



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

---

# **Application Notes for configuring Syntec CardEasy with Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration required to allow Syntec CardEasy to interoperate with Avaya Aura® Communication Manager using two separate connections, a SIP trunk connection to Avaya Session Border Controller for Enterprise and a TSAPI connection to Avaya Aura® Application Enablement Services. Syntec CardEasy allows customers to securely enter credit card details during a transaction with an agent and have the payment authorized and confirmed.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as any observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect Compliance Testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration used to verify Syntec CardEasy interoperates with Avaya Session Border Controller for Enterprise R8.0, Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Application Enablement Services R8.0.1. The solution outlined in these Application Notes describe two unique and separate connections between the CardEasy solution from Syntec and the Avaya solution consisting of the devices listed in **Section 4**.

CardEasy uses a SIP trunk connection to the Avaya Session Border Controller for Enterprise and a TSAPI connection to Avaya Aura® Application Enablement Services. Both of these connections are required in order for the CardEasy solution to interoperate with the Avaya solution and therefore both must be included in the same Application Notes.

The CardEasy Session Border Controller is placed in between a Service Provider and Avaya Aura® Communication Manager to allow Avaya Aura® Communication Manager agents to initiate a credit card payment and for a customer to enter credit card details securely during a transaction. CardEasy masks DTMF digits during the credit card verification process. Avaya Aura® Application Enablement Services is used to identify the Agent called.

CardEasy offers three deployment models.

- Network hosted
- On-premise for ISDN or SIP
- Cloud

**Note:** The on-premise SIP deployment was tested during compliance testing.

In the case of the on-premise deployment model, CardEasy hardware is located on the merchant's premises installed between the incoming SIP trunks and the PBX system. All inbound and outbound calls are routed via the CardEasy hardware which acts as a DTMF capture device. CardEasy has no requirement for hardware to be attached to agents' phones or PCs. The CardEasy hardware captures the PAN and CV2 entered by the customer using their telephone keypad, with the agent remaining in conversation with the customer throughout. This data is conveyed to the CardEasy cloud over a secure connection, where it is processed before forwarding to the PSP for authorization, returning the result to the agent (and back office systems if required) in real-time. CardEasy is a fully managed service from Syntec.

How does CardEasy work.

1. A caller wishes to pay by card over the phone.
2. The contact center agent initiates a request for card authorization in mid-conversation with the caller.
3. The caller is prompted to enter their card numbers via their telephone keypad (DTMF/ Dual Tone Multi Frequency touch tones, which are masked).
4. Audio from the agent to the caller remains open throughout.

5. Audio from the caller to the agent is cut briefly while they enter the middle six digits of their long card number (PAN) and CV2 on their phone keypad, to ensure that the agent (and call recording) cannot be exposed to the card numbers even if the caller reads out the numbers whilst entering them.
6. The complete call can be recorded as the sensitive DTMF tones are masked from the recording also.
7. The agent is alerted via their screen when payment has been authorized.

## 2. General Test Approach and Test Results

The Syntec CardEasy solution setup for compliance testing consisted of two separate servers using two unique connections to the Avaya solution. The CardEasy Session Border Controller connects to the Avaya Session Border Controller for Enterprise and the CardEasy EPID server connects to the Avaya Aura® Application Enablement Services. The general test approach was to configure CardEasy to communicate with the Avaya Session Border Controller for Enterprise (Avaya SBCE) and Communication Manager via SIP trunks. The Syntec CardEasy EPID application was connected to the AES and was used to identify the called agent. Testing was performed by calling inbound to a VDN and using Vectors to allow the calling party to speak to an agent and enter credit card details and have a payment authorized during a transaction. The DTMF digits credit card details are masked and hidden from the agent and confirmation is sent to the agent's payment page.

A simulated PSTN was created using another Communication Manager to route calls to the CardEasy Session Border Controller, the calls were then passed onto the Avaya SBCE and then onto Session Manager and Communication Manager where the call is answered by the agent, this is outlined in the diagram in **Section 3**.

Compliance testing was carried out using Communication Manager Elite agents. However this should work for Avaya Aura® Contact Center agents also as the logic in the CardEasy program connecting to AES looks to see if the address is associated with an agent ID (either Elite or AACC) and if so, uses that ID instead of the extension number for correlation with the number entered in the EPID box in the Virtual terminal web page.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is

the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and CardEasy did not include use of any specific encryption features as requested by Syntec.

## **2.1 Interoperability Compliance Testing**

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on verifying that CardEasy is capable of connecting successfully to both the Avaya SBCE and the AES in order to process credit card transactions with the DTMF digits of the credit card details being masked and hidden from the agent. Seen as there are two connections to the Avaya solution both of these connections must be tested, and the following calls were made to achieve this.

- Basic SIP calls.
- Hold Transfer and Conference SIP calls.
- Calls to agents, calls from agents.
- Credit card transaction with valid and invalid details.
- Credit card transaction calling to the VDN, direct to the extension and direct to the agent.
- Credit card transaction being transferred to the VDN, direct to the extension and direct to the agent.
- Credit card transaction calling outbound from the agent to the customer.
- Serviceability tests – testing the behaviour of the CardEasy solution during simulated LAN failures.

## **2.2 Test Results**

All test cases passed successfully.

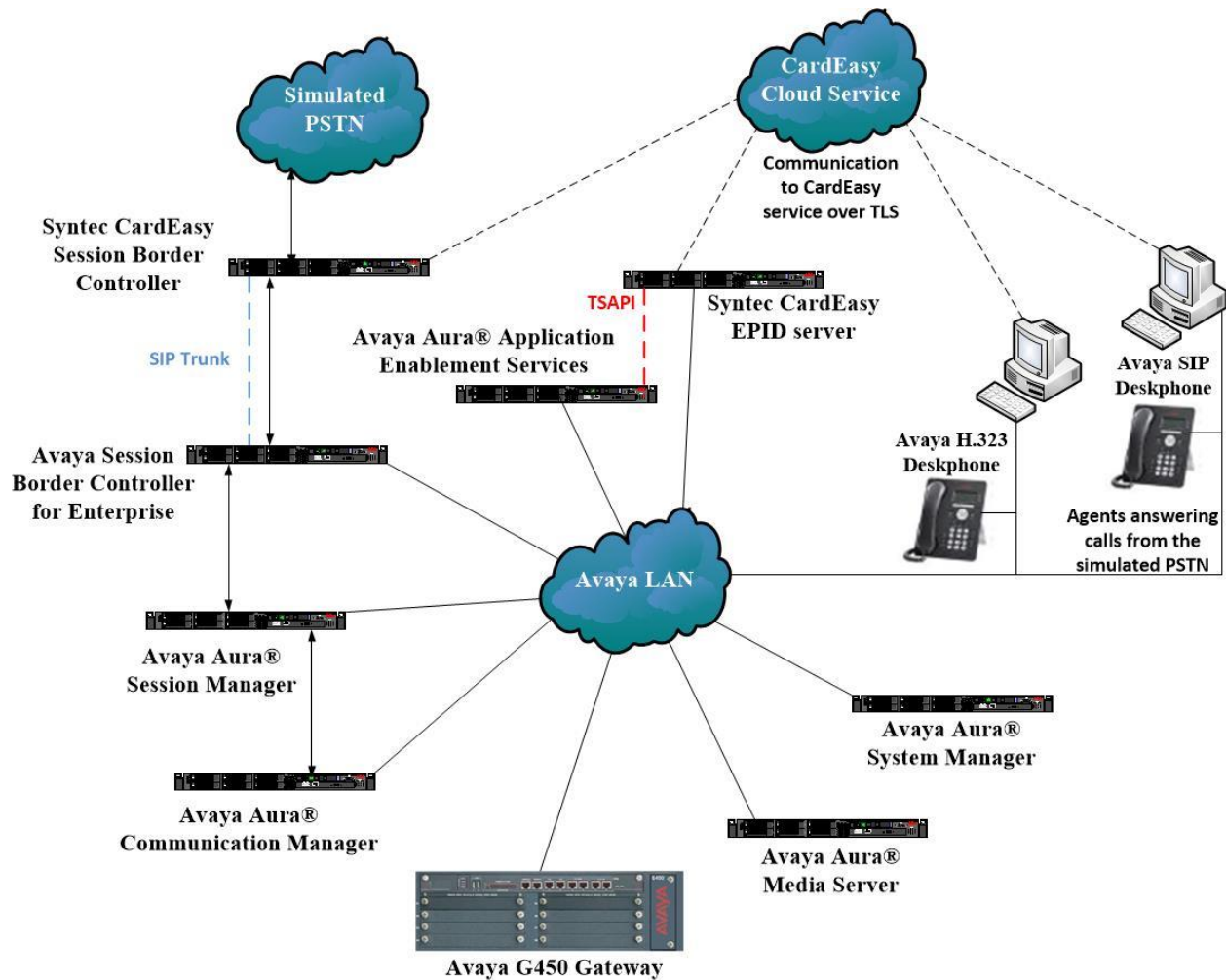
## **2.3 Support**

Technical support can be obtained for Syntec products as follows.

- Email: support@syntec.co.uk
- Website: <https://support.syntec.co.uk/portal/syntec>
- Phone: +44 (0) 207 741 8000

### 3. Reference Configuration

**Figure 1** shows the setup for compliance testing CardEasy with Communication Manager and Session Manager using SIP signalling over SIP trunks to pass callers through the CardEasy SBC and onto Communication Manager agents.



**Figure 1: Connection of CardEasy from Syntec with Avaya Session Border Controller for Enterprise and Avaya Aura® Application Enablement Services**

## 4. Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

| Avaya Equipment   | Software / Firmware Version   |
|---|---|
| Avaya Session Border Controller for Enterprise (Avaya SBCE) | 8.0.0.0-19-16991  |
| Avaya Aura® System Manager                                  | System Manager 8.0.1.1 Build No. – 8.0.0.0.931077<br>Software Update Revision No: 8.0.11.039340<br>Service Pack 1 |
| Avaya Aura® Session Manager                                 | Session Manager R8.0.1<br>Build No. – 8.0.1.1.801103  |
| Avaya Aura® Communication Manager                           | R8.0.1.1.0 – FP1SP1<br>R018x.00.0.822.0 Update ID 00.0.822.0-25183  |
| Avaya Aura® Application Enablement Services                 | 8.0.1.0.1.5-0   |
| Avaya Media Gateway G450                                    | 40.20.0 /2  |
| Avaya Aura® Media Server                                    | Appliance Version R8.0.0.6<br>Media Server 8.0.0.150<br>Element Manager 8.0.0.150                                 |
| Avaya 96x1 H323 Deskphone                                   | 6.6604  |
| Avaya 96x1 SIP Deskphone                                    | 7.1.2.0.14  |
| Avaya J179 H323 Deskphone                                   | 6.7.002U  |
| Avaya J129 SIP Deskphone                                    | 1.0.0.0.0.43  |
| Avaya Equinox running on Vantage                            | 3.4.8.36  |
| Avaya 9408 Digital Deskphone                                | V2.0  |
| Syntec Equipment  | Software / Firmware Version   |
| Syntec CardEasy SBC   | 2.2.2   |
| Syntec AES EPID Application                                 | 1.0.0   |

**Table 1: Hardware and Software Version Numbers**

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 13**.

The configuration of Communication Manager could be considered as three separate sections.

1. Configuration of the VDN, Vector and Agent for the incoming calls.
2. Configuration of the SIP trunk and call routing.
3. Configuration of the link to AES.

### 5.1 Configuration of the VDN, Vector and Agent

In order for calls to be routed to agents, Hunt Groups (skills), Vectors, and Vector Directory Numbers (VDN) must be configured.

#### 5.1.1 Hunt Groups

Enter the **add hunt-group n** command where **n** in the example below is **90**. On **Page 1** of the **hunt-group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to **y** as shown below.

- **ACD?** to **y**
- **Queue?** to **y**
- **Vector?** to **y**

| add hunt-group 90        |                           | Page 1 of 4 |
|--------------------------|---------------------------|-------------|
| HUNT GROUP               |                           |             |
| Group Number: 90         | ACD? y                    |             |
| Group Name: VoiceSales   | Queue? y                  |             |
| Group Extension: 2800    | Vector? y                 |             |
| Group Type: ucd-mia      |                           |             |
| TN: 1                    |                           |             |
| COR: 1                   | MM Early Answer? n        |             |
| Security Code:           | Local Agent Preference? n |             |
| ISDN/SIP Caller Display: |                           |             |
| Queue Limit: unlimited   |                           |             |
| Calls Warning Threshold: | Port:                     |             |
| Time Warning Threshold:  | Port:                     |             |

On **Page 2**, set the **Skill** field to **y** as shown below.

|                              |  |             |
|------------------------------|--|-------------|
| add hunt-group 90            |  | Page 2 of 4 |
| HUNT GROUP                   |  |             |
| Skill? y                     | Expected Call Handling Time (sec): 180 |             |
| AAS? n                       |  |             |
| Measured: none               |  |             |
| Supervisor Extension:        |  |             |
| Controlling Adjunct: none    |  |             |
| Multiple Call Handling: none |  |             |
| Timed ACW Interval (sec):    | After Xfer or Held Call Drops? n       |             |

Repeat the above steps to create a hunt groups for other inbound services, should they be required.

### 5.1.2 Vectors

Enter the **change vector n** command, where **n** is the vector number. For this test simple routing was used to get the call to the agent. The call is queued to the skill set out on the VDN in the 1st Skill field on the next page.

|                  |                          |                                  |
|------------------|--------------------------|----------------------------------|
| change vector 29 |                          | Page 1 of 6                      |
| CALL VECTOR      |                          |                                  |
| Number: 29       | Name: DevConnect Vector  |                                  |
| Multimedia? y    | Attendant Vectoring? n   | Meet-me Conf? n Lock? n          |
| Basic? y         | EAS? y G3V4 Enhanced? y  | ANI/II-Digits? y ASAI Routing? y |
| Prompting? y     | LAI? y G3V4 Adv Route? y | CINFO? y BSR? y Holidays? y      |
| Variables? y     | 3.0 Enhanced? y          |                                  |
| 01 queue-to      | skill 1st pri m          |                                  |
| 02 wait-time     | 10 secs hearing ringback |                                  |
| 03 stop          |                          |                                  |
| 04               |                          |                                  |
| 05               |                          |                                  |
| 06               |                          |                                  |



### 5.1.3 Vector Directory Numbers (VDN)

Enter the **add vdn n** command, where **n** is an available extension number. On **Page 1** assign a **Name** for the VDN and set the **Vector Number** to the relevant vector. The **1st Skill** should be set to that hunt group configured in **Section 5.1.1**.

|                                   |                                 |
|-----------------------------------|---------------------------------|
| <b>add vdn 2900</b>               | <b>Page 1 of 3</b>              |
| VECTOR DIRECTORY NUMBER           |                                 |
| Extension: 2900                   |                                 |
| Name*: Sales                      |                                 |
| Destination: <b>Vector Number</b> | 29                              |
| Attendant Vectoring? n            |                                 |
| Meet-me Conferencing? n           |                                 |
| Allow VDN Override? n             |                                 |
| COR: 1                            |                                 |
| TN*: 1                            |                                 |
| Measured: none                    | Report Adjunct Calls as ACD*? n |
| VDN of Origin Annc. Extension*:   |                                 |
| 1st Skill*: 90                    |                                 |
| 2nd Skill*:                       |                                 |
| 3rd Skill*:                       |                                 |
| * Follows VDN Override Rules      |                                 |

### 5.1.4 Administer Class of Restriction

Enter the **change cor x** command where **x** corresponds to the Class of Restriction to be used for the agent login IDs in **Section 5.5**. On **Page 1**, set the **Direct Agent Calling** to **y**. This will allow agents to be called directly once they are logged in.

|   |  |
|---|--|
| <b>change cor 1</b>                         | <b>Page 1 of 23</b>                    |
| CLASS OF RESTRICTION                        |  |
| COR Number: 1                               |  |
| COR Description: DefaultCOR_PG              |  |
| FRL: 7                                      | APLT? y                                |
| Can Be Service Observed? y                  | Calling Party Restriction: none        |
| Can Be A Service Observer? y                | Called Party Restriction: none         |
| Time of Day Chart: 1                        | Forced Entry of Account Codes? n       |
| Priority Queuing? n                         | <b>Direct Agent Calling? y</b>         |
| Restriction Override: none                  | Facility Access Trunk Test? n          |
| Restricted Call List? n                     | Can Change Coverage? n                 |
| Access to MCT? y                            | Fully Restricted Service? n            |
| Group II Category For MFC: 7                | Hear VDN of Origin Annc.? n            |
| Send ANI for MFE? n                         | Add/Remove Agent Skills? n             |
| MF ANI Prefix:                              | Automatic Charge Display? n            |
| Hear System Music on Hold? y                | PASTE (Display PBX Data on Phone)? n   |
| Can Be Picked Up By Directed Call Pickup? y | Can Use Directed Call Pickup? y        |
|   | Group Controlled Restriction: inactive |

### 5.1.5 Administer Agent Logins

Enter the **add agent-loginID n** command; where **n** is an available extension number. Enter a descriptive name for the agent in the **Name** field. Ensure the **COR** field is set to **1** which relates to the COR configured in **Section 5.1.4**. The **Auto Answer** field is set to **station** except for those logins that will be used for outbound services. In that case, the field will be set to **all**. Configure a password as required.

|   |                                      |             |
|---|--------------------------------------|-------------|
| add agent-loginID 4405                                      |                                      | Page 1 of 2 |
| AGENT LOGINID   |                                      |             |
| Login ID: 4405  | AAS? n                               |             |
| Name: Agent1  | AUDIX? n                             |             |
| TN: 1   | Check skill TNs to match agent TN? n |             |
| COR: 1  |                                      |             |
| Coverage Path:  | LWC Reception: spe                   |             |
| Security Code:  | LWC Log External Calls? n            |             |
| Attribute:  | AUDIX Name for Messaging:            |             |
| LoginID for ISDN/SIP Display? n                             |                                      |             |
| Password:   |                                      |             |
| Password (enter again):                                     |                                      |             |
| Auto Answer: station  |                                      |             |
| AUX Agent Remains in LOA Queue: system                      | MIA Across Skills: system            |             |
| AUX Agent Considered Idle (MIA): system                     | ACW Agent Considered Idle: system    |             |
| Work Mode on Login: system                                  | Aux Work Reason Code Type: system    |             |
|   | Logout Reason Code Type: system      |             |
| Maximum time agent in ACW before logout (sec): system       |                                      |             |
| Forced Agent Logout Time: :                                 |                                      |             |
| WARNING: Agent must log in again before changes take effect |                                      |             |

On **Page 2**, assign a skill to the agent by entering the relevant hunt group number created in **Section 5.1.1** for **SN** and entering a skill level of **1** for **SL**. In this case, an agent is able to handle both inbound and outbound calls is created. Set the **Direct Agent Skill** to the Inbound hunt group **90**.

|                                       |       |                          |
|---------------------------------------|-------|--------------------------|
| change agent-loginID 4405             |       | Page 2 of 2              |
| AGENT LOGINID                         |       |                          |
| Direct Agent Skill: 90                |       | Service Objective? n     |
| Call Handling Preference: skill-level |       | Local Call Preference? n |
| SN                                    | RL SL | SN RL SL                 |
| 1: 90                                 | 1     | 16:                      |
| 2:                                    |       | 17:                      |
| 3:                                    |       | 18:                      |
| 4:                                    |       | 19:                      |
| 5:                                    |       | 20:                      |
| 6:                                    |       |                          |
| 7:                                    |       |                          |

Repeat this task accordingly for any additional inbound or outbound agents required.

