



Avaya Solution & Interoperability Test Lab

Application Notes for Syntec CardEasy CPE with Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using a SIP trunk - Issue 1.0

Abstract

These Application Notes describe the configuration required to allow Syntec CardEasy CPE to interoperate with Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using a SIP Trunk. Syntec CardEasy CPE 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

The configuration used in these application notes was used to verify that Syntec CardEasy CPE interoperates with Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using a SIP Trunk. The CardEasy CPE 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. The Syntec CardEasy CPE masks DTMF digits and Speech during the credit card verification process. Avaya Aura Application Enablement Services is used to identify the Agent Called using DTMF to send a reference number (EPID) to the CardEasy CPE.

2. General Test Approach and Test Results

The general test approach was to configure the CardEasy CPE to communicate with the Avaya Session Border Controller for Enterprise (Avaya SBCE) and Communication Manager (CM) via a SIP trunk. The Syntec EPID application was connected to Application Enablement Services (AES) and transmitted DTMF to the CardEasy CPE 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 or spoken credit card details are masked and hidden from the agent and confirmation is sent to the Agents payment 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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on receiving calls in different call scenarios and completing a credit card payment transaction. The tests included:

- Call Placed with Available Agents.
- Calls on Hold, Mute and Transferred.
- Credit Card Transaction with valid and invalid details.
- Failover/Service – Tests the behaviour of the CardEasy CPE during certain failed conditions.

2.2. Test Results

All Tests were executed successfully.

2.3. Support

Technical Support can be obtained for Syntec products from the following.

Web: <https://support.syntec.co.uk/portal/syntec>

Email: support@syntec.co.uk

Telephone: +44 (0) 207 741 8000

3. Reference Configuration

Figure 1 below shows the system configuration for the interoperability between Syntec CardEasy CPE, Session Border Controller for Enterprise and Communication Manager using a SIP trunk. Avaya 9611g H323 IP Deskphones were used with an Avaya Call Center Elite Agent logged in to receive incoming calls.

