is prepared, access to the administration applications is available. Return to the main login page. Click on the HiPath admin link, listed as the IP Address of the HiPath server.

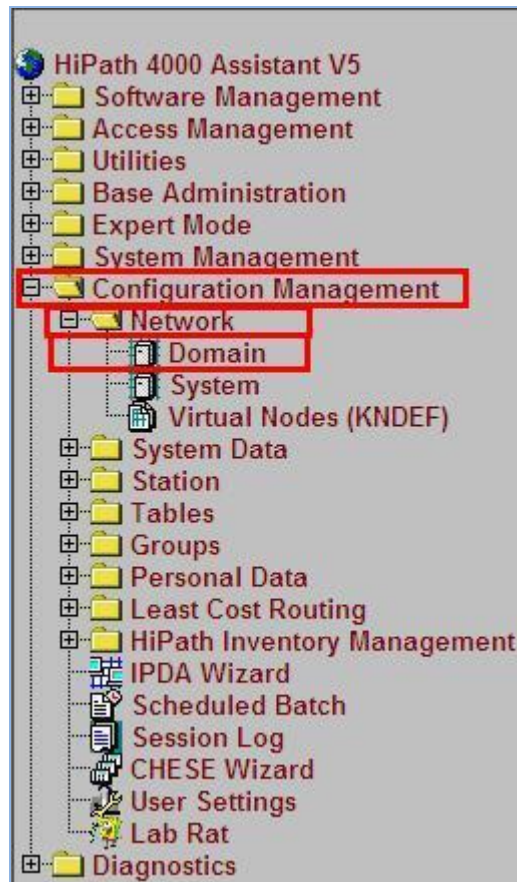


Log in to the portal using the engineering logon. (Refer to the Siemens installation engineer for client access details).



### 5.2.1. Network Domain Configuration

The HiPath Assistant portal will be displayed as a tree structure on the left. Once a final option is selected on the left, the screen will either open in new window or open on the right hand side of the screen. To check/edit the **Network Domain Configuration**. Expand **Configuration Management** → **Network** → **Domain**.



Click on the **Search** button to access the current configuration. This returns all programmed records up to a limit of 1000.

HiPath 4000 Assistant V5  
Configuration Management

Domain

Object Edit View Action Scheduled Batch Extras Help

View: ☒ Search Criteria

Domain:

Tie Line:

Description:

Systems

System	Description
<input type="text"/>	<input type="text"/>

0/1

Abort Search Search New

The domain name is entered in the **Domain** field. The associated system name is listed under the **Systems** tab.

HiPath 4000 Assistant V5  
Configuration Management

Domain

Object Edit View Action Scheduled Batch Extras Help

View: ☐ Search Criteria ☒ Object ☐ Object List

Domain:

Tie Line:

Description:

Systems

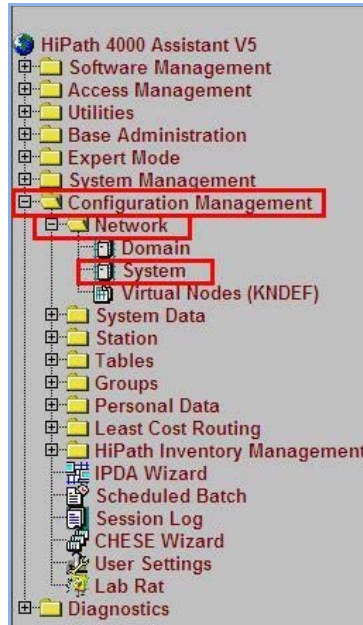
System	Description
<input type="text"/>	<input type="text"/>

0/1

Abort Search Search New

### 5.2.2. System Configuration

To check/edit the **System Configuration** which contains details of the version number, upload the system number of the HiPath 4000. Expand **Configuration Management** → **Network** → **System**. Wait for the System screen to display on the right hand side or in a new window.





Leaving all fields empty, click on the **Search** button to access the current configuration (button not shown). This will return all records found in the system up to a limit of 1000 records. Alternatively click the down arrow beside the field system to choose from a list of items. Select the **System** name as recorded from the previous step and click Search. One or more fields may be selected as Search criteria.

**HiPath 4000 Assistant V5**  
Configuration Management

System

Object Edit View Action Scheduled Batch Extras

View: Search Criteria Object Object List

System: SYS1 VNR active

Domain: DOMAIN

Description:

System Type: HiPath4000 Version: V5

Base Data Dimensioning PIN Language Cordless Additional Data External VoiceMail Service SPE & PKI

AMO Language: English

VMS System:

VM Server:

Node Number: 1-69-999

Extended Node Number: 1-69-999

Preferred Route Index:

System Number: L31906Q2966X00001

Country: DE

Area Code: 089

CO Number: 722

System supports LCR

Large Enterprise Gate Keeper

DTB Server Access Code:

Upload Status: BACKUP\_REQUIRED

Detailed Report

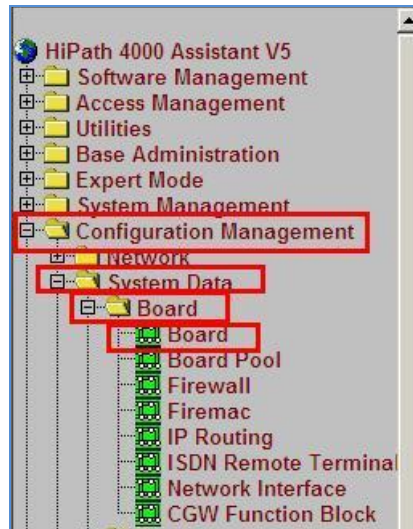
Stations: SYNCHRONOUS

LCR: SYNCHRONOUS

System Data: SYNCHRONOUS

HIM Data: SYNCHRONOUS

The HiPath 4000 Communication Server uses ISDN cable connection to the cabinets containing the Siemens **HG3500** IP gateways. The IP Gateways also communicate via IP network across the LAN. This sample configuration includes a SIP Trunk Gateway (X.X.81.6), a SIP Gateway (X.X.81.3) and a H.323 Gateway (X.X.81.4). The Gateways are collectively described by Siemens as HG3500 or HG35XX boards and are universal card. It is during configuration of these cards that the role is defined as to whether the board is SIP or H.323. To access the configuration of the **HG3500**, expand **Configuration Management** → **System Data** → **Board** → **Board**. Wait for the **Config** screen to display. Click on **Search** to access the current configuration.