## 5.1.6 Administer Agent Stations

For each station that agents will log in to, enter the command **change station n**, where **n** is the station extension. On **Page 1** ensure that **IP SoftPhone** is set to **y** as shown below.

|                           |  |             |
|---------------------------|--|-------------|
| change station 4000       |  | Page 1 of 5 |
| STATION                   |  |             |
| Extension: 4000           | Lock Messages? n                             | BCC: 0      |
| Type: 9608                | Security Code: *                             | TN: 1       |
| Port: S00000              | Coverage Path 1: 2                           | COR: 1      |
| Name: 4000, H323User      | Coverage Path 2:                             | COS: 1      |
|                           | Hunt-to Station:                             | Tests? n    |
| STATION OPTIONS           |  |             |
| Loss Group: 19            | Time of Day Lock Table:                      |             |
|                           | Personalized Ringing Pattern: 1              |             |
|                           | Message Lamp Ext: 4000                       |             |
| 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? y                              |             |
|                           | IP Video Softphone? n                        |             |
|                           | Short/Prefixed Registration Allowed: default |             |
|                           | Customizable Labels? y                       |             |

On **Page 4**, the following buttons must be assigned as shown below:

- **aux-work** – Agent is logged in to the ACD but is not available to take a call.
- **manual-in** – Agent is available to accept ACD calls.
- **after-call** – Agent state after the ACD call is completed. The agent is not available.
- **release** – State when the call is dropped.

|                     |                      |             |
|---------------------|----------------------|-------------|
| change station 4000 |                      | Page 4 of 5 |
| STATION             |                      |             |
| SITE DATA           |                      |             |
| Room:               | Headset? n           |             |
| Jack:               | Speaker? n           |             |
| Cable:              | Mounting: d          |             |
| Floor:              | Cord Length: 0       |             |
| Building:           | Set Color:           |             |
| ABBREVIATED DIALING |                      |             |
| List1:              | List2:               | List3:      |
| BUTTON ASSIGNMENTS  |                      |             |
| 1: call-appr        | 5: <b>manual-in</b>  | Grp:        |
| 2: call-appr        | 6: <b>after-call</b> | Grp:        |
| 3: call-appr        | 7: <b>release</b>    |             |
| 4: <b>aux-work</b>  | 8::                  |             |
| RC:                 | Grp:                 |             |

**Note:** The same changes should be made on a SIP station. Changes to SIP stations are made using System Manager (not shown).

## 5.2 Configuration of the SIP Trunk and Call Routing

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- System Features and Access Codes
- Administer Dial Plan
- Administer Route Selection for outgoing calls
- Configure SIP Trunk

**Note:** The configuration of the simulated PSTN is outside the scope of these Application Notes.

### 5.2.1 Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that the **Maximum Administered SIP Trunks** have sufficient capacity. Each call uses a minimum of one SIP trunk.

| display system-parameters customer-options              |  | Page         | 2 of 11    |
|---|--|--------------|------------|
| OPTIONAL FEATURES                                       |  |              |            |
| IP PORT CAPACITIES                                      |  | USED         |            |
| Maximum Administered H.323 Trunks:                      |  | 12000        | 250        |
| Maximum Concurrently Registered IP Stations:            |  | 18000        | 2          |
| 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>319</b> |
| Maximum Administered Ad-hoc Video Conferencing Ports:   |  | 24000        | 0          |

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

| display system-parameters customer-options |          | Page                              | 3 of 11 |
|--|----------|-----------------------------------|---------|
| OPTIONAL FEATURES                          |          |                                   |         |
| Abbreviated Dialing Enhanced List?         | y        | Audible Message Waiting?          | y       |
| Access Security Gateway (ASG)?             | n        | Authorization Codes?              | y       |
| Analog Trunk Incoming Call ID?             | y        | CAS Branch?                       | n       |
| A/D Grp/Sys List Dialing Start at 01?      | y        | CAS Main?                         | n       |
| Answer Supervision by Call Classifier?     | y        | Change COR by FAC?                | n       |
| <b>ARS?</b>                                | <b>y</b> | Computer Telephony Adjunct Links? | y       |
| <b>ARS/AAR Partitioning?</b>               | <b>y</b> | Cvg Of Calls Redirected Off-net?  | y       |
| ARS/AAR Dialing without FAC?               | y        | DCS (Basic)?                      | y       |

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

|  |   |                                  |          |
|--|---|----------------------------------|----------|
| display system-parameters customer-options |   | Page                             | 5 of 11  |
| OPTIONAL FEATURES                          |   |                                  |          |
| Multinational Locations?                   | n | Station and Trunk MSP?           | y        |
| Multiple Level Precedence & Preemption?    | n | Station as Virtual Extension?    | y        |
| Multiple Locations?                        | n |                                  |          |
| Personal Station Access (PSA)?             | y | System Management Data Transfer? | n        |
| PNC Duplication?                           | n | Tenant Partitioning?             | y        |
| Port Network Support?                      | y | Terminal Trans. Init. (TTI)?     | y        |
| Posted Messages?                           | y | Time of Day Routing?             | y        |
|  |   | TN2501 VAL Maximum Capacity?     | y        |
|  |   | <b>Uniform Dialing Plan?</b>     | <b>y</b> |
| Private Networking?                        | y | Usage Allocation Enhancements?   | y        |

### 5.2.2 System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 13** for supporting documentation.

|  |  |      |         |
|--|--|------|---------|
| display system-parameters features                                   |  | Page | 1 of 19 |
| FEATURE-RELATED SYSTEM PARAMETERS                                    |  |      |         |
| Self Station Display Enabled? n                                      |  |      |         |
| <b>Trunk-to-Trunk Transfer: all</b>                                  |  |      |         |
| 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                         |  |      |         |
| Abbreviated Dial Programming by Assigned Lists? n                    |  |      |         |
| Auto Abbreviated/Delayed Transition Interval (rings): 2              |  |      |         |
| Protocol for Caller ID Analog Terminals: Bellcore                    |  |      |         |
| Display Calling Number for Room to Room Caller ID Calls? n           |  |      |         |

The integration relies on the Avaya Universal Call ID which appears as a value in the SIP User-To-User header or in the UII information element in ISDN systems. To enable CardEasy to work properly with AES it is necessary to configure the UCID on **Page 5** of the system-parameters features. **Create Universal Call ID (UCID)** is set to **y**, **UCID Network Node ID** was set to **59** for this system and **Copy UCID for Station Conference/Transfer** is also set to **y**.

```
display system-parameters features                                     Page 5 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                      Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name: CM80vmpg
                                Emergency Extension Forwarding (min): 10
                                Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                                COR to Use for DPT: station
                                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
                                Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
                                Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
                                Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 59
  Copy UCID for Station Conference/Transfer? y
```

SIP trunks always send UCID so long as it is turned on globally in the system-parameters features as shown below. Ensure that **Send UCID to ASAI** is set to **y** on **Page 13**.

```
change system-parameters features                                     Page 13 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
                                Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

                                Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
                                Zip Tone Burst for Callmaster Endpoints: double

ASAI
                                Copy ASAI UII During Conference/Transfer? n
                                Call Classification After Answer Supervision? y
                                Send UCID to ASAI? y
                                For ASAI Send DTMF Tone to Call Originator? y
                                Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

|  |                   |
|--|-------------------|
| <b>display feature-access-codes</b>                  | Page 1 of 10      |
| FEATURE ACCESS CODE (FAC)                            |                   |
| Abbreviated Dialing List3 Access Code:               |                   |
| Abbreviated Dial - Prgm Group List Access Code:      |                   |
| Announcement Access Code:                            |                   |
| Answer Back Access Code:                             |                   |
| Attendant Access Code:                               |                   |
| <b>Auto Alternate Routing (AAR) Access Code: 8</b>   |                   |
| <b>Auto Route Selection (ARS) - Access Code 1: 9</b> | Access Code 2:    |
| Automatic Callback Activation: *25                   | Deactivation: #25 |

### 5.2.3 Administer Dial Plan

It was decided for compliance testing that all calls to the “PSTN” were calls that began with 351212 and these were to be sent across the SIP trunk to Session Manager and then onto the Session Border Controllers and the simulated PSTN. To achieve this routing, automatic route selection (ARS) will be used to route the calls. The dial plan and ars routing analysis need to be changed to allow this routing.

Type **change dialplan analysis** to make changes to the dial plan. Note that **3** is of call type **udp** which means any numbers beginning with 3 are a part of the uniform dial plan.

change dialplan analysis

DIAL PLAN ANALYSIS TABLE

Location: all

Page 1 of 12

Percent Full: 3

| Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type |
|---------------|--------------|-----------|---------------|--------------|-----------|---------------|--------------|-----------|
| 1             | 4            | udp       | #             | 3            | fac       |               |              |           |
| 2             | 4            | udp       |               |              |           |               |              |           |
| 3             | 4            | udp       |               |              |           |               |              |           |
| 4             | 4            | ext       |               |              |           |               |              |           |
| 5             | 4            | udp       |               |              |           |               |              |           |
| 58            | 5            | ext       |               |              |           |               |              |           |
| 5999          | 4            | ext       |               |              |           |               |              |           |
| 6             | 4            | udp       |               |              |           |               |              |           |
| 6666          | 4            | ext       |               |              |           |               |              |           |
| 7             | 4            | udp       |               |              |           |               |              |           |
| 781           | 5            | ext       |               |              |           |               |              |           |
| 8             | 1            | fac       |               |              |           |               |              |           |
| 9             | 1            | fac       |               |              |           |               |              |           |
| *             | 3            | fac       |               |              |           |               |              |           |
| *8            | 4            | dac       |               |              |           |               |              |           |

## 5.2.4 Administer Route Selection for Outgoing Calls

Use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to **3** will use Automatic Route Selection (ars). No further digits are deleted or inserted. Calls are sent to **ars** for further processing.

|                           |     |     |               |            |      |                 |  |
|---------------------------|-----|-----|---------------|------------|------|-----------------|--|
| change uniform-dialplan 6 |     |     |               |            |      | Page 1 of 2     |  |
| UNIFORM DIAL PLAN TABLE   |     |     |               |            |      | Percent Full: 0 |  |
| Matching Pattern          | Len | Del | Insert Digits | Net        | Conv | Node Num        |  |
| <b>3</b>                  | 4   | 0   |               | <b>ars</b> | n    |                 |  |
| 4                         | 4   | 0   |               | aar        | n    |                 |  |
| 5                         |     |     |               | ars        | n    |                 |  |
|                           |     |     |               |            | n    |                 |  |
|                           |     |     |               |            | n    |                 |  |
|                           |     |     |               |            | n    |                 |  |
|                           |     |     |               |            | n    |                 |  |
|                           |     |     |               |            | n    |                 |  |

Use the **change ars analysis** command to further configure the routing of the dialed digits. Calls to the 'Simulated PSTN' are achieved by dialing **351212455779** and are matched with the ARS entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

|                          |       |     |                |      |      |                 |  |
|--------------------------|-------|-----|----------------|------|------|-----------------|--|
| change aar analysis 6    |       |     |                |      |      | Page 1 of 2     |  |
| AAR DIGIT ANALYSIS TABLE |       |     |                |      |      | Percent Full: 3 |  |
| Location: all            |       |     |                |      |      |                 |  |
| Dialed String            | Total |     | <b>Route</b>   | Call | Node | ANI             |  |
|                          | Min   | Max | <b>Pattern</b> | Type | Num  | Reqd            |  |
| 3                        | 4     | 4   | 1              | aar  |      | n               |  |
| <b>351212455779</b>      | 12    | 12  | <b>1</b>       | lpvt |      | n               |  |
| 65                       | 4     | 4   | 1              | aar  |      | n               |  |
| 7                        | 7     | 7   | 254            | aar  |      | n               |  |
| 8                        | 7     | 7   | 254            | aar  |      | n               |  |
| 9                        | 7     | 7   | 254            | aar  |      | n               |  |
|                          |       |     |                |      |      | n               |  |
|                          |       |     |                |      |      | n               |  |
|                          |       |     |                |      |      | n               |  |
|                          |       |     |                |      |      | n               |  |
|                          |       |     |                |      |      | n               |  |



Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, Route Pattern Number **1** is used to route calls to trunk group (**Grp No**) **1**, this is the SIP Trunk configured in **Section 5.2.5**. The **Numbering Format** was set to **lev0-pvt**.

|                                       |   |   |   |   |   |   |   |      |  |                                   |           |        |  |
|---------------------------------------|---|---|---|---|---|---|---|------|--|-----------------------------------|-----------|--------|--|
| change route-pattern 1                |   |   |   |   |   |   |   |      |  | Page                              | 1 of      | 3      |  |
| Pattern Number: 1                     |   |   |   |   |   |   |   |      |  | Pattern Name: SIP TRUNK           |           |        |  |
| SCCAN? n                              |   |   |   |   |   |   |   |      |  | Secure SIP? n                     |           |        |  |
| Used for SIP stations? n              |   |   |   |   |   |   |   |      |  |                                   |           |        |  |
| Grp FRL NPA Pfx Hop Toll No. Inserted |   |   |   |   |   |   |   |      |  | DCS/ IXC                          |           |        |  |
| No Mrk Lmt List Del Digits            |   |   |   |   |   |   |   |      |  | QSIG                              |           |        |  |
| Dgts                                  |   |   |   |   |   |   |   |      |  | Intw                              |           |        |  |
| 1:                                    | 1 | 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 Sub | Numbering | LAR    |  |
| 0 1 2 M 4 W                           |   |   |   |   |   |   |   |      |  | Request                           | Dgts      | Format |  |
| 1:                                    | y | y | y | y | y | n | n | unre |  | lev0-pvt                          | 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      |        |  |

## 5.2.5 Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**SM80vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

|   |                    |               |
|---|--------------------|---------------|
| <b>display node-names ip</b>  |                    | IP NODE NAMES |
| <b>Name</b>   | <b>IP Address</b>  |               |
| AMS80vmpg   | 10.10.40.61        |               |
| G450  | 10.10.40.14        |               |
| IPOffice  | 10.10.40.25        |               |
| NRS   | 10.10.40.101       |               |
| PGDECT  | 10.10.40.50        |               |
| <b>SM80vmpg</b>   | <b>10.10.40.58</b> |               |
| SM_Oceana   | 10.10.41.26        |               |
| aes80vmpg   | 10.10.40.56        |               |
| default   | 0.0.0.0            |               |
| <b>procr</b>  | <b>10.10.40.59</b> |               |
| ( 16 of 18 administered node-names were displayed )                           |                    |               |
| Use 'list node-names' command to see all the administered node-names          |                    |               |
| Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name |                    |               |

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 7.1.1**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

```

display ip-network-region 1                                     Page 1 of 20
IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: devconnect.local
Name: Default region
MEDIA PARAMETERS
  Codec Set: 1      Intra-region IP-IP Direct Audio: yes
                   Inter-region IP-IP Direct Audio: yes
                   UDP Port Min: 2048      IP Audio Hairpinning? n
                   UDP Port Max: 3329
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      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5

```

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to the Simulated PSTN. The form is accessed via the **display ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G729A** which are supported by the PSTN.

**Media Encryption** is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate any extension not capable of handling encryption.