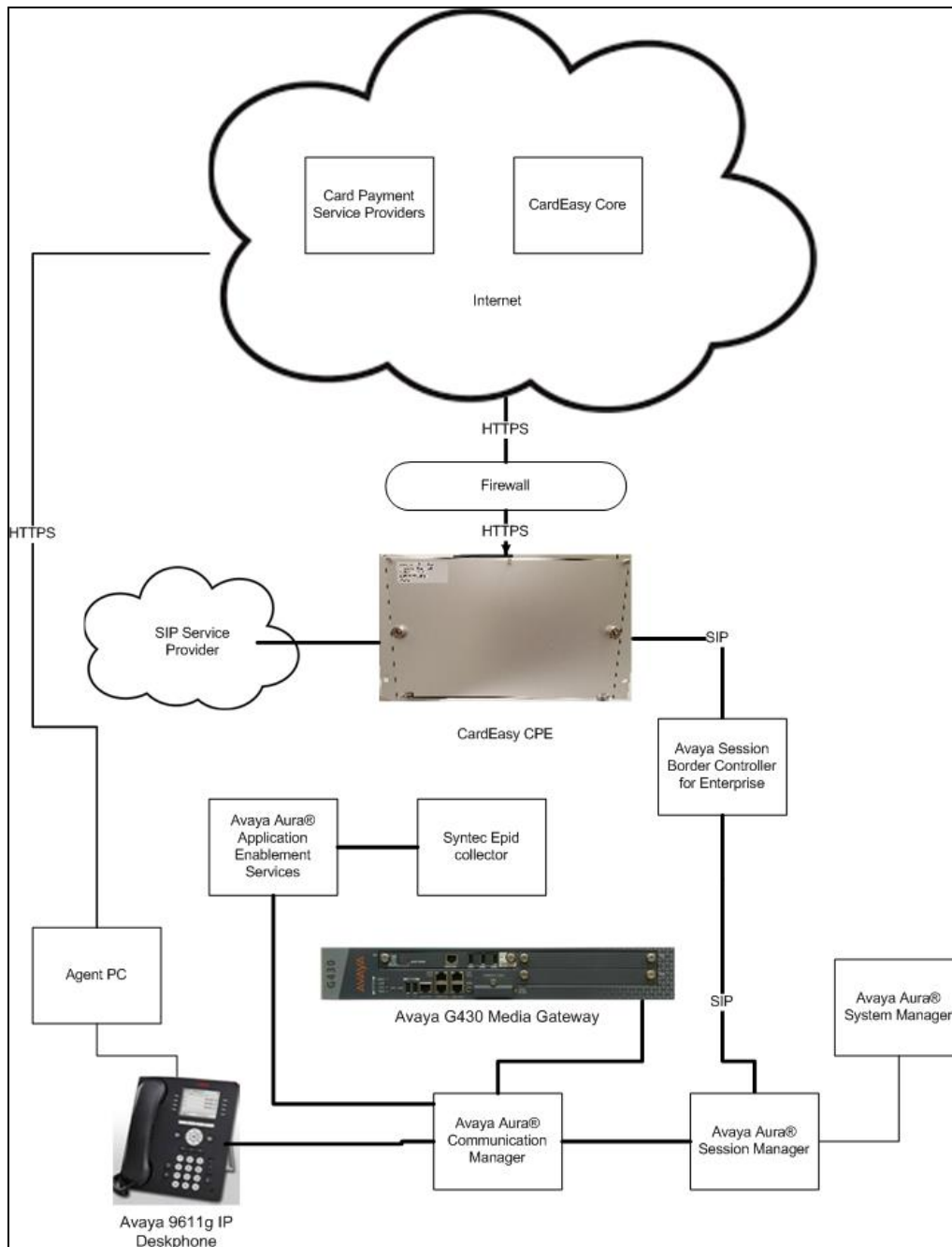


Figure 1: Syntec CardEasy CPE with Session Border Controller for Enterprise and Communication Manager using a SIP Trunk

4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|--|---|
| Avaya Aura® Communication Manager running on a VMware Virtual Server | R7.0.1.2 R017x.00.0.441.0 Version 7.0.1.2.0.441.23523 Patch: <ul style="list-style-type: none"> • Kernel-2.6.32.3.1.e16.AV4 • PLAT-rhel6.5-0050 |
| Avaya G430 Media Gateway | 37.41.0/1 |
| Avaya Session Border Controller for Enterprise | 7.1.0.0-04-11122 |
| Avaya Aura® Application Enablement Services | 7.0.1.0.3.15-0 |
| Avaya Aura® Session Manager | 7.0.1.2.701230 |
| Avaya Aura® System Manager | Version: 7.0.1.2 Build: 7.0.0.0.16266 Software Update Revision: 7.0.1.2.086007 Service Pack 2 |
| Avaya 9611g IP Deskphone (H323) | 6.6229 |
| Syntec CardEasy CPE | V2.3.21 |
| Syntec EPID Application | V1.0 |

5. Configure Avaya Aura® Communication Manager

This section describes the steps required to connect the CardEasy CPE using SIP. It is assumed that Communication Manager is installed and is in fully operational as this is out of the scope of this document. All configuration was administered using Communication Manager System Access Terminal (SAT). The steps documented are as follows.

- Check SIP Trunk ports
- Configure Dial Access Code (DAC) in Dial plan
- Add Signaling group
- Add Trunk group

5.1. Check SIP Trunk Capacity

From the command line use the command **display system-parameters customer-options**. On **Page 2** check that there are sufficient **Administered SIP Trunks** available.