Each **Board** has a specific location code, indicated by **LTG** (Line Trunk Group), **LTU** (Line Trunk Unit), and **SLOT** (Physical position with LTU where card has been inserted). In the image below, the code is **1-1-4**. This is the SIP Trunk Gateway. The board location code is important to know when creating **Stations** for telephony endpoints.

**HiPath 4000 Assistant V5 Configuration Management**

**Board**

Object: Edit View Action Scheduled Batch Extras

View: ☐ Search Criteria ☒ Object ☐ Object List

LTG: 1 LTU: 1 SLOT: 4

Part Number: Q2324-X500 Function ID: 1 Category: IPGW Board Name: STMI4 CGW Function Block: 1

System: SYS1

Domain: DOMAIN

Description:

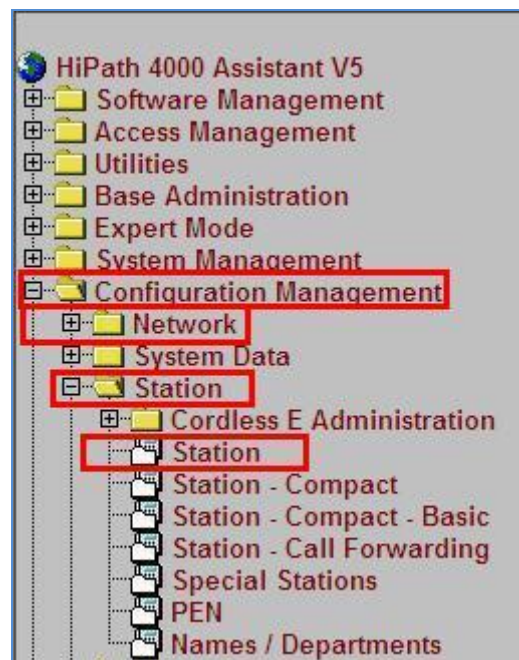


The board list for this sample configuration are:

Board Location / PEN	IP Address	Function
1-1-1	X.X.81.3	SIP Gateway Phone Reg [Siemens 420 SIP Phones]
1-1-4	X.X.81.6	SIP GW SIP Trunks
1-1-2	NA	TDM Interface [Siemens 500 Digital Phones]
1-2-1	X.X.81.4	H.323 GW [Siemens 410 H.323 Phones]
1-2-13	NA	8 Ch. Voice Card. Interface to Siemens Expressions Server
1-2-2	NA	24 Port Analog [Fax]
1-1-14	NA	Q-Sig
1-1	NA	LTU1 ISDN Admin Link
1-2	NA	LTU2 ISDN Admin Link

### 5.2.3. Siemens Station End-Points

The Siemens Stations can be managed from the HiPath Assistant. To check/edit the Stations, expand **Configuration Management** → **Station** → **Station**. Wait for the config screen to display. Click on **Search** to access the current configuration.



The image below illustrates the configuration of a TDM Station:

- **Station No.** Selected from drop down list
- **PEN.** Must match the Card location described in previous section. (1-1-2 is the TDM Interface Card)
- **Device Combination.** Select from Drop down list
- **Device Family.** Selected from Drop down list
- **Connection Type** Direct (TDM), IP2 (H.323) SIPSEC (SIP)
- **Display Name.** Enter a suitable display name
- **COS and LCRCOS.** Class of Service must be assigned. Default shown
- **Way to Display.** Set to **yes** to display Caller Name and ID

The image below illustrates the configuration of a SIP Station Endpoint.

- **Station No.** Selected from drop down list
- **PEN.** Must match the Card location described in previous section (1-1-1 is the SIP Registrar Interface Card)
- **Device Combination.** Select from Drop down list
- **Device Family.** Selected from Drop down list
- **Display Name.** Enter a suitable display name
- **COS and LCRCOS.** Class of Service must be assigned. Default shown
- **Way to Display.** Set to **yes** to display Caller Name and ID

**HiPath 4000 Assistant V5**  
Configuration Management

Station

Object Edit View Action Scheduled Batch Extras

View: Search Criteria Object Object List

Station No.: 810011 PEN: 1-1-1-0 Device Combination: S0PP

System: SYS1 VNR active: Virtual Node ID: 1-69-1 Access Code: 900001 Device Family: S0PP

Domain: DOMAIN Location Code: In Service: yes Status: READY

Remark:

Connection Type: SIPSEC Board present: ☒

Basic 1 Basic 2 Basic 3 Bus Extension Call Forwarding Group 1 Group 2 Cordless Voice-Mail PIN Class Marks Net-wide Config Key System Dev. Handler SIP Subscriber

Display Name: HiPath SIP\*

Speed Dial Facility: no

Speed Dial List 1:

DPLN Group: 0

ITR Group: 0

Speed Dial List 2:

COSX Group: 0

Auto Download:

Manual Download:

Max. Callbacks - Busy: 5

Hotline Index:

COS 1: 31

COS 2: 31

LCRCOS 1 Voice: 7

LCRCOS 1 Data: 7

LCRCOS 2 Voice: 7

LCRCOS 2 Data: 7

Key Layout:

Key System: ☒

Alarm Number:

Way to Display: yes

Indiv. Key Layout

0/1

Abort Search

6 / 8

Save Discard New Delete

The image below illustrates the configuration of a H.323 Station Endpoint.