```

display ip-codec-set 1                                         Page 1 of 2
IP MEDIA PARAMETERS
Codec Set: 1
Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711A      n          2          20
2: G.711MU     n          2          20
3: G.729A     n          2          20
4:
5:
Media Encryption      Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: none
3:

```

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, **tls** (Transport Layer Security) should be used for DevConnect testing.
- The **Peer Detection Enabled** field should be set to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM80vmppg**), also shown above.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region **1**.
- The **Far-end Domain** field can be set to the domain name specified in the IP Network Region.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

**Note:** These were the settings for compliance testing, however, this trunk may be setup differently on each customer site depending on the customer's requirements for SIP routing.

| change signaling-group 1  |  | Page 1 of 2 |
|---|--|-------------|
| SIGNALING GROUP   |  |             |
| Group Number: 1   | <b>Group Type: sip</b>                   |             |
| IMS Enabled? n  | <b>Transport Method: tls</b>             |             |
| Q-SIP? n  |  |             |
| IP Video? n   | Enforce SIPS URI for SRTP? n             |             |
| <b>Peer Detection Enabled? y</b>  | Peer Server: SM                          |             |
| Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y  |  |             |
| Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n |  |             |
| Alert Incoming SIP Crisis Calls? n  |  |             |
| <b>Near-end Node Name: procr</b>  | <b>Far-end Node Name: SM80vmppg</b>      |             |
| <b>Near-end Listen Port: 5061</b>   | <b>Far-end Listen Port: 5061</b>         |             |
|   | <b>Far-end Network Region: 1</b>         |             |
| <b>Far-end Domain: devconnect.local</b>   |  |             |
| Incoming Dialog Loopbacks: eliminate  | Bypass If IP Threshold Exceeded? n       |             |
| <b>DTMF over IP: rtp-payload</b>  | RFC 3389 Comfort Noise? n                |             |
| Session Establishment Timer(min): 3   | <b>Direct IP-IP Audio Connections? y</b> |             |
| 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            |             |

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from the PSTN. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

| change trunk-group 1     |                                | Page 1 of 5    |                  |
|--------------------------|--------------------------------|----------------|------------------|
| TRUNK GROUP              |                                |                |                  |
| Group Number: 1          | <b>Group Type: sip</b>         | CDR Reports: y |                  |
| Group Name: SIPTRUNK     | COR: 1                         | TN: 1          | <b>TAC: *801</b> |
| Direction: two-way       | Outgoing Display? n            |                |                  |
| Dial Access? n           | Night Service:                 |                |                  |
| Queue Length: 0          |                                |                |                  |
| <b>Service Type: tie</b> | Auth Code? n                   |                |                  |
|                          | Member Assignment Method: auto |                |                  |
|                          | <b>Signaling Group: 1</b>      |                |                  |
|                          | <b>Number of Members: 10</b>   |                |                  |

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Syntec to prevent unnecessary SIP messages during call setup. For the compliance test a value of **600** was used.

| change trunk-group 1  |   | Page 2 of 5 |  |
|---|---|-------------|--|
| Group Type: sip   |   |             |  |
| TRUNK PARAMETERS  |   |             |  |
| Unicode Name: auto  |   |             |  |
| Redirect On OPTIM Failure: 5000                                 |   |             |  |
| SCCAN? n  | Digital Loss Group: 18                                      |             |  |
|   | <b>Preferred Minimum Session Refresh Interval(sec): 600</b> |             |  |
| Disconnect Supervision - In? y Out? y                           |   |             |  |
| XOIP Treatment: auto  | Delay Call Setup When Accessed Via IGAR? n                  |             |  |
| Caller ID for Service Link Call to H.323 1xC: station-extension |   |             |  |

Settings on **Page 3** are as follows. These are the values used during compliance testing. The **UII Treatment** was set to **shared** and the **Send UCID** parameter is set to **y**.

|   |                                   |
|---|-----------------------------------|
| change trunk-group 1                                  | Page 3 of 5                       |
| TRUNK FEATURES  |                                   |
| ACA Assignment? n                                     | Measured: none                    |
|   | Maintenance Tests? y              |
| Suppress # Outpulsing? n    Numbering Format: private |                                   |
|   | <b>UII Treatment: shared</b>      |
|   | Maximum Size of UII Contents: 128 |
|   | Replace Restricted Numbers? n     |
|   | Replace Unavailable Numbers? n    |
|   | Hold/Unhold Notifications? y      |
|   | Modify Tandem Calling Number: no  |
| <b>Send UCID? y</b>                                   |                                   |
| Show ANSWERED BY on Display? y                        |                                   |
| DSN Term? n   |                                   |

Settings on **Page 4** are as follows. The **Universal Call ID (UCID)** priority is set to **2**. If set to a lower priority, it's possible that the UCID can be lost if there is a lot of data being sent in the UII field.

|                                    |             |
|------------------------------------|-------------|
| change trunk-group 1               | Page 4 of 5 |
| SHARED UII FEATURE PRIORITIES      |             |
| ASAI: 1                            |             |
| <b>Universal Call ID (UCID): 2</b> |             |
| MULTI SITE ROUTING (MSR)           |             |
| In-VDN Time: 3                     |             |
| VDN Name: 4                        |             |
| Collected Digits: 5                |             |
| Other LAI Information: 6           |             |
| Held Call UCID: 7                  |             |

Settings on **Page 5** are as follows.

|   |                    |
|---|--------------------|
| change trunk-group 1  | <b>Page 5 of 5</b> |
| PROTOCOL VARIATIONS   |                    |
| Mark Users as Phone? n  |                    |
| Prepend '+' to Calling/Alerting/Diverting/Connected Number? n         |                    |
| Send Transferring Party Information? y                                |                    |
| Network Call Redirection? y   |                    |
| Build Refer-To URI of REFER From Contact For NCR? n                   |                    |
| Send Diversion Header? n  |                    |
| Support Request History? y  |                    |
| Telephone Event Payload Type: 101                                     |                    |
| Convert 180 to 183 for Early Media? n                                 |                    |
| Always Use re-INVITE for Display Updates? n                           |                    |
| Identity for Calling Party Display: P-Asserted-Identity               |                    |
| Block Sending Calling Party Location in INVITE? n                     |                    |
| Accept Redirect to Blank User Destination? n                          |                    |
| Enable Q-SIP? n   |                    |
| Interworking of ISDN Clearing with In-Band Tones: keep-channel-active |                    |
| Request URI Contents: may-have-extra-digits                           |                    |

## 5.3 Configure the link to the Avaya Aura® Application Enablement Services

The configuration operations described in this section can be summarized as follows:

- Note procr IP Address
- Configure Transport Link
- Configure CTI Link for TSAPI Service

### 5.3.1 Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP Address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes80vmpg**).

|                       |                    |               |
|-----------------------|--------------------|---------------|
| display node-names ip |                    | Page 1 of 2   |
|                       |                    | IP NODE NAMES |
| Name                  | IP Address         |               |
| SM100                 | 10.10.40.58        |               |
| <b>aes80vmpg</b>      | <b>10.10.40.56</b> |               |
| default               | 0.0.0.0            |               |
| g450                  | 10.10.40.15        |               |
| <b>procr</b>          | <b>10.10.40.59</b> |               |

### 5.3.2 Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**.
- **Enabled:** set to **y**.
- **Local Node:** set to the node name assigned for the **procr** in **Section 5.3.1**.
- **Local Port** Retain the default value of **8765**.

|                    |         |       |       |        |        |        |
|--------------------|---------|-------|-------|--------|--------|--------|
| change ip-services |         |       |       |        | Page   | 1 of 4 |
| IP SERVICES        |         |       |       |        |        |        |
| Service            | Enabled | Local | Local | Remote | Remote |        |
| Type               |         | Node  | Port  | Node   | Port   |        |
| AESVCS             | y       | procr | 8765  |        |        |        |

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes80vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

**Note:** The password entered for **Password** field must match the password on the AES server in **Section 8.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

|                            |                    |          |         |             |
|----------------------------|--------------------|----------|---------|-------------|
| change ip-services         |                    |          |         | Page 4 of 4 |
| AE Services Administration |                    |          |         |             |
| Server ID                  | AE Services Server | Password | Enabled | Status      |
| 1:                         | aes80vmpg          | *****    | y       | idle        |
| 2:                         |                    |          |         |             |
| 3:                         |                    |          |         |             |

## 5.4 Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

|                 |  |             |
|-----------------|--|-------------|
| add cti-link 1  |  | Page 1 of 3 |
| CTI LINK        |  |             |
| CTI Link: 1     |  |             |
| Extension: 2002 |  |             |
| Type: ADJ-IP    |  |             |
| COR: 1          |  |             |
| Name: aes80vmpg |  |             |



## 6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signaling to provide an interface to the CardEasy SBC.

**Note:** There are two interfaces used on the Avaya SBCE one to the CardEasy SBC server and another to Session Manager. It is assumed that the connection and interface to Session Manager is already in place and these Application Notes will focus solely on the connection to CardEasy.

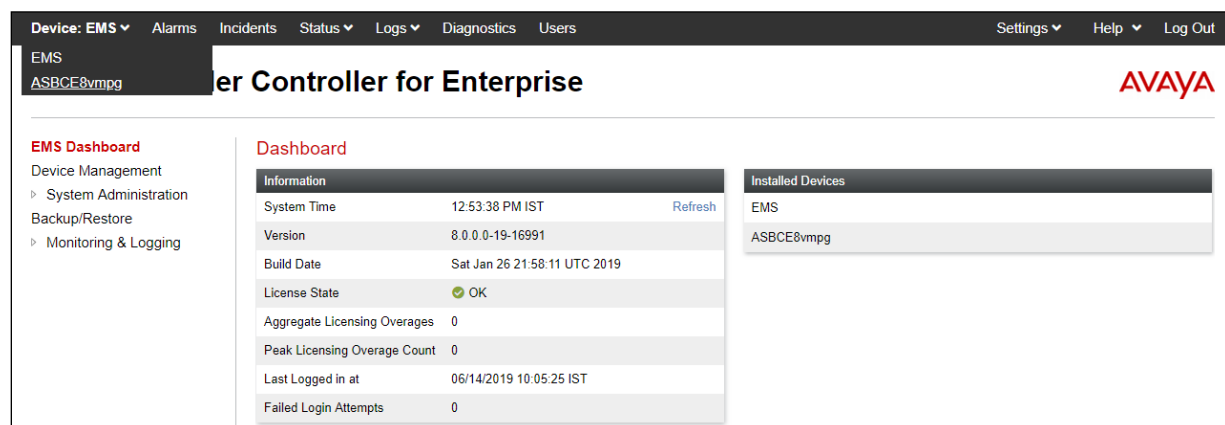
### 6.1 Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



The login page features the Avaya logo in red on the left. To the right, under the heading "Log In", is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, there is a block of text stating: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." This is followed by another paragraph: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." A final line reads: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, it says "© 2011 - 2016 Avaya Inc. All rights reserved."

Once logged in, a dashboard is presented with a menu on the left-hand side. From the top left select the Session Border Controller (**ASBCE8vmpg** as an example below). This is the starting point for all configuration of the Avaya SBCE.



The dashboard has a top navigation bar with links: Device: EMS, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below this, the left sidebar shows "EMS" and "ASBCE8vmpg" under the heading "Session Border Controller for Enterprise". The main content area is titled "Dashboard" and contains two panels. The "Information" panel lists system details: System Time (12:53:38 PM IST), Version (8.0.0.0-19-16991), Build Date (Sat Jan 26 21:58:11 UTC 2019), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (06/14/2019 10:05:25 IST), and Failed Login Attempts (0). The "Installed Devices" panel lists "EMS" and "ASBCE8vmpg".

| Information                  |                              |
|------------------------------|------------------------------|
| System Time                  | 12:53:38 PM IST              |
| Version                      | 8.0.0.0-19-16991             |
| Build Date                   | Sat Jan 26 21:58:11 UTC 2019 |
| License State                | OK                           |
| Aggregate Licensing Overages | 0                            |
| Peak Licensing Overage Count | 0                            |
| Last Logged in at            | 06/14/2019 10:05:25 IST      |
| Failed Login Attempts        | 0                            |

| Installed Devices |
|-------------------|
| EMS               |
| ASBCE8vmpg        |

## 6.2 Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the connection to Session Manager i.e., the internal side and **B1** is used for the external connection. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Network & Flows → Network Management** on the left-hand side and click on **Add** from the main menu.

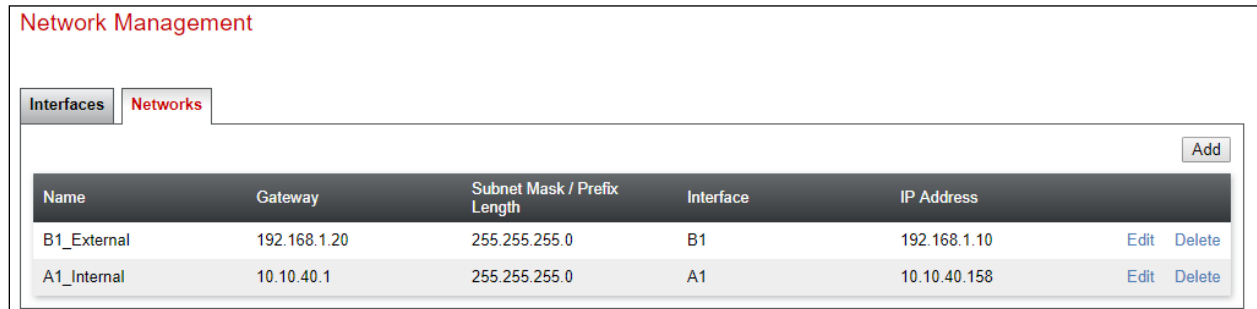
The screenshot shows the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', and 'Network & Flows'. Under 'Network & Flows', 'Network Management' is highlighted. The main area is titled 'Network Management' and contains two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, showing a table with columns: Name, Gateway, Subnet Mask / Prefix Length, Interface, and IP Address. There is one entry: 'A1\_Internal' with Gateway '10.10.40.1', Subnet Mask '255.255.255.0', Interface 'A1', and IP Address '10.10.40.158'. An 'Add' button is in the top right, and 'Edit' and 'Delete' buttons are at the end of the row.

Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field. In the example below this is the IP address of the CardEasy SBC.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The screenshot shows a configuration dialog box. The top section has four fields: 'Name' (B1\_External), 'Default Gateway' (192.168.1.20), 'Network Prefix or Subnet Mask' (255.255.255.0), and 'Interface' (B1). An 'Add' button is at the bottom right of this section. Below is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The first row contains '192.168.1.10', 'Use IP Address', and 'Use Default'. A 'Delete' button is at the end of the row. At the bottom of the dialog is a 'Finish' button.

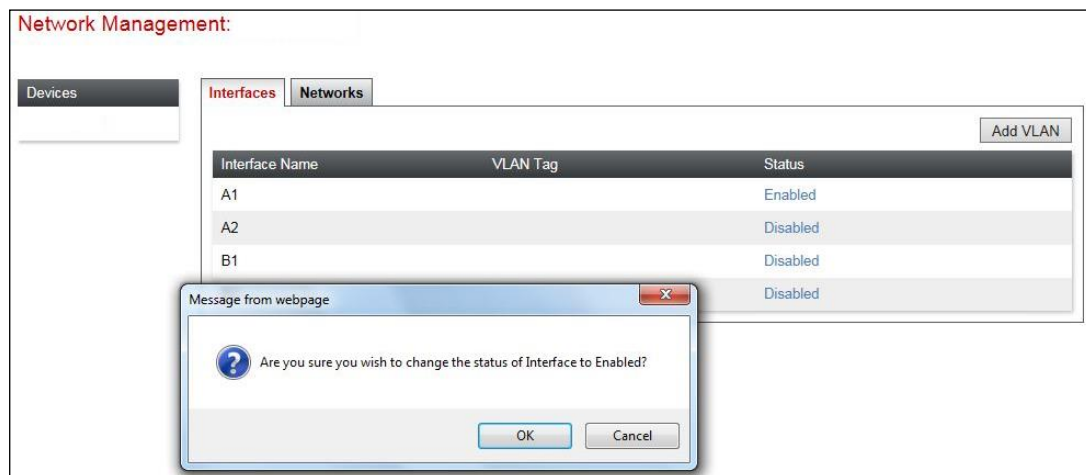
The following screenshot shows the completed **Network Management** configuration:



The screenshot shows the 'Network Management' interface with the 'Networks' tab selected. It displays a table with two network entries. Each entry has 'Edit' and 'Delete' links.

| Name        | Gateway      | Subnet Mask / Prefix Length | Interface | IP Address   |             |
|-------------|--------------|-----------------------------|-----------|--------------|-------------|
| B1_External | 192.168.1.20 | 255.255.255.0               | B1        | 192.168.1.10 | Edit Delete |
| A1_Internal | 10.10.40.1   | 255.255.255.0               | A1        | 10.10.40.158 | Edit Delete |

Select the **Interfaces** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.



**Note:** to ensure that the Avaya SBCE uses the interfaces defined, the Avaya SBCE application must be restarted. Click on **System Management** in the main menu (not shown) and select **Restart Application** indicated by an icon in the status bar (not shown).

## 6.3 Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signaling and media interfaces. Testing was carried out with TCP used for transport of signaling between the Avaya SBCE and CardEasy.

**Note:** All interfaces on the Avaya Enterprise use a secure connection using TLS.

### 6.3.1 Signaling Interfaces

To define the signaling interfaces on the Avaya SBCE, click on **Signaling Interface** on the left-hand side and select **Add**.

| Name    | Signaling IP Network                     | TCP Port | UDP Port | TLS Port | TLS Profile  |