| display system-parameters customer-options | | Page 2 of 10 |
|---|--------------|--------------|
| OPTIONAL FEATURES | | |
| IP PORT CAPACITIES | USED | |
| Maximum Administered H.323 Trunks: | 12000 | 16 |
| 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: | 41000 | 1 |
| Maximum Video Capable IP Softphones: | 18000 | 4 |
| Maximum Administered SIP Trunks: | 24000 | 180 |
| Maximum Administered Ad-hoc Video Conferencing Ports: | 24000 | 0 |
| Maximum Number of DS1 Boards with Echo Cancellation: | 522 | 0 |
| Maximum TN2501 VAL Boards: | 128 | 0 |
| Maximum Media Gateway VAL Sources: | 250 | 0 |
| Maximum TN2602 Boards with 80 VoIP Channels: | 128 | 0 |
| Maximum TN2602 Boards with 320 VoIP Channels: | 128 | 0 |
| Maximum Number of Expanded Meet-me Conference Ports: | 300 | 0 |
| (NOTE: You must logoff & login to effect the permission changes.) | | |

5.2. Add Dial Access Code in Dialplan

Use the **change dialplan analysis** command and enter under **Dialed String** the leading number of the Dial Access Code (DAC) (**7** in the example), a **Total Length** of **3** and **Call Type** **dac**.

| change dialplan analysis | | | | | | Page 1 of 12 | | |
|--------------------------|--------------|-----------|---------------|--------------|-----------|-----------------|--------------|-----------|
| DIAL PLAN ANALYSIS TABLE | | | | | | | | |
| Location: all | | | | | | Percent Full: 1 | | |
| Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type |
| 2 | 7 | ext | | | | | | |
| 7 | 3 | dac | | | | | | |
| 8 | 4 | udp | | | | | | |
| * | 3 | fac | | | | | | |
| # | 3 | fac | | | | | | |

5.3. Configure Session Manager Node

For Communication Manager to communicate with Session Manager a node must be configured. The screen shot below shows **SM71676** with IP address **10.10.16.77** was used.

Note: 10.10.16.77 IP address of Session Manager SIP Signaling Interface.

change node-names ip

Page 1 of 2

IP NODE NAMES

| Name | IP Address |
|----------------|--------------------|
| AES63RP | 10.10.60.210 |
| SM71676 | 10.10.16.77 |
| default | 0.0.0.0 |
| procr | 10.10.16.211 |
| procr6 | :: |

5.4. Configure Signaling Group

A signaling group is required before a trunk-group can be configured. Use the **add signaling-group** command followed by next available signaling-group number to configure the following:

- **Group Type:** Enter **SIP**
- **Transport Method** Enter **tcp**
- **Near-end Node Name:** Enter **procr**
- **Far-end Node Name:** Enter **SM71676** (Session Manager Node as configured in **Section 5.3**)
- **Far-end Network Region:** Enter the appropriate Network region (i.e. **1**)
- **Far End Domain:** Enter the appropriate Domain

```
add signaling-group 1                                     Page 1 of 2
                                                         SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
Q-SIP? n
IP Video? n                        Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y 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
Near-end Node Name: procr              Far-end Node Name: SM71676
Near-end Listen Port: 5060             Far-end Listen Port: 5060
Far-end Network Region: 1

Far-end Domain: devconnect.local

Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3 IP Audio Hairpinning? n
Enable Layer 3 Test? y              Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

5.5. Configure Trunk Group

This section describes the Trunk Group configuration used during compliance testing. Use the **add trunk-group** command followed by next available Group number and configure the following:

- **Group Type:** Enter **sip**
- **Group Name:** Enter an informative name for the trunk (i.e. **To SM7.0 SIP**)
- **TAC** Enter a TAC number (i.e. **701**)
- **Service Type:** Enter **public-ntwrk**
- **Signaling Group:** Enter the Signaling Group number as configured in **Section 5.4**
- **Number of Members:** Enter the number of channels required to connect to Session Manger (during compliance testing 30 channels were used).

```
add trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                                     Group Type: sip          CDR Reports: y
  Group Name: To SM7.0 SIP                        COR: 1          TN: 1          TAC: 701
    Direction: two-way          Outgoing Display? n
    Dial Access? n
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 30
```

On page 3 enter **private** for **Numbering format**.