- **Station No.** Selected from drop down list
- **PEN.** Must match the Card location described in previous section. (1-2-1 is the H.323 GW Interface Card)
- **Device Combination.** Select from Drop down list
- **Device Family.** Selected from Drop down list
- **Display Name.** Enter a suitable display name
- **COS and LCRCOS.** Class of Service must be assigned. Default shown
- **Way to Display.** Set to **yes** to display Caller Name and ID

**HiPath 4000 Assistant V5**  
Configuration Management

Station

Object Edit View Action Scheduled Batch Extras

View: Search Criteria Object Object List

Station No.: 810103 PEN: 1-2-1-0 Device Combination: optP410-std

System: SYS1 VNR active Virtual Node ID: 1-69-1 Access Code: 900001 Device Family: OPTIPOINT

Domain: DOMAIN Location Code: In Service: yes

Remark: Status: READY

Connection Type: IP2 Board present

Basic 1 Basic 2 Basic 3 Bus Extension Call Forwarding Group 1 Group 2 Cordless Voice-Mail PIN Class Marks Net-wide Config Key System Dev. Handler SIP Subscriber

Display Name: HiPath H323\*

Speed Dial Facility: no

Speed Dial List 1:

DPLN Group: 0

ITR Group: 0

Speed Dial List 2:

COSX Group: 0

Auto Download:

Manual Download:

Max. Callbacks - Busy: 5

Hotline Index:

COS 1: 31

COS 2: 31

LCRCOS 1 Voice: 7

LCRCOS 1 Data: 7

LCRCOS 2 Voice: 7

LCRCOS 2 Data: 7

Key Layout: 8

Indiv. Key Layout

Key System

Alarm Number:

Way to Display: yes

0/1

Abort Search

3 / 8

Save Discard New Delete

### 5.3. HG 3500 Gateway Configuration

To access the configuration of the HG3500 Gateway, use the Web Console interface <https://IPAddress-Of-HGGW/> and Login screen will appear.

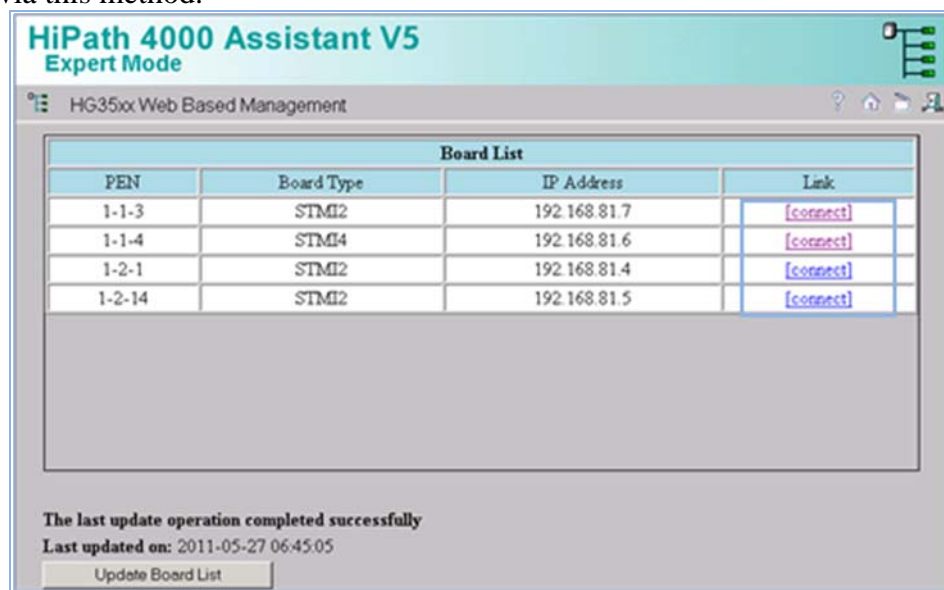


A screenshot of the 'Local administrator login' window. It features a title bar with the text 'Local administrator login'. Below the title bar, there are two input fields: 'User name:' with the text 'TRM' entered, and 'Password:' with masked characters (dots). Both fields are enclosed in red rectangular boxes. Below the password field, there are two buttons: 'Login' and 'Cancel'. The 'Login' button is also enclosed in a red rectangular box.

Alternatively the configuration of a card may be reached via HiPath Assistant by accessing **Expert Mode→HG35XX Web Based Management**.



Once you have selected this screen, a pop up window will appear offering a list of boards accessible via this method.



A screenshot of the 'HiPath 4000 Assistant V5 Expert Mode' window. The title bar shows 'HiPath 4000 Assistant V5 Expert Mode'. Below the title bar, there is a tab labeled 'HG35xx Web Based Management'. The main content area displays a 'Board List' table with four columns: 'PEN', 'Board Type', 'IP Address', and 'Link'. The table contains four rows of data. Below the table, there is a message: 'The last update operation completed successfully' and 'Last updated on: 2011-05-27 06:45:05'. At the bottom, there is a button labeled 'Update Board List'.