|---------|--|----------|----------|----------|--------------|
| Sig_Int | 10.10.40.158<br>A1_Internal (A1, VLAN 0) | 5060     | ---      | 5061     | SM_Interface |

- In the **Name** field enter a descriptive name for the external signaling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop-down menu is populated with the available IP addresses as defined in **Section 6.2**. In the test environment, this was IP address **192.168.1.10** for the Avaya SBCE interface on the SIP Trunk.
- Enter the TCP port number in the **TCP Port** field, **5060** is used for the CardEasy SBC.
- Click on **Finish**.

Name:

IP Address:

TCP Port:  (Leave blank to disable)

UDP Port:  (Leave blank to disable)

TLS Port:  (Leave blank to disable)

TLS Profile:

Enable Shared Control: ☐

Shared Control Port:

The following screenshot shows details of the signaling interfaces:

| Signaling Interface |  |          |          |          |              |      |        |
|---------------------|--|----------|----------|----------|--------------|------|--------|
| Signaling Interface |  |          |          |          |              | Add  |        |
| Name                | Signaling IP Network                     | TCP Port | UDP Port | TLS Port | TLS Profile  |      |        |
| Sig_Ext             | 192.168.1.10<br>B1_External (B1, VLAN 0) | 5060     | 5060     | ---      | None         | Edit | Delete |
| Sig_Int             | 10.10.40.158<br>A1_Internal (A1, VLAN 0) | 5060     | ---      | 5061     | SM_Interface | Edit | Delete |

### 6.3.2 Media Interfaces

To define the media interfaces on the Avaya SBCE, click on **Media Interface** in the menu on the left-hand side. Details of the RTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signaling. Click on **Add**.

EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

TLS Management

Network & Flows

Network Management

Media Interface

Signaling Interface

Media Interface

| Name    | Media IP Network                         | Port Range    |   |
|---------|--|---------------|---|
| Med_Int | 10.10.40.158<br>A1_Internal (A1, VLAN 0) | 35000 - 40000 | <a href="#">Edit</a> <a href="#">Delete</a> |

Add

- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop-down menu is populated with the available IP addresses as defined in **Section 6.2**. In the test environment, this was IP address **192.168.1.10**.
- Define the RTP **Port Range** for the media path with the CardEasy SBC, during testing this was left at default values of **35000 - 40000**.

|            |   |
|------------|---|
| Name       | Med_Ext   |
| IP Address | <div>B1_External (B1, VLAN 0)</div> <div>192.168.1.10</div> |
| Port Range | 35000 - 40000   |
| Finish     |   |

The following screenshot shows details of the media interfaces:

| Name    | Media IP Network                         | Port Range    |   |
|---------|--|---------------|---|
| Med_Int | 10.10.40.158<br>A1_Internal (A1, VLAN 0) | 35000 - 40000 | <a href="#">Edit</a> <a href="#">Delete</a> |
| Med_Ext | 192.168.1.10<br>B1_External (B1, VLAN 0) | 35000 - 40000 | <a href="#">Edit</a> <a href="#">Delete</a> |

## 6.4 Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the CardEasy SBC is connected as the Trunk Server. To define server interworking on the Avaya SBCE, navigate to **Configuration Profiles** → **Server internetworking** in the menu on the left-hand side. To define Server Interworking for the CardEasy, click on **Add**.

Session Border Controller for Enterprise

EMS Dashboard  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Domain DoS  
**Server Interworking**  
Media Forking

Interworking Profiles: cs2100

Add

Interworking Profiles

- cs2100
- avaya-ru
- Avaya
- Telia

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

Hold Support RFC3264

A pop-up menu is generated. In the **Profile Name** field enter a descriptive name for the CardEasy network and click **Next**.

Interworking Profile X

Profile Name Cardeasy

Next

The general settings are default for Interworking Profile:

Interworking Profile

General

Hold Support

☒ None

☐ RFC2543 - c=0.0.0.0

☐ RFC3264 - a=sendonly

180 Handling

☒ None

☐ SDP

☐ No SDP

181 Handling

☒ None

☐ SDP

☐ No SDP

182 Handling

☒ None

☐ SDP

☐ No SDP

183 Handling

☒ None

☐ SDP

☐ No SDP

Refer Handling

☐

URI Group

None

Send Hold

☒

Delayed Offer

☒

3xx Handling

☐

Diversion Header Support

☐

Delayed SDP Handling

☐

Re-Invite Handling

☐

Prack Handling

☐

Allow 18X SDP

☐

T.38 Support

☐

URI Scheme

☒ SIP

☐ TEL

☐ ANY

Via Header Format

☒ RFC3261

☐ RFC2543

Back

Next

Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

In the final dialogue box, leave the **Record Routes** at the default setting of **Both Sides** and ensure that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk, set the value to **None**. Click on **Finish**



## 6.5 Define Servers

A server definition is required for each server connected to the Avaya SBCE. The CardEasy SBC is connected as a Trunk Server. Session Manager is connected as a Call Server.

To define the CardEasy SBC Server, navigate to **Services → SIP Servers** in the menu on the left-hand side. To define Server Interworking for the CardEasy, click on **Add**.

The screenshot shows the 'SIP Servers: Avaya' configuration page. On the left is a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, SIP Servers (highlighted), LDAP, RADIUS, Domain Policies, Application Rules, and Border Rules. The main area has a tabbed interface with 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced' tabs. The 'General' tab is active, showing 'Server Type' as 'Call Server' and 'DNS Query Type' as 'NONE/A'. Below this is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one entry: IP Address / FQDN: 10.10.3.42, Port: 5060, Transport: TCP. There are 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' buttons.

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 10.10.3.42        | 5060 | TCP       |

Enter an appropriate name in the pop-up menu.

The screenshot shows a pop-up dialog titled 'Add Server Configuration Profile' with a close button (X) in the top right corner. Inside the dialog, there is a 'Profile Name' label followed by a text input field containing the text 'Cardeasy'. Below the input field is a 'Next' button.

Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the CardEasy SBC IP address.
- In the **Port** box, enter the port to be used for the SIP Trunk.
- In the **Transport** drop down menu, select **TCP**.
- Click on **Next**.

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 192.168.1.20      | 5060 | TCP       |

Click on **Next** until the final dialogue box is shown. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for CardEasy SBC defined in **Section 6.4**.
- Leave the other fields at default settings.
- Click **Finish**.

|                               |                          |
|-------------------------------|--------------------------|
| Enable DoS Protection         | <input type="checkbox"/> |
| Enable Grooming               | <input type="checkbox"/> |
| Interworking Profile          | CardEasy                 |
| Signaling Manipulation Script | None                     |
| Securable                     | <input type="checkbox"/> |
| Enable FGDN                   | <input type="checkbox"/> |
| TCP Failover Port             | 5060                     |
| TLS Failover Port             | 5061                     |

## 6.6 Define Routing

Routing information is required for routing to the CardEasy SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signaling. To define routing to CardEasy SBC, navigate to **Global Profiles** → **Routing** in the menu on the left-hand side. Click on **Add**.

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles (selected), Domain DoS, Server Interworking, Media Forking, **Routing** (highlighted), Topology Hiding, and Signaling Manipulation. The main area is titled 'Routing Profiles: default' and includes an 'Add' button. Below this is a list of profiles: default (selected), Avaya, Telia, Cardeasy, and SessionManager. A warning banner states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below the warning is a 'Routing Profile' section with an 'Update Priority' button and a table. The table has columns: Priority, URI Group, Time of Day, Load Balancing, and Next Hop Address. The first row shows Priority '1', URI Group '\*', Time of Day 'default', Load Balancing 'DNS/SRV', and Next Hop Address 'Auto-Detect'.

| Priority | URI Group | Time of Day | Load Balancing | Next Hop Address |
|----------|-----------|-------------|----------------|------------------|
| 1        | *         | default     | DNS/SRV        | Auto-Detect      |

Enter an appropriate name in the dialogue box and click on **Next**.

The screenshot shows a 'Routing Profile' dialog box with a close button (X) in the top right corner. It contains a 'Profile Name' label and a text input field with the text 'Cardeasy' entered. Below the input field is a 'Next' button.

Click on **Next** and enter details for the **Routing Profile** for the SIP Trunk:

- During testing, **Load Balancing** was not required and was left at the default value of **Priority**.
- Click on **Add** to specify an address for the SIP Trunk.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration defined in **Section 6.5** in the **SIP Server Profile** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

Profile : Cardeasy - Edit Rule

|                            |                                     |                       |                          |
|----------------------------|-------------------------------------|-----------------------|--------------------------|
| URI Group                  | *                                   | Time of Day           | default                  |
| Load Balancing             | Priority                            | NAPTR                 | <input type="checkbox"/> |
| Transport                  | None                                | LDAP Routing          | <input type="checkbox"/> |
| LDAP Server Profile        | None                                | LDAP Base DN (Search) | None                     |
| Matched Attribute Priority | <input type="checkbox"/>            | Alternate Routing     | <input type="checkbox"/> |
| Next Hop Priority          | <input checked="" type="checkbox"/> | Next Hop In-Dialog    | <input type="checkbox"/> |
| Ignore Route Header        | <input type="checkbox"/>            |                       |                          |
| ENUM                       | <input type="checkbox"/>            | ENUM Suffix           |                          |

Add

| Priority / Weight | LDAP Search Attribute | LDAP Search Regex Pattern | LDAP Search Regex Result | SIP Server Profile | Next Hop Address | Transport |        |
|-------------------|-----------------------|---------------------------|--------------------------|--------------------|------------------|-----------|--------|
| 1                 |                       |                           |                          | Cardeasy           | 192.168.1.20:50  | None      | Delete |

Finish

## 6.7 Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop for termination information and the external interfaces for origination information.

To define Topology Hiding for CardEasy, navigate to **Configuration Profiles → Topology Hiding** in the menu on the left-hand side.

The screenshot displays the 'Session Border Controller for Enterprise' configuration page. On the left is a navigation menu with options: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles (selected), Domain DoS, Server Interworking, Media Forking, Routing, Topology Hiding (highlighted in red), Signaling Manipulation, URI Groups, and SNMP Traps. The main content area is titled 'Topology Hiding Profiles: default' and includes an 'Add' button. Below this is a list of profiles: 'default' (highlighted in red), 'cisco\_th\_profile', 'Avaya', 'Telia', 'Cardeasy', and 'SessionManager'. To the right of the list is a warning box stating 'It is not recommended to edit the' followed by a 'Topology Hiding' tab. Below the tab is a 'Header' section with a table containing the following rows: 'SDP', 'To', 'Record-Route', 'From', and 'Refer-To'.

Click on **Add** (above) to bring up a dialogue box, assign an appropriate name and click on **Next** to configure Topology Hiding for each header as required:

The screenshot shows a 'Topology Hiding Profile' configuration dialog box. It has a title bar with 'Topology Hiding Profile' and a close button 'X'. Inside the dialog, there is a 'Profile Name' label followed by a text input field containing the value 'Cardeasy'. Below the input field is a 'Next' button.

Enter details in the **Topology Hiding Profile** pop-up menu.

- Click on **Add Header** and choose **Request-Line** from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing the default **IP/Domain** was used for all headers that hides both domain names and IP addresses.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.

The screenshot shows a 'Topology Hiding Profile' dialog box. It has a title bar with a close button (X). Inside, there's an 'Add Header' button in the top right. Below it is a table with four columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The 'Header' column has a dropdown menu with 'Request-Line' selected. The 'Criteria' column has a dropdown menu with 'IP/Domain' selected. The 'Replace Action' column has a dropdown menu with 'Auto' selected. The 'Overwrite Value' column has an empty text input field. To the right of the input field is a 'Delete' button. At the bottom of the dialog are 'Back' and 'Finish' buttons.

| Header       | Criteria  | Replace Action | Overwrite Value |
|--------------|-----------|----------------|-----------------|
| Request-Line | IP/Domain | Auto           |                 |

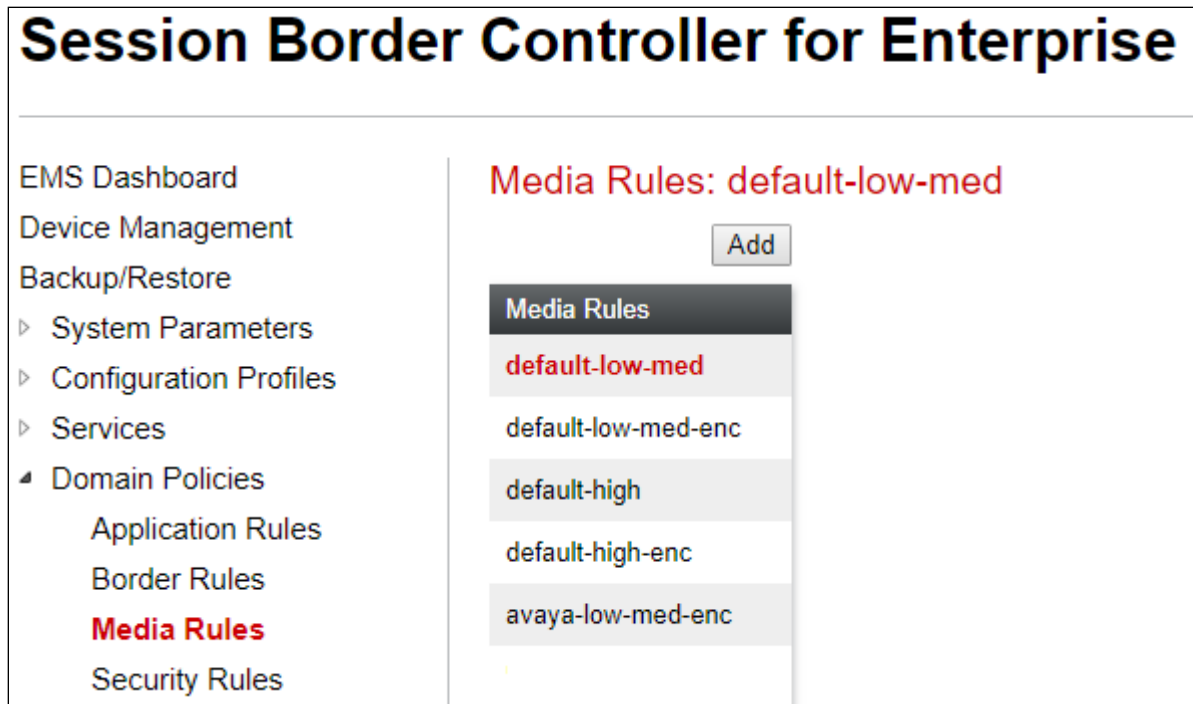
The following screenshot shows the completed **Topology Hiding** configuration for the CardEasy SBC.

The screenshot shows a web interface for 'Topology Hiding Profiles: Cardeasy'. On the left is a sidebar with a list of profiles: 'default', 'cisco\_th\_profile', 'Avaya', 'Telia', 'Cardeasy' (highlighted in red), and 'SessionManager'. Above the list is an 'Add' button. To the right of the sidebar is a main area with a blue header bar that says 'Click here to add a description.' Below this is a tab labeled 'Topology Hiding'. Under the tab is a table with four columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table contains eight rows of headers: 'SDP', 'To', 'Record-Route', 'From', 'Refer-To', 'Via', 'Request-Line', and 'Referred-By'. All 'Criteria' are 'IP/Domain' and all 'Replace Action' are 'Auto'. The 'Overwrite Value' column contains dashes ('---'). To the right of the table are buttons for 'Rename', 'Clone', and 'Delete'. Below the table is an 'Edit' button.

| Header       | Criteria  | Replace Action | Overwrite Value |
|--------------|-----------|----------------|-----------------|
| SDP          | IP/Domain | Auto           | ---             |
| To           | IP/Domain | Auto           | ---             |
| Record-Route | IP/Domain | Auto           | ---             |
| From         | IP/Domain | Auto           | ---             |
| Refer-To     | IP/Domain | Auto           | ---             |
| Via          | IP/Domain | Auto           | ---             |
| Request-Line | IP/Domain | Auto           | ---             |
| Referred-By  | IP/Domain | Auto           | ---             |

## 6.8 Media Rule for CardEasy

A media rule and an endpoint policy are setup before the server flow is created for CardEasy. The media rule is configured before the endpoint policy as it is reference by the endpoint policy



Enter a suitable name for the **Media Rule**.

The screenshot shows a 'Media Rule' configuration window. It has a title bar with 'Media Rule' and a close button. Inside, there is a 'Rule Name' label and a text input field containing 'MediaRule\_CardEasy'. Below the input field is a 'Next' button.

There is no **Audio** or **Video Encryption** set for the connection to CardEasy, this is set as shown below, click on **Next** to continue.

| Media Rule   |                                     |
|--|-------------------------------------|
| <b>Audio Encryption</b>                                    |                                     |
| Preferred Format #1  | RTP                                 |
| Preferred Format #2  | NONE                                |
| Preferred Format #3  | NONE                                |
| Encrypted RTCP   | <input type="checkbox"/>            |
| MKI  | <input type="checkbox"/>            |
| Lifetime<br><small>Leave blank to match any value.</small> | 2^ <input type="text"/>             |
| Interworking   | <input checked="" type="checkbox"/> |
| <b>Video Encryption</b>                                    |                                     |
| Preferred Format #1  | RTP                                 |
| Preferred Format #2  | NONE                                |