```
display trunk-group 1                               Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n          Measured: none
                               Maintenance Tests? y

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

                               Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

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 CPE SIP Trunk.

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 screen for the Avaya Session Border Controller for Enterprise. It features the Avaya logo in red at the top left. Below the logo, the text "Session Border Controller for Enterprise" is displayed. To the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, there are three paragraphs of legal disclaimer text. At the bottom, it states "© 2011 - 2016 Avaya Inc. All rights reserved."

AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Continue

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.

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.


All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2016 Avaya Inc. All rights reserved.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.

[Alarms](#) [Incidents](#) [Status](#) [Logs](#) [Diagnostics](#) [Users](#) [Settings](#) [Help](#) [Log Out](#)

Session Border Controller for Enterprise



Dashboard

[Administration](#)
[Backup/Restore](#)
[System Management](#)
 ▸ [Global Parameters](#)
 ▸ [Global Profiles](#)
 ▸ [PPM Services](#)
 ▸ [Domain Policies](#)
 ▸ [TLS Management](#)
 ▸ [Device Specific Settings](#)

Dashboard

| Information | | |
|------------------------------|------------------------------|-------------------------|
| System Time | 10:44:37 AM GMT | Refresh |
| Version | 7.1.0.0-04.11122 | |
| Build Date | Tue Oct 11 15:52:41 EDT 2016 | |
| License State | OK | |
| Aggregate Licensing Overages | 0 | |
| Peak Licensing Overage Count | 0 | |
| Last Logged in at | 01/13/2017 10:22:27 GMT | |
| Failed Login Attempts | 0 | |

| Alarms (past 24 hours) | |
|------------------------|--|
| None found. | |

| Installed Devices | |
|-------------------|--|
| EMS | |
| GSSCP_45 | |

| Incidents (past 24 hours) | |
|---------------------------|--|
| None found. | |

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 internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side and click on **Add**.

The screenshot shows the 'Network Management' section of the Avaya SBCE interface. On the left is a sidebar menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The 'Device Specific Settings' option is selected, and within it, 'Network Management' is highlighted. The main content area is titled 'Network Management:' and contains two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, displaying a table with columns: Name, Gateway, Subnet Mask / Prefix Length, Interface, and IP Address. An 'Add' button is located at the top right of the table.

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.
- 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 the 'Add Network' dialog box. It has a title bar with 'Add Network' and a close button (X). The dialog contains several input fields: 'Name' (with 'External' entered), 'Default Gateway' (with '192.168.122.9' entered), 'Network Prefix or Subnet Mask' (with '255.255.255.128' entered), and 'Interface' (a dropdown menu with 'B1' selected). An 'Add' button is at the bottom right. Below these fields is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The 'IP Address' column has a value of '192.168.122.46'. The 'Public IP' column has a button labeled 'Use IP Address'. The 'Gateway Override' column has a button labeled 'Use Default'. A 'Delete' button is at the bottom right of the table. A 'Finish' button is at the bottom center of the dialog.

Perform the same task to define the external interface. From **Device Specific Settings** → **Network Management** in the main menu on the left hand side and click on **Add**.

Enter details in the dialogue box (not shown):

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address for the Avaya SBCE in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

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

Network Management:

Devices **Interfaces** **Networks**

Add

| Name | Gateway | Subnet Mask / Prefix Length | Interface | IP Address | Edit | Delete |
|----------|---------------|-----------------------------|-----------|----------------|------|--------|
| Internal | 10.10.9.1 | 255.255.255.0 | A1 | 10.10.9.81 | Edit | Delete |
| External | 192.168.122.9 | 255.255.255.128 | B1 | 192.168.122.46 | 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.

Network Management:

Devices **Interfaces** **Networks**

Add VLAN

| Interface Name | VLAN Tag | Status |
|----------------|----------|----------|
| A1 | | Enabled |
| A2 | | Disabled |
| B1 | | Disabled |
| | | Disabled |

Message from webpage

Are you sure you wish to change the status of Interface to Enabled?