PEN	Board Type	IP Address	Link
1-1-3	STMI2	192.168.81.7	[connect]
1-1-4	STMI4	192.168.81.6	[connect]
1-2-1	STMI2	192.168.81.4	[connect]
1-2-14	STMI2	192.168.81.5	[connect]

Click on the **connect** link of the board you wish to review. On initial load of the screens, Java is used and can take some time before the screens are available to use. Main menus of use are:

- **Explorers** Offers access to configure SIP parameters
- **Save** Save any changes made to the board via these screens
- **Reset** Some changes require the board to be restarted

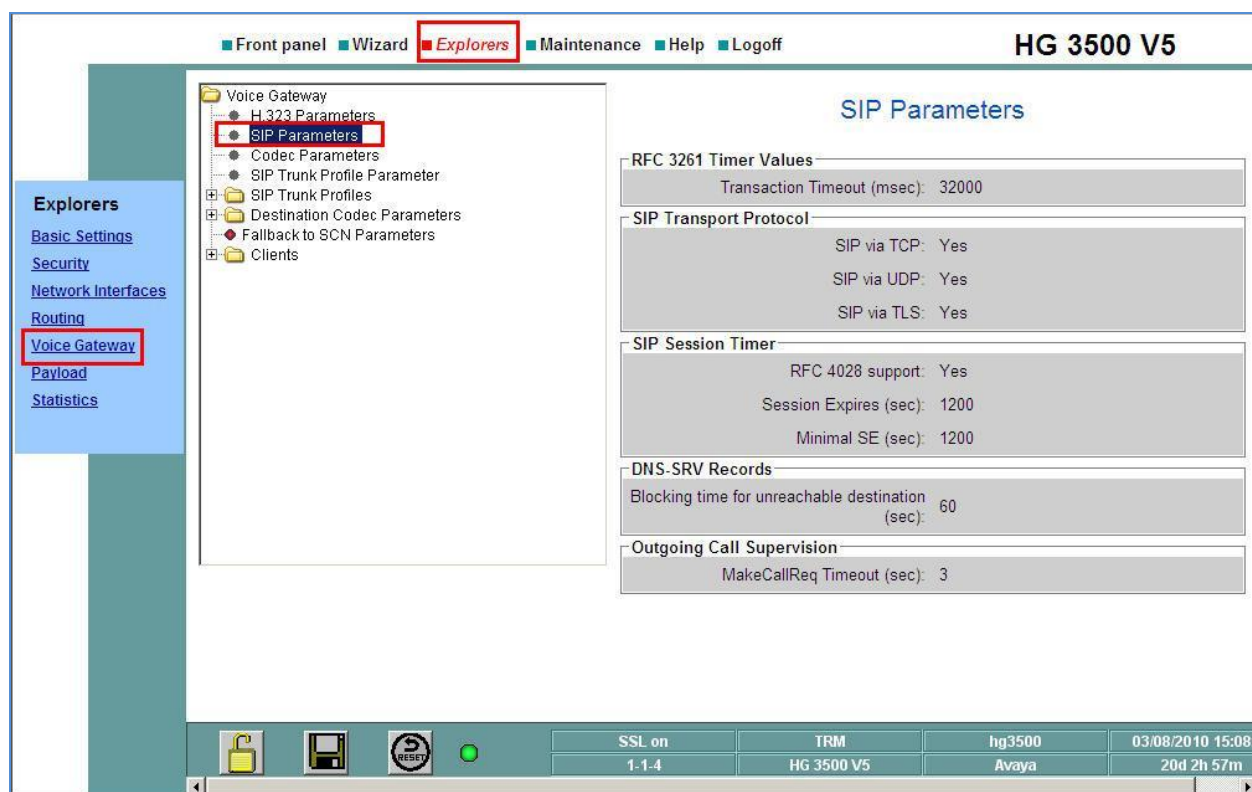




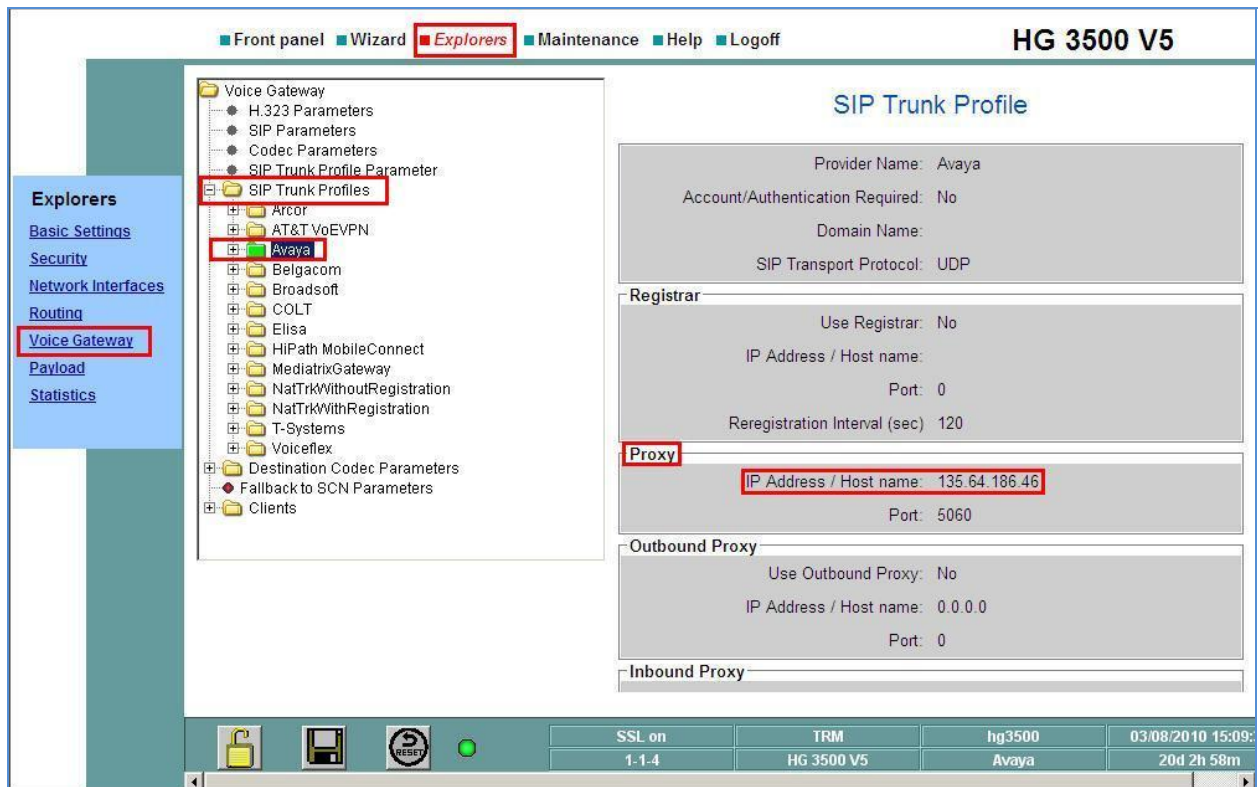
### 5.3.1. SIP Trunk Gateway

The image below shows the SIP Trunk Gateway configuration, listing the **SIP Parameters** used in these sample notes. Select **Explorers** → **Voice Gateway** → **SIP Parameters**. To edit any of these settings, right click on **SIP Parameters** and choose **Edit SIP Parameters**. Not all fields are configurable. Only the following fields are configurable via these screens:-

Section	Field Name
SIP Server (Registrar / Redirect)	Period of registration (sec):
RFC 3261 Timer Values	Transaction Timeout (msec):
SIP Transport Protocol	SIP via UDP:
SIP Session Timer	RFC 4028 support:
SIP Session Timer	Session Expires (sec):
SIP Session Timer	Minimal SE (sec):
DNS-SRV Records	Blocking time for unreachable destination(sec):
Outgoing Call Supervision	MakeCallReq Timeout (sec):



The image below shows the **SIP Trunk Profile** configuration created for **Avaya**. Select **Explorers** → **Voice Gateway** → **SIP Trunk Profiles** → **Avaya**. Under the section **Proxy**, verify that the SM100 card IP address is entered. To edit the settings, right click the folder and select **edit**. Make the necessary changes and click the **Apply** button at the bottom of the screen (not shown). Click the **SAVE** disk icon if it goes **Red**. The SIP Trunk Profile must then be activated, as shown in the image below. To activate a SIP Trunk Profile, right click on the profile and choose **Activate** (not shown). The folder will then go Green to indicate it is the active Trunk Profile.





### 5.3.1.1 SIP Registrar Gateway

This is the card used by the handsets when they register. The image below shows the SIP Trunk Gateway configuration, listing the **SIP Parameters** used in these sample notes. Select **Explorer** → **Voice Gateway** → **SIP Parameters**.

The screenshot shows the HG 3500 V5 configuration interface. The top navigation bar includes 'Front panel', 'Wizard', 'Explorers' (highlighted), 'Maintenance', 'Help', and 'Logoff'. The left sidebar shows 'Explorers' with a tree view where 'Voice Gateway' is expanded and 'SIP Parameters' is selected. The main content area is titled 'SIP Parameters' and contains several configuration sections:

- RFC 3261 Timer Values**: Transaction Timeout (msec): 32000
- SIP Transport Protocol**: SIP via TCP: Yes, SIP via UDP: Yes, SIP via TLS: Yes
- SIP Session Timer**: RFC 4028 support: Yes, Session Expires (sec): 1200, Minimal SE (sec): 1200
- DNS-SRV Records**: Blocking time for unreachable destination (sec): 60
- Outgoing Call Supervision**: MakeCallReq Timeout (sec): 3

The bottom status bar shows 'SSL on', 'TRM', 'hg3500', and the date/time '03/08/2010 15:08'.

To view registered SIP clients, select **Explorers** → **Voice Gateway** → **Clients** → **SIP**.

The screenshot shows the HG 3500 V5 configuration interface. The top navigation bar is the same as the previous screenshot. The left sidebar shows 'Explorers' with a tree view where 'Voice Gateway' is expanded and 'Clients' is selected. The main content area is titled 'SIP Clients' and displays a table of registered clients:

DID number of Client	IP Address of Client	Client Registered	User ID of Client	Security Zone of Client	Use Fixed IP Address	Authentication required
810011	192.168.81.110	true			false	false

Below the table, there is a 'Refresh' button, a checkbox for 'auto refresh' (checked), and a label 'Seconds until next automatic refresh: 54'.

### 5.3.1.2 H.323 Gateway

The image below shows the H.323 GW configuration listing the **H.323 Parameters** used in these sample notes. Select **Explorers** → **Voice Gateway** → **H.323 Parameters**.

The screenshot shows the HG 3500 V5 configuration interface. The top navigation bar includes 'Front panel', 'Wizard', 'Explorers' (highlighted), 'Maintenance', 'Help', and 'Logoff'. The left sidebar shows 'Explorers' with sub-items: 'Basic Settings', 'Security', 'Network Interfaces', 'Routing', 'Voice Gateway' (highlighted), 'Payload', and 'Statistics'. The main content area is titled 'H.323 Stack Parameters' and displays two configuration items: 'Basic User Input String for Outband Signaling: Enabled' and 'User Input for DTMF Outband Signaling: Enabled'.

To view registered H.323 clients, select **Explorers** → **Voice Gateway** → **Clients** → **HFA**.

The screenshot shows the HG 3500 V5 configuration interface. The top navigation bar includes 'Front panel', 'Wizard', 'Explorers' (highlighted), 'Maintenance', 'Help', and 'Logoff'. The left sidebar shows 'Explorers' with sub-items: 'Basic Settings', 'Security', 'Network Interfaces', 'Routing', 'Voice Gateway' (highlighted), 'Payload', and 'Statistics'. The main content area is titled 'HFA System Client' and displays a table of registered clients. The table has columns: Circuit, Locked, Station Number, Authentication required, Circuit Status, IP Address, TLS, and SRT. Below the table is a 'Refresh' button and a checkbox for 'auto refresh' with a timer set to 55 seconds.