| Preferred Format #3  | NONE                                |
| Encrypted RTCP   | <input type="checkbox"/>            |
| MKI  | <input type="checkbox"/>            |
| Lifetime<br><small>Leave blank to match any value.</small> | 2^ <input type="text"/>             |
| Interworking   | <input checked="" type="checkbox"/> |
| <b>Miscellaneous</b>                                       |                                     |
| Capability Negotiation                                     | <input checked="" type="checkbox"/> |
| <div>BackNext</div>  |                                     |



The values here were left as default, click on **Next** to continue.

The screenshot shows the 'Media Rule' configuration window. It is divided into two main sections: 'Audio Codec' and 'Video Codec'. Each section has a 'Preferred Codescs' area with an 'Available' list, a 'P-Time (Optional)' dropdown, and a 'Selected' list. In the 'Audio Codec' section, the 'Available' list includes PCMU (0) [T], Reserved (1), Reserved (2), GSM (3), G723 (4), DVI4 (5), DVI4 (6), and LPC (7). The 'P-Time' dropdown is set to 10. In the 'Video Codec' section, the 'Available' list includes CelB (25), JPEG (26), nv (28), H261 (31), MPV (32), MP2T (33), and H263 (34). At the bottom of the window are 'Back' and 'Next' buttons.

| Section                       | Option                       | Value  |          |  |
|-------------------------------|------------------------------|--|----------|--|
| Audio Codec                   | Codec Prioritization         | <input type="checkbox"/>   |          |  |
|                               | Allow Preferred Codescs Only | <input type="checkbox"/>   |          |  |
|                               | Transcode                    | <input type="checkbox"/>   |          |  |
|                               | Transrating                  | <input type="checkbox"/>   |          |  |
| Audio Codec Preferred Codescs | Available                    | PCMU (0) [T], Reserved (1), Reserved (2), GSM (3), G723 (4), DVI4 (5), DVI4 (6), LPC (7) |          |  |
|                               | P-Time (Optional)            | 10   |          |  |
| Video Codec                   | Codec Prioritization         | <input type="checkbox"/>   |          |  |
|                               | Allow Preferred Codescs Only | <input type="checkbox"/>   |          |  |
|                               | Transcode When Needed        | <input type="checkbox"/>   |          |  |
|                               | Transrating                  | <input type="checkbox"/>   |          |  |
| Video Codec Preferred Codescs | Available                    | CelB (25), JPEG (26), nv (28), H261 (31), MPV (32), MP2T (33), H263 (34)                 | Selected |  |

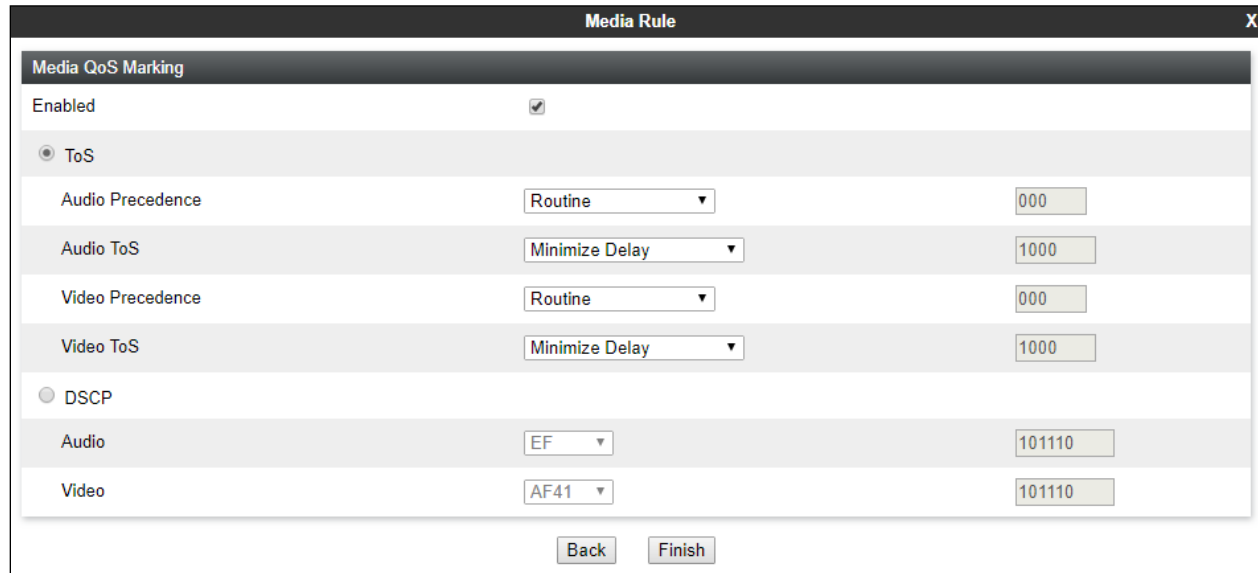
The values here were left as default, click on **Next** to continue.

The screenshot shows the 'Media Rule' configuration window with the following settings:

- Silencing:** Silencing Enabled ☒. Timeout: 60 second(s).
- Binary Floor Control Protocol:** BFCP Enabled ☐.
- Far End Camera Control:** FECC Enabled ☐.
- ANAT:** ANAT Enabled ☐. Local Preference: IPv4 (selected) or IPv6. Use Remote Preference ☐.
- Media Line Compliance:** Media Line Compliance Enabled ☐.

At the bottom of the window are 'Back' and 'Next' buttons.

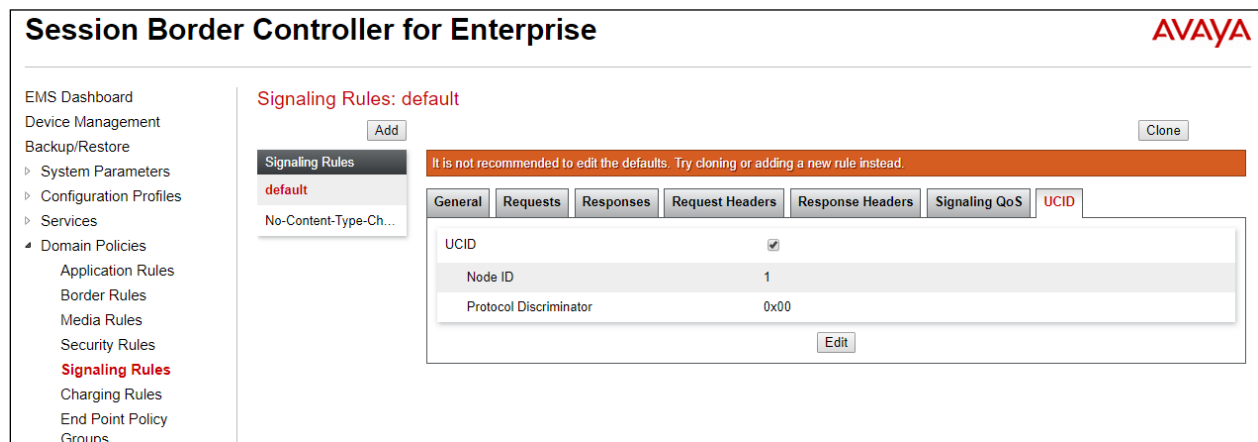
The values here were left as default, click on **Finish** to continue.



The image shows a 'Media Rule' configuration window. It has a title bar 'Media Rule' with a close button 'X'. Below the title bar is a section 'Media QoS Marking'. Under this section, there is a checkbox 'Enabled' which is checked. Below the checkbox, there are two radio buttons: 'ToS' (selected) and 'DSCP'. Under the 'ToS' radio button, there are four rows of configuration: 'Audio Precedence' with a dropdown set to 'Routine' and a text box '000'; 'Audio ToS' with a dropdown set to 'Minimize Delay' and a text box '1000'; 'Video Precedence' with a dropdown set to 'Routine' and a text box '000'; and 'Video ToS' with a dropdown set to 'Minimize Delay' and a text box '1000'. Under the 'DSCP' radio button, there are two rows: 'Audio' with a dropdown set to 'EF' and a text box '101110'; and 'Video' with a dropdown set to 'AF41' and a text box '101110'. At the bottom of the window are two buttons: 'Back' and 'Finish'.

## 6.9 Signaling Rules

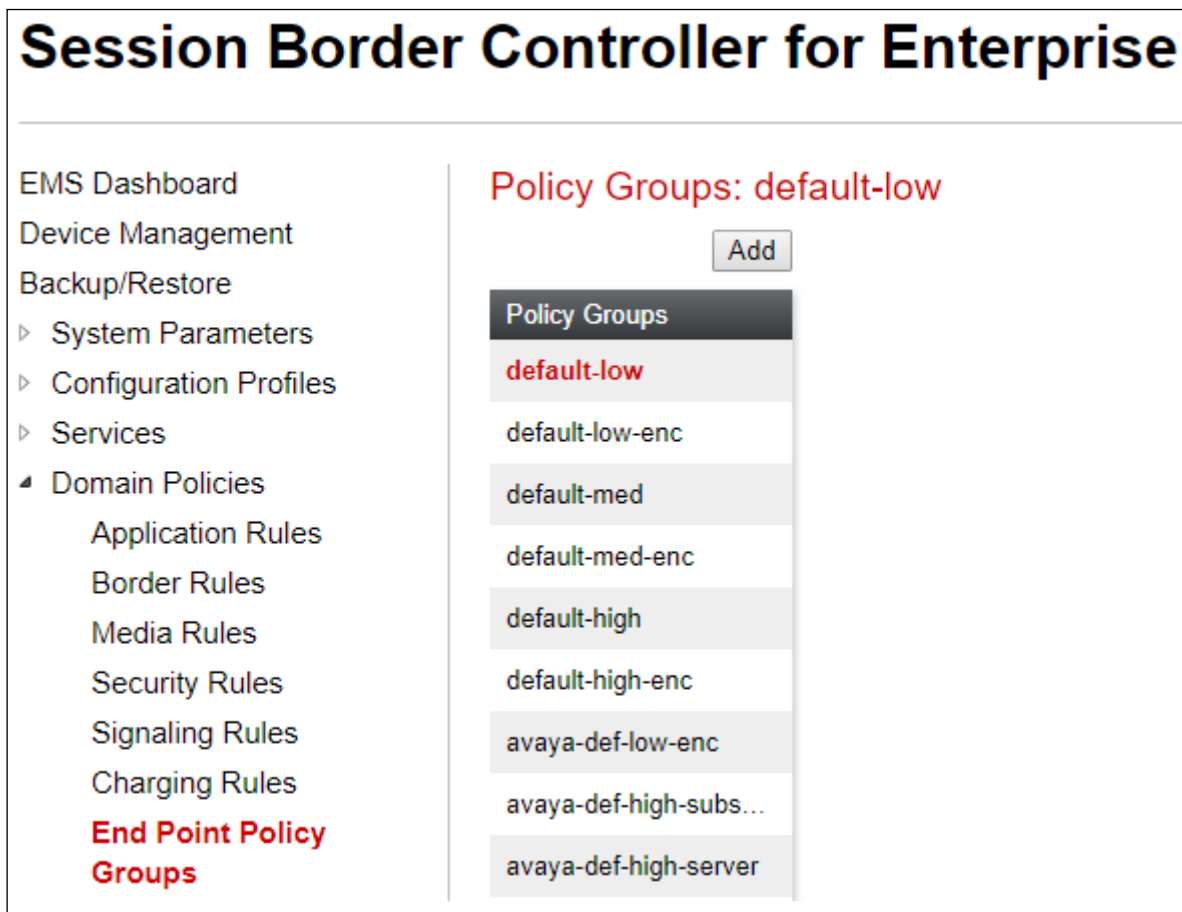
In order to allow the UCID pass through the Session Border Controller this must be setup in the Signaling Rules. Navigate to **Domain Policies** → **Signaling Rules** in the left window and click on **default** rule in the main window, alternatively a new rule can be setup if required. Click in the **UCID** tab and ensure that **UCID** is ticked as shown below. The **Node ID** can be left at **1** as this is unique to the Session Border Controller. Set the **Protocol Discriminator** to **0x00**.



The image shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with items: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies (expanded), Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (highlighted), Charging Rules, End Point Policy, and Groups. The main area is titled 'Signaling Rules: default' and has an 'Add' button. Below the title is a list of rules: 'default' (selected) and 'No-Content-Type-Ch...'. To the right of the list is a 'Clone' button. Below the list is a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below the warning is a tabbed interface with tabs: General, Requests, Responses, Request Headers, Response Headers, Signaling QoS, and UCID (selected). Under the 'UCID' tab, there is a checkbox 'UCID' which is checked. Below the checkbox are two rows: 'Node ID' with a value of '1' and 'Protocol Discriminator' with a value of '0x00'. At the bottom of the tab is an 'Edit' button.

## 6.10 End Point Policy Group for CardEasy

Click on **End Point Policy Groups** from the left menu and select **Add** from the main window.



Enter an appropriate **Group Name** for the **Policy Group** and click on **Next**.

The screenshot shows a 'Policy Group' configuration dialog box. It has a title bar with 'Policy Group' and a close button 'X'. Inside the dialog, there is a 'Group Name' label followed by a text input field containing the text 'Cardeasy'. Below the input field is a 'Next' button.

The **Media Rule** setup in **Section 6.8** is selected, all other fields can be left as default which should be as shown below. Click on **Finish** to continue.

The 'Policy Group' window displays the following configuration:

- Application Rule: default
- Border Rule: default
- Media Rule: MediaRule\_Cardeasy
- Security Rule: default-low
- Signaling Rule: default
- Charging Rule: None
- RTCP Monitoring Report Generation: Off

Buttons: Back, Finish

## 6.11 Endpoint Server Flows

Server Flows combine the previously defined profile into End Point Server Flows. This configuration ties all the previously entered information together so that calls can be routed to and from the CardEasy SBC.

To define a Server Flow, navigate to **Network Flows → End Point Flows**. Select the **Server Flows** tab and click on **Add**.

The 'Session Border Controller for Enterprise' interface shows the 'End Point Flows' section. The 'Server Flows' tab is selected, and an 'Add' button is visible. A message states: 'Modifications made to a Server Flow will only take effect on new sessions.' Below this, a table lists the configuration for the 'SIP Server: Cardeasy'.

| Priority | Flow Name   | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile                       |
|----------|-------------|-----------|--------------------|---------------------|------------------------|---------------------------------------|
| 1        | Cardeasy_In | *         | Sig_Int            | Sig_Ext             | PG                     | SessionManager View Clone Edit Delete |

Define the Server flow for the CardEasy SBC as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for the CardEasy SBC, in the test environment **CardEasy\_In** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for CardEasy defined in **Section 6.5**.
- In the **Received Interface** drop-down menu, select the internal SIP signaling interface defined in **Section 6.3**. This is the interface that signaling bound for the SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signaling interface defined in **Section 6.3**. This is the interface that signaling bound for the SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.3**. This is the interface that media bound for the SIP Trunk is sent on.
- In the **Endpoint Policy Group** drop-down menu, select the Endpoint policy that was created in **Section 6.9**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 6.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the CardEasy SBC defined in **Section 6.7** and click **Finish**.

| Edit Flow: Cardeasy_In        |                          |
|-------------------------------|--------------------------|
| Flow Name                     | Cardeasy_In              |
| SIP Server Profile            | Cardeasy                 |
| URI Group                     | *                        |
| Transport                     | *                        |
| Remote Subnet                 | *                        |
| Received Interface            | Sig_Int                  |
| Signaling Interface           | Sig_Ext                  |
| Media Interface               | Med_Ext                  |
| Secondary Media Interface     | None                     |
| End Point Policy Group        | Cardeasy                 |
| Routing Profile               | SessionManager           |
| Topology Hiding Profile       | Cardeasy                 |
| Signaling Manipulation Script | None                     |
| Remote Branch Office          | Any                      |
| Link Monitoring from Peer     | <input type="checkbox"/> |
| <b>Finish</b>                 |                          |

The information for all **Server Flows** is shown on a single screen on the Avaya SBCE.

**End Point Flows**

Subscriber Flows

Server Flows

Add

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: Cardeasy

| Priority | Flow Name   | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |  |
|----------|-------------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| 1        | Cardeasy_In | *         | Sig_Int            | Sig_Ext             | Cardeasy               | SessionManager  | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |

SIP Server: SessionManager

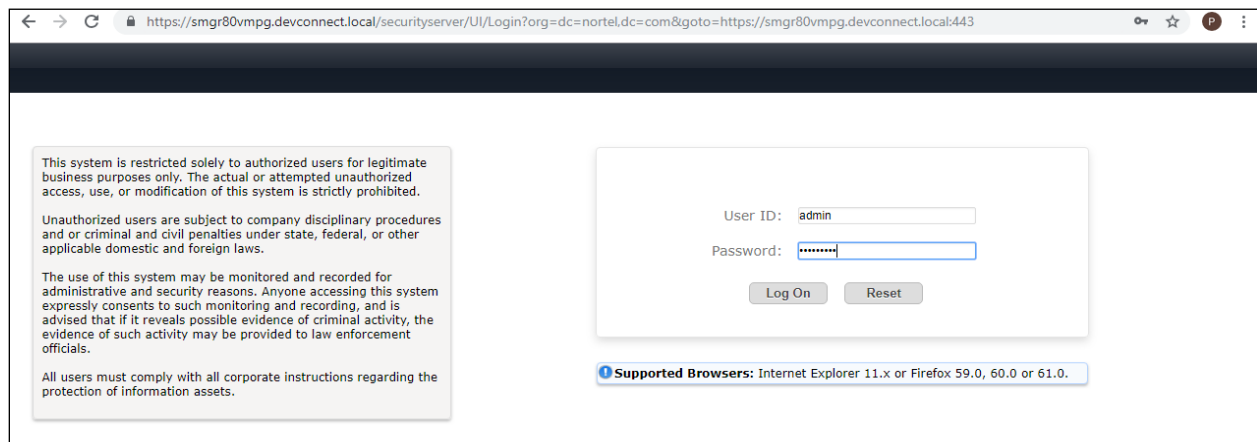
| Priority | Flow Name      | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |  |
|----------|----------------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| 1        | SM_Call_Server | *         | Sig_Ext            | Sig_Int             | PG                     | Cardeasy        | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |

## 7. Configuring Avaya Aura® Session Manager

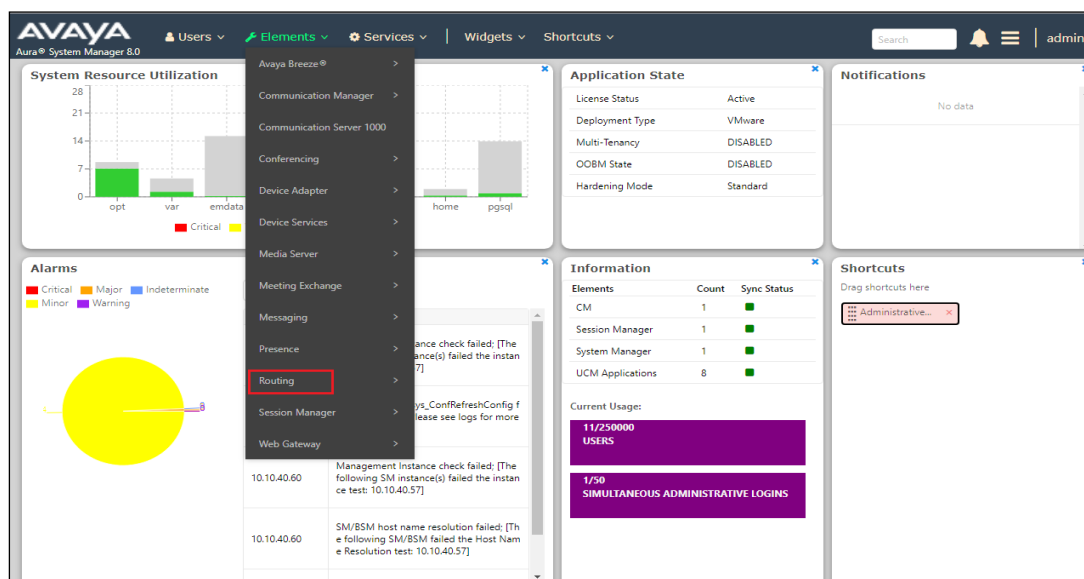
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure SIP Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to <https://<System Manager FQDN>/SMGR>. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



Once logged in navigate to **Elements** and click on **Routing** highlighted below.

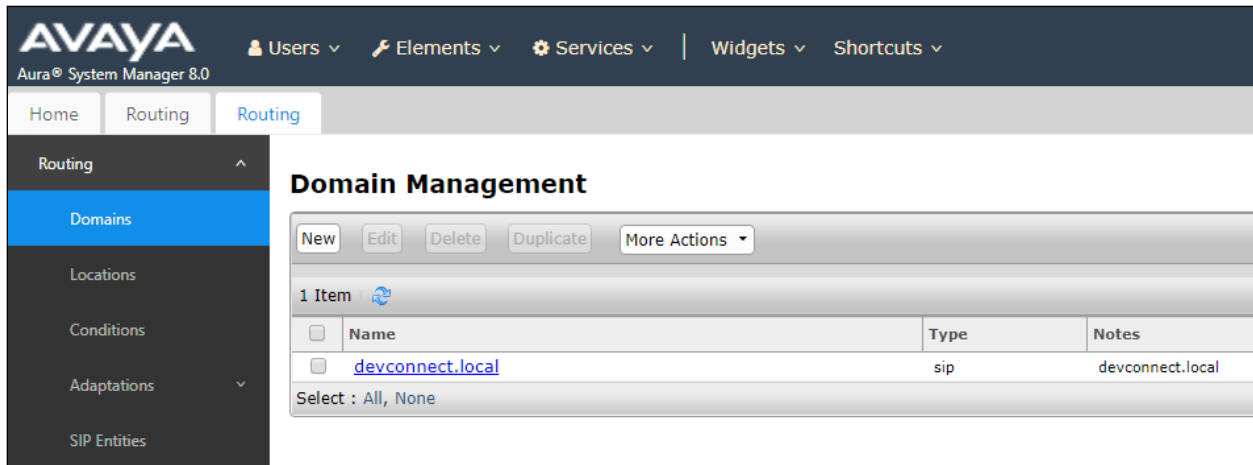


## 7.1 Domains and Locations

**Note:** It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

### 7.1.1 Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.

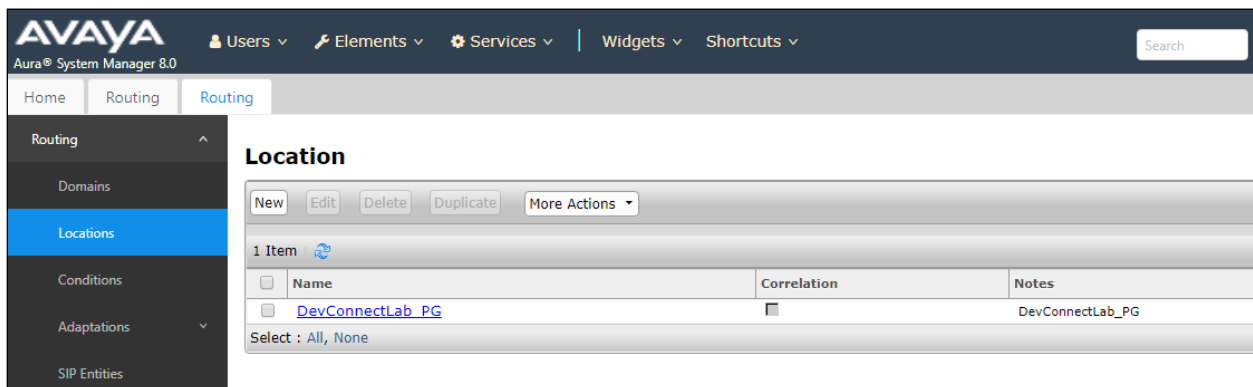


The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar has 'Routing' expanded, with 'Domains' selected. The main content area is titled 'Domain Management' and features a table with one item: 'devconnect.local' of type 'sip'.

| Name             | Type | Notes            |
|------------------|------|------------------|
| devconnect.local | sip  | devconnect.local |

### 7.1.2 Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab\_PG** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



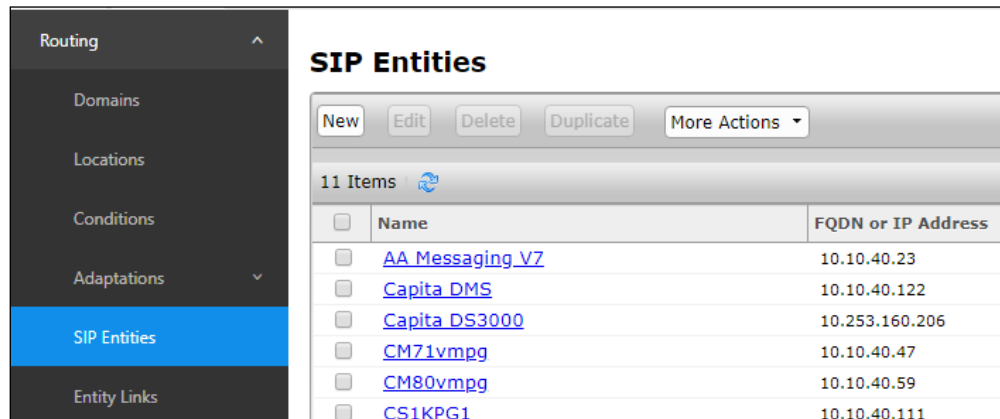
The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar has 'Routing' expanded, with 'Locations' selected. The main content area is titled 'Location' and features a table with one item: 'DevConnectLab\_PG' with correlation '1'.

| Name             | Correlation | Notes            |
|------------------|-------------|------------------|
| DevConnectLab_PG | 1           | DevConnectLab_PG |



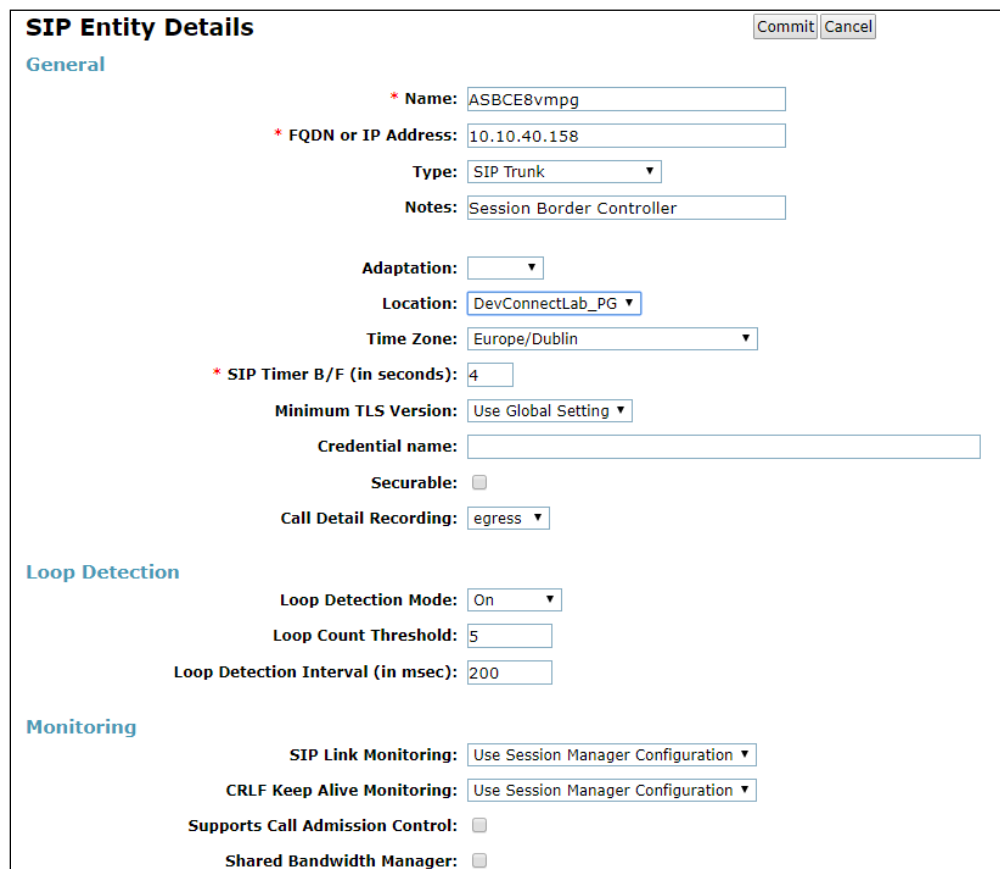
## 7.2 Configure Avaya Aura® Session Border Controller for Enterprise SIP Entity

Each SIP device (other than Avaya SIP phones) that communicates with Session Manager requires a SIP Entity and Entity Link configuration. Click on **SIP Entities** in the left column and select **New** in the main window.



|                          | Name                            | FQDN or IP Address |
|--------------------------|---------------------------------|--------------------|
| <input type="checkbox"/> | <a href="#">AA Messaging_V7</a> | 10.10.40.23        |
| <input type="checkbox"/> | <a href="#">Capita DMS</a>      | 10.10.40.122       |
| <input type="checkbox"/> | <a href="#">Capita DS3000</a>   | 10.253.160.206     |
| <input type="checkbox"/> | <a href="#">CM71vmpg</a>        | 10.10.40.47        |
| <input type="checkbox"/> | <a href="#">CM80vmpg</a>        | 10.10.40.59        |
| <input type="checkbox"/> | <a href="#">CS1KPG1</a>         | 10.10.40.111       |

Enter a suitable **Name** and the **IP Address** for the Avaya SBCE SIP Entity. Enter the correct **Time Zone** and **Location** and scroll down to SIP Entity Links.



**SIP Entity Details** [Commit] [Cancel]

**General**

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

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

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:

**Loop Detection**

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

**Monitoring**

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

## 7.3 Configure Avaya Session Border Controller for Enterprise Entity Link

An Entity link can be added from the SIP Entities page. Using the page from the previous page scroll down to Entity Links.

Upon scrolling down to **Entity Links** click on **Add**.

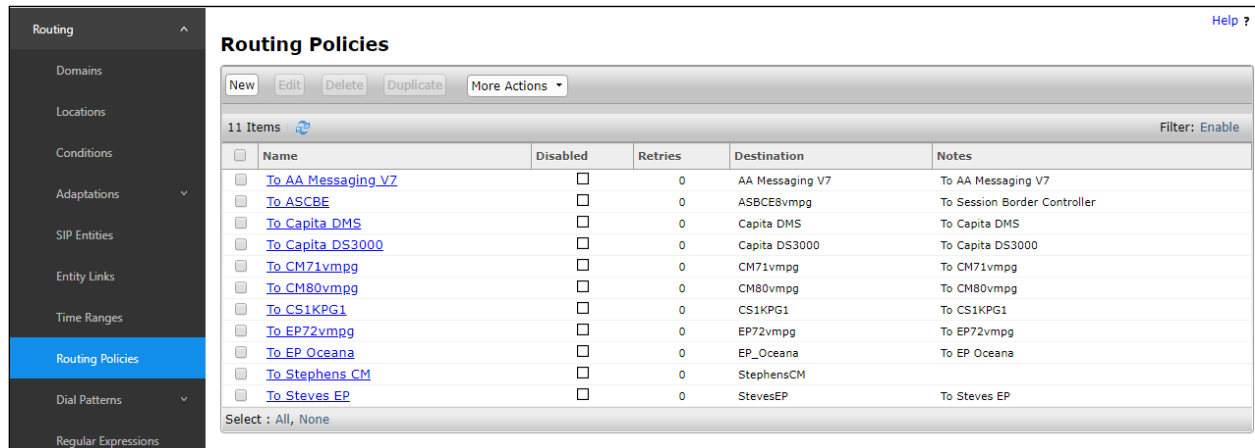
The screenshot shows the 'Monitoring' and 'Entity Links' sections of the Avaya Session Border Controller configuration page. In the 'Monitoring' section, 'SIP Link Monitoring' and 'CRLF Keep Alive Monitoring' are set to 'Use Session Manager Configuration'. 'Supports Call Admission Control' and 'Shared Bandwidth Manager' are unchecked. 'Primary Session Manager Bandwidth Association' and 'Backup Session Manager Bandwidth Association' are set to empty dropdowns. In the 'Entity Links' section, 'Override Port & Transport with DNS SRV' is unchecked. Below this is a table with 0 items. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. Below the table is a section for 'SIP Responses to an OPTIONS Request' with 0 items. The table has columns: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom are 'Commit' and 'Cancel' buttons.

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created Avaya SCBE SIP Entity for **SIP Entity 2**. All connections between Avaya Enterprise products use a secure connection and so **TLS** is selected for the **Protocol** and **Port 5061** is used. Click on **Commit** once finished to save the new Entity Link.

The screenshot shows the 'Entity Links' section of the Avaya Session Border Controller configuration page. 'Override Port & Transport with DNS SRV' is unchecked. Below this is a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. The item is: Name: \*SM80vmpg\_ASBC8vmpg, SIP Entity 1: SM80vmpg, Protocol: TLS, Port: \*5061, SIP Entity 2: ASBC8vmpg, Port: \*5061, Connection Policy: trusted, Deny New Service: unchecked. Below the table is a section for 'SIP Responses to an OPTIONS Request' with 0 items. The table has columns: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom are 'Commit' and 'Cancel' buttons.

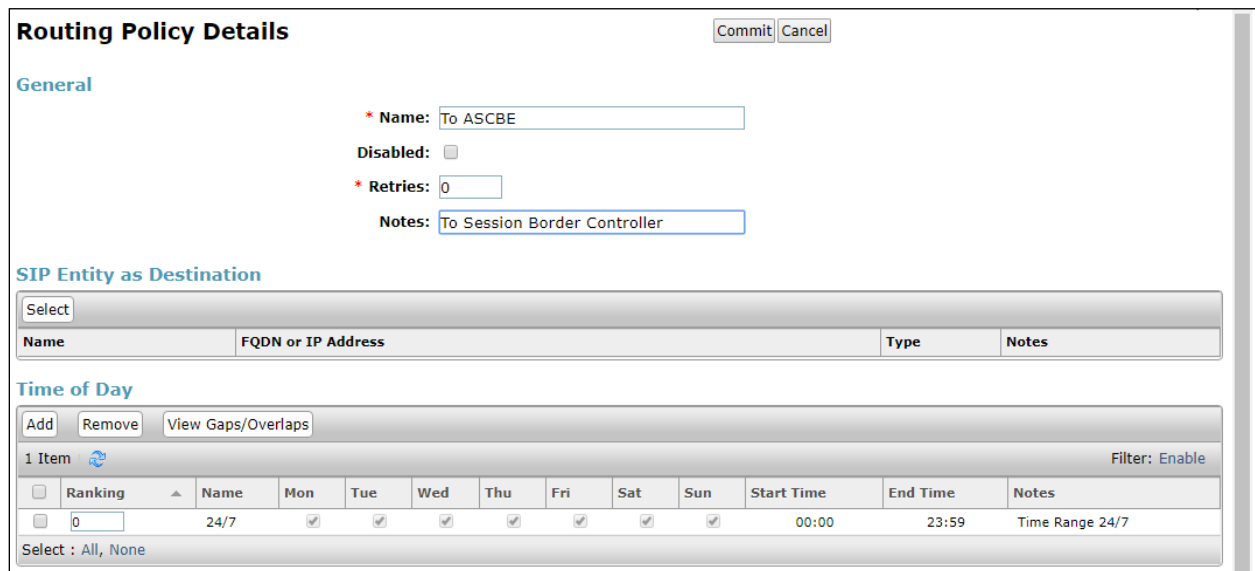
## 7.4 Configure Routing Policy for Avaya Session Border Controller for Enterprise

Click on **Routing Policies** in the left window and select **New** in the main window.



| Name               | Disabled                 | Retries | Destination     | Notes                        |
|--------------------|--------------------------|---------|-----------------|------------------------------|
| To AA Messaging V7 | <input type="checkbox"/> | 0       | AA Messaging V7 | To AA Messaging V7           |
| To ASCBE           | <input type="checkbox"/> | 0       | ASBCE8vmpg      | To Session Border Controller |
| To Capita DMS      | <input type="checkbox"/> | 0       | Capita DMS      | To Capita DMS                |
| To Capita DS3000   | <input type="checkbox"/> | 0       | Capita DS3000   | To Capita DS3000             |
| To CM71vmpg        | <input type="checkbox"/> | 0       | CM71vmpg        | To CM71vmpg                  |