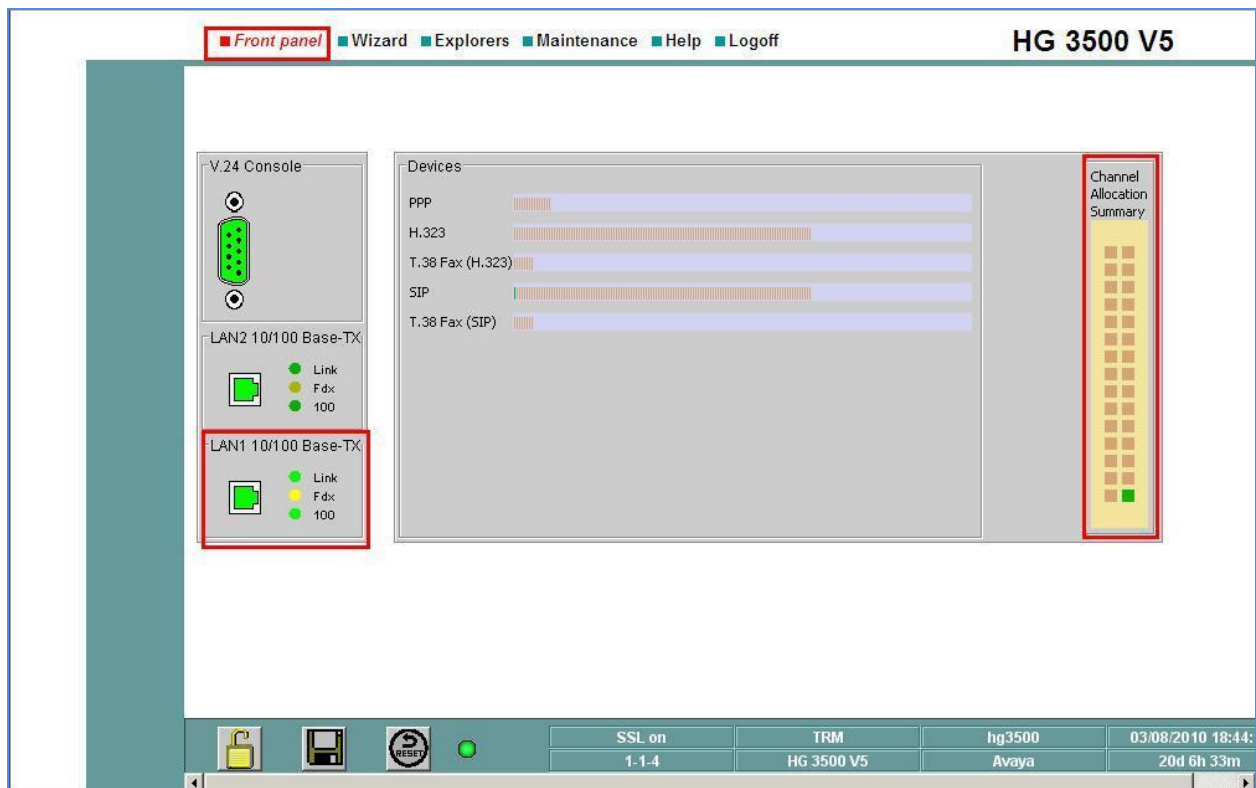
Circuit	Locked	Station Number	Authentication required	Circuit Status	IP Address	TLS	SRT
0	No	810103	Yes	logged	192.168.81.103	No	No
1	No	810104	Yes		0.0.0.0	No	No

## 6. Verification Steps

This section provides details on how to verify network connectivity, the main configuration set-up of Avaya and Siemens phone endpoints and also the SIP Trunk between Avaya and Siemens PBX environments.

### 6.1. Verify Network Connectivity

The HiPath 4000 Communications Server is the central controlling unit in the Siemens PBX set-up. Connection to the HG3500 gateway chassis is via ISDN link. Check the ISDN link light on the front panel of the HG3500 chassis to verify that it displays “green” link light. Connection to the HG3500 IP gateways is via LAN. Verify that the link light on the front of the cards for the LAN1 connection is a “bright green”. (Screen shot below shows lights on for LAN1, but lights off for LAN2 as it is not in use.) Using a PC on the same network, verify ping tests to the SIP Trunk GW, the H.323 GW and the SIP Registrar GW. Each of the Siemens gateways can be accessed via web browser. Use the **Front Panel** tab to view link status and line status. The image below shows the **Front Panel** status for the SIP Trunk gateway. LAN link status is displayed on the bottom left. Channel status is listed on the right, in this example a single call from Siemens to Avaya is active, indicated by the green indicator.