| To CM80vmpg        | <input type="checkbox"/> | 0       | CM80vmpg        | To CM80vmpg                  |
| To CS1KPG1         | <input type="checkbox"/> | 0       | CS1KPG1         | To CS1KPG1                   |
| To EP72vmpg        | <input type="checkbox"/> | 0       | EP72vmpg        | To EP72vmpg                  |
| To EP_Oceana       | <input type="checkbox"/> | 0       | EP_Oceana       | To EP Oceana                 |
| To Stephens CM     | <input type="checkbox"/> | 0       | StephensCM      |                              |
| To Steves EP       | <input type="checkbox"/> | 0       | StevesEP        | To Steves EP                 |

Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**.



**Routing Policy Details** [Commit] [Cancel]

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

[Select]

| Name | FQDN or IP Address | Type | Notes |
|------|--------------------|------|-------|
|------|--------------------|------|-------|

**Time of Day**

[Add] [Remove] [View Gaps/Overlaps]

1 Item [Filter: Enable]

| Ranking | Name | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                                 | Sun                                 | Start Time | End Time | Notes           |
|---------|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| 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      | 23:59    | Time Range 24/7 |

Select the Avaya SBCE SIP Entity as shown below and click on **Select**.

**SIP Entities**SelectCancel

**SIP Entities**

11 Items Filter: Enable

| Name   | FQDN or IP Address | Type         | Notes                     |
|--|--------------------|--------------|---------------------------|
| <input type="radio"/> AA Messaging V7        | 10.10.40.23        | SIP Trunk    | AA Messaging V7           |
| <input checked="" type="radio"/> ASBCE8vmppg | 10.10.40.158       | SIP Trunk    | Session Border Controller |
| <input type="radio"/> Capita DMS             | 10.10.40.122       | SIP Trunk    | Capita DMS                |
| <input type="radio"/> Capita DS3000          | 10.253.160.206     | SIP Trunk    | Capita DS3000             |
| <input type="radio"/> CM71vmppg              | 10.10.40.47        | CM           | CM71vmppg                 |
| <input type="radio"/> CM80vmppg              | 10.10.40.59        | CM           | CM80vmppg                 |
| <input type="radio"/> CS1KPG1                | 10.10.40.111       | SIP Trunk    | CS1000 (CS1KPG1)          |
| <input type="radio"/> EP72vmppg              | 10.10.40.63        | Voice Portal | EP72vmppg                 |
| <input type="radio"/> EP_Oceana              | 10.10.41.16        | Voice Portal | EP_Oceana                 |
| <input type="radio"/> StephensCM             | 10.10.16.23        | CM           | StephensCM                |
| <input type="radio"/> StevesEP               | 10.10.16.20        | Voice Portal | StevesEP                  |

Select : None

The selected destination is now shown, click on **Commit** to save this.

**Routing Policy Details**CommitCancel

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

Select

| Name        | FQDN or IP Address | Type      | Notes                     |
|-------------|--------------------|-----------|---------------------------|
| ASBCE8vmppg | 10.10.40.158       | SIP Trunk | Session Border Controller |

## 7.5 Configure Avaya Session Border Controller for Enterprise Dial Patterns

Select **Dial Patterns** in the left window and select **New** in the main window.

| Pattern      | Min | Max | Emergency Call           | Emergency Type | Emergency Priority | SIP Domain       | Notes                                 |
|--------------|-----|-----|--------------------------|----------------|--------------------|------------------|---------------------------------------|
| 09173        | 9   | 9   | <input type="checkbox"/> |                |                    | -ALL-            | To CM80vmpg from Syntec               |
| 2            | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To CM80vmpg                           |
| 280          | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To EP72vmpg                           |
| 290          | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To EP Oceana                          |
| 30           | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To CS1KPG1                            |
| 351212455779 | 12  | 12  | <input type="checkbox"/> |                |                    | -ALL-            | To SBC8 for Syntec                    |
| 380          | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To Steves EP                          |
| 4            | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To CM71vmpg                           |
| 52           | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To CM80vmpg for simulated PSTN to IPO |
| 6666         | 4   | 4   | <input type="checkbox"/> |                |                    | devconnect.local | To AA Messaging V7                    |
| 7080         | 4   | 6   | <input type="checkbox"/> |                |                    | devconnect.local | To Capita DMS                         |
| 8000         | 5   | 5   | <input type="checkbox"/> |                |                    | devconnect.local | To Capita DS3000                      |
| 823          | 7   | 7   | <input type="checkbox"/> |                |                    | devconnect.local | To Stephens CM 823 000x               |

Enter the required digits for the Routing Pattern, in the example below **351212455779** was entered and that ensures that calls to this number are routed to the Avaya SBCE and then onto CardEasy and ultimately onto the simulated PSTN. Enter the appropriate domain for **SIP Domain** in this example all domains are excepted. Click on **Add** under **Originating Locations and Routing Policies** to select this Routing Policy.

| Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|---------------------------|----------------------------|---------------------|------|-------------------------|----------------------------|----------------------|
|                           |                            |                     |      |                         |                            |                      |

Select the **Originating Location**, this will be the location added in **Section 7.1.2** select the newly created Routing Policy for the Avaya SBCE.

**Originating Location**
Select Cancel

---

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item Filter: Enable

| <input checked="" type="checkbox"/> | Name             | Notes            |
|-------------------------------------|------------------|------------------|
| <input checked="" type="checkbox"/> | DevConnectLab_PG | DevConnectLab_PG |

Select : All, None

---

**Routing Policies**

☐

9 Items Filter: Enable

| <input type="checkbox"/>            | Name               | Disabled                 | Destination     | Notes                        |
|-------------------------------------|--------------------|--------------------------|-----------------|------------------------------|
| <input type="checkbox"/>            | To AA Messaging V7 | <input type="checkbox"/> | AA Messaging V7 | To AA Messaging V7           |
| <input checked="" type="checkbox"/> | To ASCBE           | <input type="checkbox"/> | ASBCE8vmppg     | To Session Border Controller |
| <input type="checkbox"/>            | To CM71vmppg       | <input type="checkbox"/> | CM71vmppg       | To CM71vmppg                 |
| <input type="checkbox"/>            | To CM80vmppg       | <input type="checkbox"/> | CM80vmppg       | To CM80vmppg                 |
| <input type="checkbox"/>            | To CS1KPG1         | <input type="checkbox"/> | CS1KPG1         | To CS1KPG1                   |
| <input type="checkbox"/>            | To EP72vmppg       | <input type="checkbox"/> | EP72vmppg       | To EP72vmppg                 |
| <input type="checkbox"/>            | To EP Oceana       | <input type="checkbox"/> | EP_Oceana       | To EP Oceana                 |
| <input type="checkbox"/>            | To Stephens CM     | <input type="checkbox"/> | StephensCM      |                              |
| <input type="checkbox"/>            | To Steves EP       | <input type="checkbox"/> | StevesEP        | To Steves EP                 |

Select : All, None

Select Cancel

With the Routing Policy selected click on **Commit** to finish adding the Dial Pattern.

**Dial Pattern Details**
Commit Cancel

---

**General**

\* Pattern: 351212455779

\* Min: 12

\* Max: 12

Emergency Call: ☐

SIP Domain: -ALL-

Notes: To SBC8 for Syntec

---

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes         |
|--------------------------|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|------------------------------|
| <input type="checkbox"/> | DevConnectLab_PG          | DevConnectLab_PG           | To ASCBE            | 0    | <input type="checkbox"/> | ASBCE8vmppg                | To Session Border Controller |

Select : All, None

## 8. Configure Avaya Aura® Application Enablement Services Server

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable Unrestricted Access for CTI User
- Identify TLinks
- Configure Networking Ports

### 8.1 Verify Licensing

To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of the AES. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the **TSAPI Service** is licensed by ensuring that the **License Mode** is showing **NORMAL MODE**.

| Service                 | Status         | State   | License Mode | Cause* |
|-------------------------|----------------|---------|--------------|--------|
| ASAI Link Manager       | N/A            | Running | N/A          | N/A    |
| CVLAN Service           | OFFLINE        | Running | N/A          | N/A    |
| DLG Service             | OFFLINE        | Running | N/A          | N/A    |
| DMCC Service            | ONLINE         | Running | NORMAL MODE  | N/A    |
| TSAPI Service           | ONLINE         | Running | NORMAL MODE  | N/A    |
| Transport Layer Service | N/A            | Running | N/A          | N/A    |
| AE Services HA          | Not Configured | N/A     | N/A          | N/A    |

### 8.2 Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button.

**AVAYA** Application Enablement Services Management Console

Communication Manager Interface | Switch Connections

- AE Services
  - Communication Manager Interface
    - Switch Connections**
    - Dial Plan
    - High Availability
    - Licensing
    - Maintenance

Switch Connections

cm80vmpg **Add Connection**

| Connection Name                   | Processor Ethernet               | Msg Period                              |
|-----------------------------------|----------------------------------|---|
| <a href="#">Edit Connection</a>   | <a href="#">Edit PE/CLAN IPs</a> | <a href="#">Edit H.323 Gatekeeper</a>   |
| <a href="#">Delete Connection</a> |                                  | <a href="#">Survivability Hierarchy</a> |

In the resulting screen enter the **Switch Password**, the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3.2**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

**Connection Details - cm80vmpg**

Switch Password

Confirm Switch Password

Msg Period  Minutes (1 - 72)

Provide AE Services certificate to switch ☐

Secure H323 Connection ☐

Processor Ethernet ☒

**Apply**



From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button.

**Switch Connections**

cm80vmpg Add Connection

| Connection Name | Processor Ethernet      | Msg Period              |
|-----------------|-------------------------|-------------------------|
| Edit Connection | <b>Edit PE/CLAN IPs</b> | Edit H.323 Gatekeeper   |
|                 | Delete Connection       | Survivability Hierarchy |

In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.3.1** that will be used for the AES connection and select the **Add Name or IP** button.

**Edit Processor Ethernet IP - cm80vmpg**

10.10.40.59 Add/Edit Name or IP

| Name or IP Address |
|--------------------|
| 10.10.40.59        |

Back

### 8.3 Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.

**AVAYA** **Application Enablement Services**  
Management Console

AE Services | TSAPI | TSAPI Links

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - **TSAPI Links**
  - TSAPI Properties
- ▶ TWS

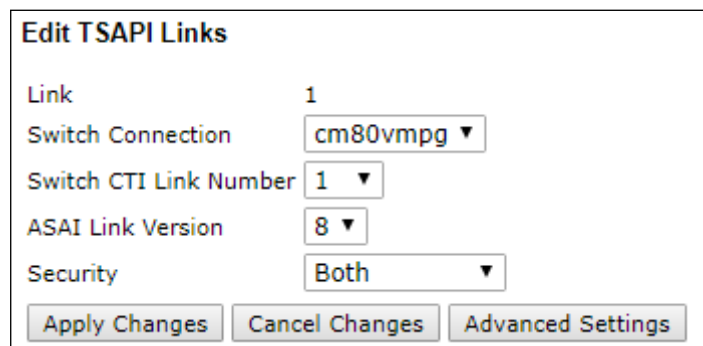
**TSAPI Links**

| Link | Switch Connection | Switch CTI Link # |
|------|-------------------|-------------------|
|      |                   |                   |

Add Link Edit Link Delete Link

On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm80vmppg**, which has already been configured in **Section 8.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4**.
- **ASAI Link Version:** This can be left at the default value of **8**.
- **Security:** This can be left at the default value. The value **both** was used in this test.
- Once completed, select **Apply Changes**.



**Edit TSAPI Links**

Link 1

Switch Connection cm80vmppg ▼

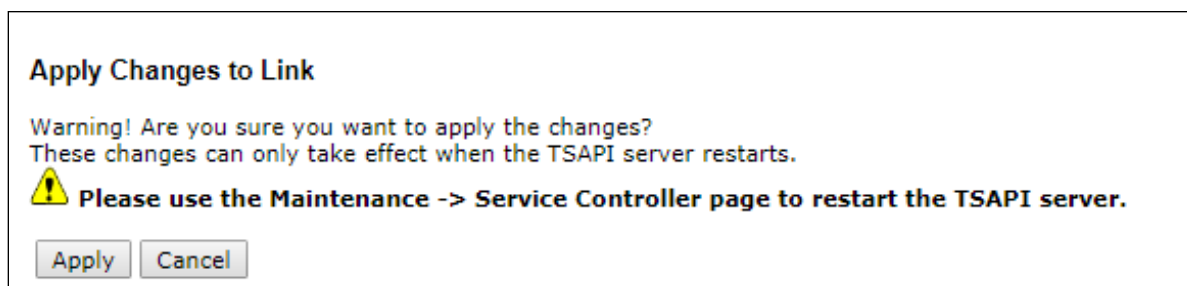
Switch CTI Link Number 1 ▼

ASAI Link Version 8 ▼

Security Both ▼

Apply Changes Cancel Changes Advanced Settings

Another screen appears for confirmation of the changes. Choose **Apply**.



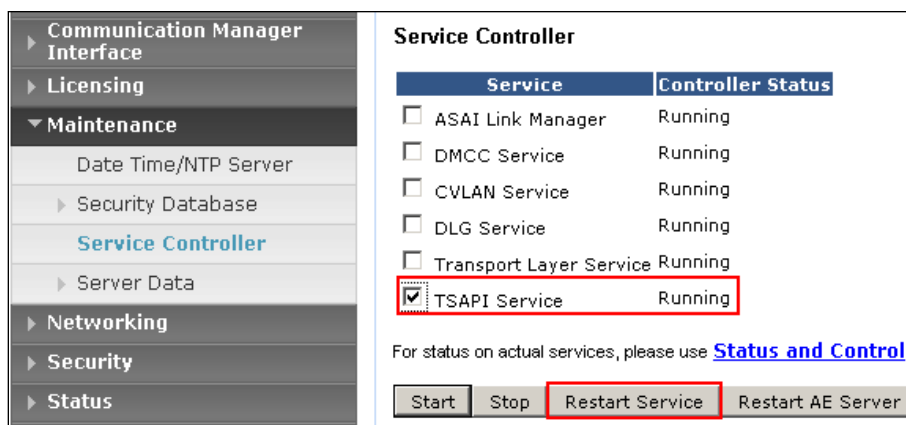
**Apply Changes to Link**

Warning! Are you sure you want to apply the changes?  
These changes can only take effect when the TSAPI server restarts.

⚠ Please use the Maintenance -> Service Controller page to restart the TSAPI server.

Apply Cancel

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



**Service Controller**

| Service   | Controller Status |
|---|-------------------|
| <input type="checkbox"/> ASAI Link Manager        | Running           |
| <input type="checkbox"/> DMCC Service             | Running           |
| <input type="checkbox"/> CVLAN Service            | Running           |
| <input type="checkbox"/> DLG Service              | Running           |
| <input type="checkbox"/> Transport Layer Service  | Running           |
| <input checked="" type="checkbox"/> TSAPI Service | Running           |

For status on actual services, please use [Status and Control](#)

Start Stop **Restart Service** Restart AE Server

## 8.4 Create CTI User

A User ID and password need to be configured for the CardEasy EDIP server to communicate as a TSAPI client with the Application Enablement Services. Navigate to the **User Management** → **User Admin** and choose **Add User**. In the **Add User** screen, enter the following values:

- **User Id** – This will be used by the CardEasy EDIP server.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used by the CardEasy EDIP server.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen.

The screenshot shows the 'Add User' screen within the 'User Management | User Admin | Add User' context. On the left is a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under 'User Admin', 'Add User' is selected. The main area is titled 'Add User' and contains a form with the following fields: User Id (cardeasy), Common Name (cardeasy), Surname (cardeasy), User Password (masked with dots), Confirm Password (masked with dots), Admin Note (empty), Avaya Role (None), Business Category (empty), Car License (empty), CM Home (empty), Csx Home (empty), CT User (Yes), Department Number (empty), Display Name (empty), Employee Number (empty), Employee Type (empty), Enterprise Handle (empty), Given Name (empty), Home Phone (empty), Home Postal Address (empty), Initials (empty), Labeled URI (empty), Mail (empty), MM Home (empty), Mobile (empty), Organization (empty), Pager (empty), Preferred Language (English), Room Number (empty), and Telephone Number (empty). Fields marked with an asterisk (\*) are required. At the bottom are 'Apply' and 'Cancel' buttons.

## 8.5 Configure Security Database

The security database must be configured to allow the user “CardEasy” monitor and receive events from the Avaya endpoints. The following steps ensure that this will happen.

### 8.5.1 Configure Security Database Control for TSAPI

Navigate to selecting **Security** → **Security Database** → **Control**. Ensure that Enable SDB for TASPI Service, JTAPI and Telephony Web Services is ticked, as shown below.

The screenshot shows a web interface for configuring the Security Database. The top navigation bar is red with the text "Security | Security Database | Control". On the left is a sidebar menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two checkboxes: "Enable SDB for DMCC Service" (unchecked) and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services" (checked). Below the checkboxes is an "Apply Changes" button.

| Security   Security Database   Control   |  |
|--|--|