## 6.2. Verify Avaya Phones

List the Station configuration on the Access Element. In these sample notes, there are two stations configured on the Access Element, **Avaya H.323** and **Avaya TDM**.

```
list station
```

STATIONS									
Ext/ Cable/ Hunt-to Jack	Port/ Type	Name/ Surv GK NN	Room/ Data Ext	Cv1/ Cv2	COR/ COS	TN			
23000	01A0401	Digital Phone			1				
	2420		no		1	1			
23100	S00000	AVAYA_H323			1				
	9650		no		1	1			
23200	S00001	Phone, SIP			1				
	9620SIP		no		1	1			
23300	S00004	NORTEL Phone			1				
	9630SIP		no		1	1			
23301	S00002	phone, nortel2			1				
	9630SIP		no		1	1			

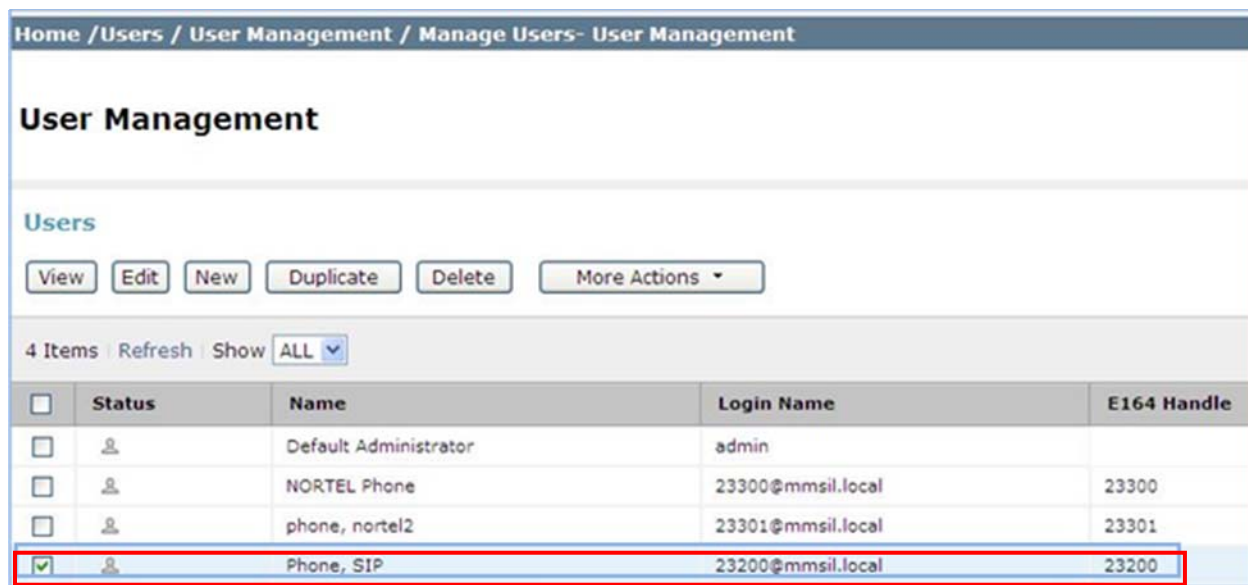
List the registered IP stations using the command **list registered-ip-stations**. The **Avaya H.323** station will be listing here.

```
list registered-ip-stations
```

REGISTERED IP STATIONS				
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt Gatekeeper	Station IP Address/ IP Address
-----	-----	-----	---	-----
-				
23100	9650	IP_Phone	y	10.10.99.13
	1	3.110b		192.168.81.104

The **Avaya SIP** station configuration is created on the Session Manager, which is then pushed down to the **Feature Server**. The station will not show up on **list registered-ip-stations**. Therefore a simple test call to another Avaya Station was carried out to verify connectivity.

The parent configuration for station **34008** was created on the Session Manager. To verify, browse to **Home → Users → User Management → Manage Users → User Management**. Verify that the user is displayed with the correct **User Name** and **Handle**.



The screenshot shows the 'User Management' page with a breadcrumb trail: Home / Users / User Management / Manage Users - User Management. Below the title, there are buttons for View, Edit, New, Duplicate, Delete, and More Actions. A summary bar indicates '4 Items', a 'Refresh' button, and a 'Show ALL' dropdown. The main table lists users with columns for Status, Name, Login Name, and E164 Handle. The last row, 'Phone, SIP', is highlighted with a red box.

	Status	Name	Login Name	E164 Handle
<input type="checkbox"/>		Default Administrator	admin	
<input type="checkbox"/>		NORTEL Phone	23300@mmsil.local	23300
<input type="checkbox"/>		phone, nortel2	23301@mmsil.local	23301
<input checked="" type="checkbox"/>		Phone, SIP	23200@mmsil.local	23200

Carry out a simple test calls between the various Avaya Stations, and verify connection and duplex audio path.

### 6.3. Verify Siemens Phones

To verify the Siemens SIP phone registration status, see **Section 5.3.1.1. SIP Registrar Gateway**. To verify the Siemens H.323 phone registration status, see **Section 5.3.1.2 H.323 Gateway**. Carry out a simple test calls between the various Siemens stations, and verify connection and duplex audio path.

### 6.4. Verify SIP Trunk between Avaya Aura® Session Manager and HiPath SIP Gateway

Use the Session Manager SIP Entity Monitor to verify that SIP Trunk between SM and Siemens HiPath SIP GW. Browse to **Home → Elements → Session Manager → System Status → SIP Entity Monitoring**. From the list of **All Monitored SIP Entities** (not shown), select the SiemensHiPath entity link. Verify that **Conn-Status** is Up.

The screenshot displays the Session Manager SIP Entity Monitor interface. The top section, titled "All Monitored SIP Entities", includes a "Run Monitor" button and a list of two entities: "CM EvolutionServer" and "SiemensHipath". A "Select : All, None" option is also present. An arrow points from the "SiemensHipath" link to the bottom section, titled "All Entity Links to SIP Entity: SiemensHipath". This section shows a "Summary View" of the entity links, with a table containing one item. The table has columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The data row shows "Session Manager" with IP "192.168.81.6", Port "5060", Proto. "UDP", Conn. Status "Up", Reason Code "200 OK", and Link Status "Up".

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Session Manager	192.168.81.6	5060	UDP	Up	200 OK	Up

## 7. Conclusion

The interoperability between Siemens HiPath 4000 V5 with an IP Communications Solution and Avaya Aura® Communication Manager with Avaya Aura® Session Manager did function. However some issues were detected.

### 7.1. Issues detected on all Siemens Endpoints.

This section provides details on the issues detected during interoperability testing, which were general to the Siemens Phone models 410s, 420s and 500 and OpenStage SIP.

#### 7.1.1. IP Shuffling

Intermittently one-way audio experienced when a call is put on hold from either Avaya or Siemens devices. When the Siemens handsets (H.323 or SIP) dialed the Avaya H.323 handset the connection would only be made between Siemens HiPath and the Avaya Media Processor card, not using IP Shuffle. In this event the audio would function correctly until either end put the call on hold. On retrieving the call, one way Audio would be experienced between Siemens to Avaya, but not between Avaya to Siemens.

#### 7.1.2. Cross PBX transfer using Unattended or Attended Transfer

Caller Name/ID not updated on Siemens endpoint when transfer is completed by the Avaya endpoint. When the transfer complete step is carried out, the caller display on the Siemens endpoint retains the initial Caller Name/ID instead of updated to the “transfer-to” Caller Name/ID.

#### 7.1.3. Cross PBX transfer using Unattended or Attended Transfer Fails

Transfer request is from Avaya to Siemens endpoint which then attempts to transfer the call back to an Avaya endpoint, the feature fails consistently. The issue occurs when the Siemens endpoint attempt an un-attended or attended transfer. Each of the endpoints reports error message:

- Siemens 410s H323 IP Phone “Not Possible”,
- Siemens 420s SIP IP Phone “488 Not Acceptable Here”,
- Siemens 500s TDM Phone “Not Possible”.

#### 7.1.4. Siemens SIP Devices using Call Forward Busy

When attempting to dial a Siemens SIP device which has Call Forward Busy programmed and the device is busy, the caller receives a busy signal, rather than follow the forward busy setting. Under tracing conditions, a busy signal is issued by the Siemens device and can be traced in Wireshark as **SIP Status Message 486 Busy Here**. The tests for Call Forward No Answer and Always were successful and the calls were forwarded to the forwarding destination successfully, both Avaya handset and Siemens Device.

#### 7.1.5. Call forwarding fails when the forwarded call is picked up

Call Forwarding Always is configured on the Avaya endpoint to either Siemens or Avaya destination. When the Siemens device rings the Avaya handset, the call is forwarded, however call completion fails when the line is picked up at the “forwarded-to endpoint”.

A **BYE** sent from the SIP Gateway to Avaya Aura® Session Manager contains a message ***“Resource unavailable, unspecified”***. The Call Forward No Answer/Reply and Call Forward Busy programmed on the Avaya device work successfully.

## **7.2. Issues detected on Siemens 420S SIP Phone only**

This section provides details on the issues detected during interoperability testing, which are isolated to the Siemens phone model 420S (SIP).

### **7.2.1. Call Hold / Reconnect Fail on Siemens 420s SIP phone**

This issue is isolated to the Siemens HiPath 420s SIP Phone. Independent of where the call is from Avaya or Siemens. When the 420s SIP user selects “Reconnect” on a line that is in a “Hold” state the reconnect fails to work. Wire shark trace from Siemens SIP Phone indicates **488 “Not Acceptable Here”** response from SIP Gateway to Siemens SIP Endpoint, after attempting to retrieve the call. Call is cleared. SIP Signaling and SIP Call Control logs were captured from the Siemens 420s SIP Phone. Log message **“state = ccCallHoldFeatureRejected, reason = Unreachable : 1195”** is generated. The line is then cleared.

**Workaround:** This issue can be resolved with the programming of a Line key on the handset, either via accessing the Web Based Management tool for the handset, or via the Siemens DLS (Deployment Server) Software, which may have been installed for SIP phone management. This key allows a held call to be retrieved by the user.

### **7.2.2. Blind Transfer Fail on Siemens 420s SIP Phone**

The 420S SIP user selects Blind Transfer, a valid phone number of another Siemens endpoint was entered, and Dial was selected. The attempted dial fails, Reconnect option is displayed. The 420s SIP user select Reconnect, this also fails and the line is cleared. Wire shark trace from Siemens SIP Phone. Notify message from the SIP registration Gateway shows SIP error code **503 “Service Unavailable”**. SIP Signaling and SIP Call Control logs were captured from the Siemens 420s SIP Phone. Log message **“ccFeatureFailed, feature = ccTransfer, reason = Transfer\_Rejected”**. No suitable workaround has been found to resolve the issue.



## 8. Additional References

Product Documentation for Avaya Products may be found at <http://support.avaya.com>

- [1] Administering Avaya Aura®™ Communication Manager 03-300509 Release 6.0 Issue 6.0
- [2] Administering Avaya Aura® Communication Manager Server Options 03-603479 Release 6.0.1, Issue 2.2
- [3] Administering Avaya Aura® Session Manager 03-603324 Release 6.1 Issue 1.0
- [4] Maintaining and Troubleshooting Avaya Aura® Session Manager 03-603325 Release 6.1 Issue 4.1

Product Documentation for Siemens Products may be found the following websites and service manuals.

- [5] Siemens Wiki Website [http://wiki.siemens-enterprise.com/index.php/Main\\_Page](http://wiki.siemens-enterprise.com/index.php/Main_Page)
- [6] Siemens eTAC (a support website with limited information available to customer/end user) [7] <http://siemenstac.custhelp.com/app/home>
- [7] HiPath 4000 V5 IP Solutions, SIP Connectivity Service Documentation ref: A31003-H3150-S104-2-7620 Dec 2008.
- [8] Other Service Documentation may be obtained via your Service Support Provider or Account Manager within Siemens Enterprise Communications.

---

**©2011 Avaya Inc. All Rights Reserved.**

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)