| <ul style="list-style-type: none"><li>▶ AE Services</li><li>▶ Communication Manager Interface</li><li>▶ High Availability</li><li>▶ Licensing</li><li>▶ Maintenance</li><li>▶ Networking</li><li>▼ Security<ul style="list-style-type: none"><li>▶ Account Management</li><li>▶ Audit</li><li>▶ Certificate Management</li><li>Enterprise Directory</li><li>▶ Host AA</li><li>▶ PAM</li><li>▼ Security Database<ul style="list-style-type: none"><li>▪ Control</li><li>⊕ CTI Users</li></ul></li></ul></li></ul> | <h3>SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services</h3> <p><input type="checkbox"/> Enable SDB for DMCC Service</p> <p><input checked="" type="checkbox"/> Enable SDB for TSAPI Service, JTAPI and Telephony Web Services</p> <p><button>Apply Changes</button></p> |

## 8.5.2 Edit CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 8.4** and select the **Edit** button.

| User ID                                   | Common Name | Worktop Name | Device ID |
|---|-------------|--------------|-----------|
| <input type="radio"/> asc                 | asc         | NONE         | NONE      |
| <input checked="" type="radio"/> cardeasy | cardeasy    | NONE         | NONE      |
| <input type="radio"/> NICE                | NICE        | NONE         | NONE      |
| <input type="radio"/> paul                | paul        | NONE         | NONE      |

The **Edit CTI User** screen appears. Check the **Call Monitoring** box and **Apply Changes** at the bottom of the screen.

**Edit CTI User**

User Profile:

User ID: cardeasy  
Common Name: cardeasy  
Worktop Name: NONE ▼  
Unrestricted Access: ☐

Call and Device Control:

Call Origination/Termination and Device Status: Any ▼

Call and Device Monitoring:

Device Monitoring: Any ▼  
Calls On A Device Monitoring: Any ▼  
Call Monitoring: ☒

Routing Control:

Allow Routing on Listed Devices: Any ▼

**Note:** It's also possible configure the Communication Manager stations to be monitored in a CardEasy config file and tick the box in AES to allow CardEasy to 'monitor all' instead of adding each extension to the security database. If there are a number of AES servers or a large number of extensions to monitor this approach is easier as the config file allows ranges of extensions to be defined instead of listing them all individually.

### 8.5.3 Configure Devices

Click on **Devices** and add each Avaya endpoint that is to be monitored. This will allow CardEasy get TSAPI events from these Avaya extensions. The screen below shows several extensions such as **2000**, **2003** and **2100** already entered. To enter a new **Device ID**, enter the Avaya extension number into the box and click on **Add Device**.

Security | Security Database | Devices Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Account Management  
Audit  
Certificate Management  
Enterprise Directory  
Host AA  
PAM  
Security Database  
Control  
CTI Users  
Devices  
Device Groups

Devices

Upload devices from file  No file chosen

|                          | Device ID | Tlink Group | Device Type | Location |
|--------------------------|-----------|-------------|-------------|----------|
| <input type="checkbox"/> | 2000      | Any         | PHONE       |          |
| <input type="checkbox"/> | 2003      | Any         | PHONE       |          |
| <input type="checkbox"/> | 2050      | Any         | PHONE       |          |
| <input type="checkbox"/> | 2100      | Any         | PHONE       |          |
| <input type="checkbox"/> | 2103      | Any         | PHONE       |          |
| <input type="checkbox"/> | 2109      | Any         | PHONE       |          |

0-6 of 6

### 8.5.4 Identify Tlinks

Click on **Tlinks**. Verify the value of the **Tlink Name**. This will be used by the CardEasy application.

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Account Management  
Audit  
Certificate Management  
Enterprise Directory  
Host AA  
PAM  
Security Database  
Control  
CTI Users  
Devices  
Device Groups  
Tlinks  
Tlink Groups  
Worktops

Tlinks

Tlink Name

☒ AVAYA#CM80VMMPG#CSTA#AES80VMMPG  
☐ AVAYA#CM80VMMPG#CSTA-S#AES80VMMPG

## 8.6 Configure Networking Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

| Networking   Ports   |                         |                                    |  |  |
|--|-------------------------|------------------------------------|--|--|
| <ul style="list-style-type: none"> <li>&gt; AE Services</li> <li>&gt; Communication Manager Interface</li> <li>&gt; High Availability</li> <li>&gt; Licensing</li> <li>&gt; Maintenance</li> <li>&gt; <b>Networking</b></li> <li>    AE Service IP (Local IP)</li> <li>    Network Configure</li> <li>    <b>Ports</b></li> <li>    TCP/TLS Settings</li> <li>&gt; Security</li> <li>&gt; Status</li> <li>&gt; User Management</li> <li>&gt; Utilities</li> <li>&gt; Help</li> </ul> | <b>Ports</b>            |                                    |  |  |
|  | CVLAN Ports             |                                    |  | Enabled Disabled                                       |
|  |                         | Unencrypted TCP Port               | 9999   | <input checked="" type="radio"/> <input type="radio"/> |
|  |                         | Encrypted TCP Port                 | <input type="text" value="9998"/>                      | <input type="radio"/> <input checked="" type="radio"/> |
|  | <hr/>                   |                                    |  |  |
|  | DLG Port                | TCP Port                           | 5678   |  |
|  | TSAPI Ports             |                                    |  | Enabled Disabled                                       |
|  |                         | TSAPI Service Port                 | 450  | <input checked="" type="radio"/> <input type="radio"/> |
|  |                         | Local TLINK Ports                  |  |  |
|  |                         | TCP Port Min                       | 1024   |  |
|  | TCP Port Max            | 1039                               |  |  |
|  | Unencrypted TLINK Ports |                                    |  |  |
|  | TCP Port Min            | <input type="text" value="1050"/>  |  |  |
|  | TCP Port Max            | <input type="text" value="1065"/>  |  |  |
|  | Encrypted TLINK Ports   |                                    |  |  |
|  | TCP Port Min            | <input type="text" value="1066"/>  |  |  |
|  | TCP Port Max            | <input type="text" value="1081"/>  |  |  |
| <hr/>  |                         |                                    |  |  |
|  | DMCC Server Ports       |                                    | Enabled Disabled                                       |  |
|  | Unencrypted Port        | <input type="text" value="4721"/>  | <input checked="" type="radio"/> <input type="radio"/> |  |
|  | Encrypted Port          | <input type="text" value="4722"/>  | <input type="radio"/> <input checked="" type="radio"/> |  |
|  | TR/87 Port              | <input type="text" value="4723"/>  | <input checked="" type="radio"/> <input type="radio"/> |  |
| <hr/>  |                         |                                    |  |  |
|  | H.323 Ports             |                                    |  |  |
|  | TCP Port Min            | <input type="text" value="20000"/> |  |  |
|  | TCP Port Max            | <input type="text" value="29999"/> |  |  |
|  | Local UDP Port Min      | <input type="text" value="20000"/> |  |  |
|  | Local UDP Port Max      | <input type="text" value="29999"/> |  |  |
|  |                         |                                    | Enabled Disabled                                       |  |
|  | Server Media            |                                    | <input checked="" type="radio"/> <input type="radio"/> |  |
|  | RTP Local UDP Port Min* | <input type="text" value="30000"/> |  |  |

Once all the necessary changes are made it is a good idea to restart of the AE Server. Navigate to **Maintenance → Service Controller**. In the main screen select **Restart AE Server** highlighted.

The screenshot displays the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, Licensing, Maintenance (highlighted with a red box), Date Time/NTP Server, Security Database, Service Controller (highlighted with a red box), Server Data, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Service Controller' and features a table with the following data:

| Service  | Controller Status |
|--|-------------------|
| <input type="checkbox"/> ASAI Link Manager       | Running           |
| <input type="checkbox"/> DMCC Service            | Running           |
| <input type="checkbox"/> CVLAN Service           | Running           |
| <input type="checkbox"/> DLG Service             | Running           |
| <input type="checkbox"/> Transport Layer Service | Running           |
| <input type="checkbox"/> TSAPI Service           | Running           |

Below the table, there is a link: 'For status on actual services, please use [Status and Control](#)'. At the bottom, there is a row of buttons: Start, Stop, Restart Service, Restart AE Server (highlighted with a red box), Restart Linux, and Restart Web Server.



## **9. Configure CardEasy SBC**

All configuration of the CardEasy appliance and service is undertaken by Syntec as part of its managed service PCI offering.

## **10. Configure CardEasy EPID Application**

All configuration of the EPID application is undertaken by Syntec as part of its managed service PCI offering.

## 11. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

### 11.1 Verify CardEasy application

Before any links between the Avaya products are verified the application from Syntec can be checked by opening a URL as was done during compliance testing and making a call to the “incoming VDN”. A URL was opened to a ‘test page’ as shown below. This URL was provided by Syntec. The **Customer** was **demo** and the **End Point ID** should be the agent ID of the agent answering the call.



The screenshot shows a web browser window with the URL <https://us-west.ceclients.syntec.co.uk/cpe/psp-paypal.jsp>. The browser's address bar and tabs are visible at the top. The main content area is titled "Demo Virtual Terminal" and includes a "Customer:" label with a text input field containing "demo". To the right is the CardEasy logo, which includes a green telephone handset icon and the text "CardEasy™ Keypad payment by 'phone'", along with a "PCI DSS Level 1" badge. Below the header is a large form with two main sections. The first section is for order details, with labels and input fields for: "Order Ref:" (7tjrse1n8mmd), "Order Description:" (3 telephone cards), "Customer First Name:" (Bill), "Surname:" (Smith), "Customer Address:" (45 fourth street), "Customer Postcode:" (GU56 6YH), "Customer eMail:" (rubbish@syntec.co.uk), "Amount:" (23.45), and "Currency:" (EUR). The second section is for card payment details, with labels and input fields for: "End Point ID (EPID):" (2400), "Card number:" (masked), "Issuer:" (blank), "Scheme:" (blank), "Product Type:" (blank), "Expiry Date:" (two dropdown menus), and "Card verification code:" (masked). A "Capture" button is located next to the card number field. At the bottom of the form is the PayPal logo. Below the PayPal logo, the text "Test PANs:" is followed by three test card numbers: 4137357692954813, 4001700241144803, and 4683075410516684.

← → ↻ <https://us-west.ceclients.syntec.co.uk/cpe/psp-paypal.jsp>

Apps Suggested Sites Imported From IE Oceana Login RealTime Login SupervisorLogin RT LOGIN

### Demo Virtual Terminal

Customer:

 **CardEasy™**  
Keypad payment by 'phone' 

Order Ref:  (Merchant's unique reference)

Order Description:

Customer First Name:  Surname:

Customer Address:

Customer Postcode:

Customer eMail:

Amount:  (use decimal point as necessary)

Currency:

End Point ID (EPID):  (Service agent's unique call reference)

Card number:


Issuer:

Scheme:

Product Type:

Expiry Date:  /

Card verification code:





Test PANs:  
4137357692954813  
4001700241144803  
4683075410516684

When **Capture** is pressed (see the screen on the previous page), the caller is asked to input their credit card details and the following shows how this is “masked” from the agent. This verifies that the application is working correctly as the call can be placed correctly to the agent and the capture for the credit card input is working properly.

### Demo Virtual Terminal

Customer:



Order Ref:  (Merchant's unique reference)

Order Description:

Customer First Name:  Surname:

Customer Address:

Customer Postcode:

Customer eMail:

Amount:  (use decimal point as necessary)

Currency:

End Point ID (EPID):  (Service agent's unique call reference)

Card number:   PAN:


Issuer :

Scheme :

Product Type :

Expiry Date:  /

Card verification code:



Test PANs:  
4137357692954813  
4001700241144803  
4683075410516684

## 11.2 Verify connection to Avaya Aura® Application Enablement Services

The following can be checked to ensure that the connections to the AES are in operation correctly.

### 11.2.1 Verify link between Communication Manager and the Application Enablement Services

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the TSAPI link status with Application Enablement Services by using the command **status aesvcs cti-link**. Verify the **Service State** of the TSAPI link is **established**.

|                               |         |          |                    |                      |           |           |
|-------------------------------|---------|----------|--------------------|----------------------|-----------|-----------|
| <b>status aesvcs cti-link</b> |         |          |                    |                      |           |           |
| AE SERVICES CTI LINK STATUS   |         |          |                    |                      |           |           |
| CTI Link                      | Version | Mnt Busy | AE Services Server | <b>Service State</b> | Msgs Sent | Msgs Rcvd |
| 1                             | 8       | no       | aes80vmpg          | <b>established</b>   | 87        | 61        |

Use the command **status aesvcs interface** to verify that the status **Local Node** of Application Enablement Services interface is connected and **listening**.

|                                |          |                       |                  |
|--------------------------------|----------|-----------------------|------------------|
| <b>status aesvcs interface</b> |          |                       |                  |
| AE SERVICES INTERFACE STATUS   |          |                       |                  |
| <b>Local Node</b>              | Enabled? | Number of Connections | Status           |
| procr                          | yes      | 1                     | <b>listening</b> |

Verify that there is a link with the Application Enablement Services and that messages are being sent and received by using the command **status aesvcs link**.

|                           |                    |             |             |              |            |            |
|---------------------------|--------------------|-------------|-------------|--------------|------------|------------|
| <b>status aesvcs link</b> |                    |             |             |              |            |            |
| AE SERVICES LINK STATUS   |                    |             |             |              |            |            |
| Srvr/ Link                | AE Services Server | Remote IP   | Remote Port | Local Node   | Msgs Sent  | Msgs Rcvd  |
| 01/01                     | aes80vmpg          | 10.10.40.56 | 57650       | <b>procr</b> | <b>683</b> | <b>665</b> |

## 11.2.2 Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

**TSAPI Link Details**

☐ Enable page refresh every 60 seconds

|                                  | Link | Switch Name | Switch CTI Link ID | Status  | Since                    | State  | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|----------------------------------|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| <input checked="" type="radio"/> | 1    | cm80vmpg    | 1                  | Talking | Mon Jan 28 11:08:16 2019 | Online | 18             | 11           | 632            | 657              | 30          |

For service-wide information, choose one of the following:

Click in **User Status** on the screen above. A new window is displayed below showing the CTI user **cardeasy** connected to receive the TSAPI events.

**CTI User Status**

☐ Enable page refresh every 60 seconds

CTI Users

Open Streams 1  
Closed Streams 50

**Open Streams**

| Name     | Time Opened                     | Time Closed | Tlink Name                    |
|----------|---------------------------------|-------------|-------------------------------|
| cardeasy | Tue 11 Jun 2019 02:12:11 PM IST |             | AVAYA#CM80VMPG#CSTA#AES80VMPG |

## 11.3 Verify connection to Avaya Session Border Controller

A PuTTY connection is opened to the Avaya SBCE using an SSH connection on port 222 (not shown). The resulting screen is shown below with a call being placed from the “PSTN” through the CardEasy SBC and on through the Avaya SBCE and onto Communication Manager and the agent’s phone. The screen below shows a trace taken from the Avaya SBCE showing this call and thus proving that the links each side of the Avaya SBCE are up and working properly.

```
SBCE - traceSBC - Captured: 30 Displayed: 26

192.168.1.20      10.10.40.58
SBC

10:28:08.927  --INVITE--> SIP: sip:091732900@192.168.1.10:5060 T:091732900 F:+351212455779
10:28:08.927  --Trying--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --INVITE--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --Trying--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --Ringing--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --Ringing--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --PRACK--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --PRACK--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --200 OK--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:08.927  --200 OK--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --200 OK--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --ACK--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --ACK--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --reINVIT--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --trying--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --200 OK--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --200 OK--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --ACK--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --ACK--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --BYE--> SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --200 OK--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
10:28:12.933  --200 OK--< SIP: sip:091732900@10.10.40.58:5061 T:091732900 F:+351212455779
```

## 11.4 Verify SIP Trunk Connection

The SIP trunk from Communication Manager to Session Manager can be checked using the following steps.

### 11.4.1 Verify Avaya Aura® Communication Manager

The following steps can be taken if there are any issues with calls being made. This should help verify the links between the products. From the SAT interface, verify the status of the SIP trunk groups by using the **status trunk n** command, where “n” is the trunk group number administered in **Section 5.2.5**. Verify that all trunks are in the **in-service/idle** state as shown below (just a sample of the trunks configured).

```
status trunk 1
```

| TRUNK GROUP STATUS |        |                 |                              |
|--------------------|--------|-----------------|------------------------------|
| Member             | Port   | Service State   | Mtce Connected Ports<br>Busy |
| 0001/0001          | T00001 | in-service/idle | no                           |
| 0001/0002          | T00002 | in-service/idle | no                           |
| 0001/0003          | T00003 | in-service/idle | no                           |

Verify the status of the SIP signaling groups by using the **status signaling-group n** command, where “n” is the signaling group number administered in **Section 5.2.5**. Verify that the signaling group is **in-service** as indicated in the **Group State** field shown below.

```
status signaling-group 1
                        STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

      Group State: in-service
```

## 11.4.2 Verify Avaya Session Border Controller SIP Entity is up

Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The 'Elements' menu is open, displaying a list of system components. 'Session Manager' is highlighted with a red box. The main dashboard includes several widgets: 'System Resource Utilization' (a bar chart showing utilization for 'opt', 'var', and 'emdata'), 'Alarms' (a yellow circle indicating a critical alarm), 'Application State' (showing License Status: Active, Deployment Type: VMware, Multi-Tenancy: DISABLED, OOBM State: DISABLED, and Hardening Mode: Standard), 'Information' (a table listing system elements and their counts), and 'Notifications' (showing no data). The 'Information' table is as follows:

| Elements         | Count | Sync Status |
|------------------|-------|-------------|
| CM               | 1     | Green       |
| Session Manager  | 1     | Green       |
| System Manager   | 1     | Green       |
| UCM Applications | 8     | Green       |

The 'Current Usage' section shows 11/250000 USERS and 1/50 SIMULTANEOUS ADMINISTRATIVE LOGINS.

Select the Avaya SBCE SIP Entity.

**SIP Entity Link Monitoring Status Summary**  
This page provides a summary of Session Manager SIP entity link monitoring status.

**SIP Entities Status for All Monitoring Session Manager Instances**  
Run Monitor

1 Item

|                          | Session Manager          | Type | Monitored Entities |              |
|--------------------------|--------------------------|------|--------------------|--------------|
|                          |                          |      | Down               | Partially Up |
| <input type="checkbox"/> | <a href="#">SM80vmpg</a> | Core | 5                  | 0            |

Select : All, None

**All Monitored SIP Entities**  
Run Monitor

9 Items

| <input type="checkbox"/> | SIP Entity Name                 |
|--------------------------|---------------------------------|
| <input type="checkbox"/> | <a href="#">CM71vmpg</a>        |
| <input type="checkbox"/> | <a href="#">StevesEP</a>        |
| <input type="checkbox"/> | <a href="#">StephensCM</a>      |
| <input type="checkbox"/> | <a href="#">EP72vmpg</a>        |
| <input type="checkbox"/> | <a href="#">EP_Oceana</a>       |
| <input type="checkbox"/> | <a href="#">CS1KPG1</a>         |
| <input type="checkbox"/> | <a href="#">CM80vmpg</a>        |
| <input type="checkbox"/> | <a href="#">ASBCE8vmpg</a>      |
| <input type="checkbox"/> | <a href="#">AA Messaging V7</a> |

Select : All, None

The SIP Entity should show as **UP** as it is shown below.

**SIP Entity, Entity Link Connection Status**  
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

**All Entity Links to SIP Entity: ASBCE8vmpg**  
Summary View

1 Item Filter: Enable

|                       | Session Manager Name     | IP Address Family | SIP Entity Resolved IP | Port | Proto. | Deny  | Conn. Status | Reason Code   | Link Status |
|-----------------------|--------------------------|-------------------|------------------------|------|--------|-------|--------------|---------------|-------------|
| <input type="radio"/> | <a href="#">SM80vmpg</a> | IPv4              | 10.10.40.158           | 5061 | TLS    | FALSE | UP           | 200 Keepalive | UP          |

Select : None



## 12. Conclusion

These Application Notes describe the configuration used to verify Syntec CardEasy interoperates with Avaya Session Border Controller for Enterprise R8.0, Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Application Enablement Services R8.0.1. The solution outlined in these Application Notes describe two unique and separate connections between the CardEasy solution from Syntec and the Avaya solution. All functionality and serviceability test cases were completed successfully.

## 13. Additional References

This section references the Avaya and Presence Suite product documentation that are relevant to these Application Notes.

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

- [1] *Deploying Avaya Session Border Controller in Virtualized Environment*- Release 8.0
- [2] *Administering Avaya Session Border Controller for Enterprise* - Release 8.0
- [3] *Administering Avaya Aura® Communication Manager* – Release 8.0
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0
- [5] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 8.0
- [6] *Administering Avaya Aura® Session Manager* – Release 8.0

Documentation for CardEasy can be obtained by contacting Syntec (see **Section 2.3**).

---

**©2019 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 DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).