OK Cancel

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 Session Manager and the Avaya SBCE, and between the Avaya SBCE and the Card easy CPE. A signaling and media interface was required on both the internal and external sides of the Avaya SBCE. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

6.3.1. Signaling Interfaces

To define the signaling interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Signaling Interface** in the main menu on the left hand side. Details of transport protocol and ports for the external and internal SIP signaling are entered here.

- Select **Add** (not shown) and enter details of the external signaling interface in the pop-up menu.
- 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 **192.168.122.46** 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 CPE.
- Click on **Finish**

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
DMZ Services
TURN/STUN Service
SNMP

Add Signaling InterfaceX

TLS Port has been disabled because no [TLS Server Profiles](#) exist. Create a new [TLS Server Profile](#) to allow creation of a TLS enabled Signaling Interface.

NameExternal

IP Address

External (B1, VLAN 0)

192.168.122.46

TCP Port

Leave blank to disable

5060

UDP Port

Leave blank to disable

5060

TLS Port

Leave blank to disable

TLS Profile

None

Enable Shared Control

☐

Shared Control Port

Finish

The internal signaling interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signaling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signaling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TCP** port number, **5060** is used for Session Manager.

The following screenshot shows details of the signaling interfaces:

Signaling Interface:

Devices

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

| Name | Signaling IP Network | TCP Port | UDP Port | TLS Port | TLS Profile | |
|----------|---|----------|----------|----------|-------------|-------------|
| External | 192.168.122.46 External (B1, VLAN 0) | --- | 5060 | --- | None | Edit Delete |
| Internal | 10.10.9.81 Internal (A1, VLAN 0) | 5060 | 5060 | --- | None | Edit Delete |

6.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** in the main 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.

- Select **Add** (not shown) and enter details of the external media interface in the pop-up menu.
- 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 **192.168.122.46**.
- Define the **RTP Port Range** for the media path with the CardEasy CPE, during testing this was left at default values of **35000 - 40000**.

System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface

Add Media Interface X

Name
External

IP Address
External (B1, VLAN 0)
192.168.122.46

Port Range
35000 - 40000

Finish

The internal media interfaces are defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

Media Interface:

Devices

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

| Name | Media IP Network | Port Range | |
|----------|---|---------------|-------------|
| Internal | 10.10.9.81 Internal (A1, VLAN 0) | 35000 - 40000 | Edit Delete |
| External | 192.168.122.46 External (B1, VLAN 0) | 35000 - 40000 | Edit Delete |

6.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the CardEasy CPE is connected as the Trunk Server and the Session Manager is connected as the Call Server.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the CardEasy CPE, click on **Add**.

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise AVAYA

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles Domain DoS **Server Interworking** Media Forking

Interworking Profiles: cs2100

Add Clone

Interworking Profiles

cs2100

avaya-ru

Session Manager

Session Manager

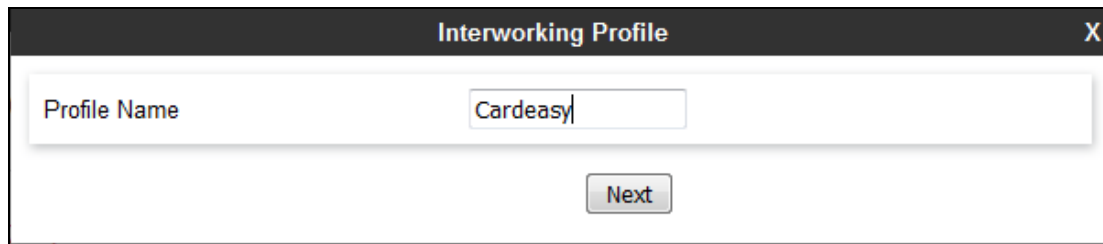
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

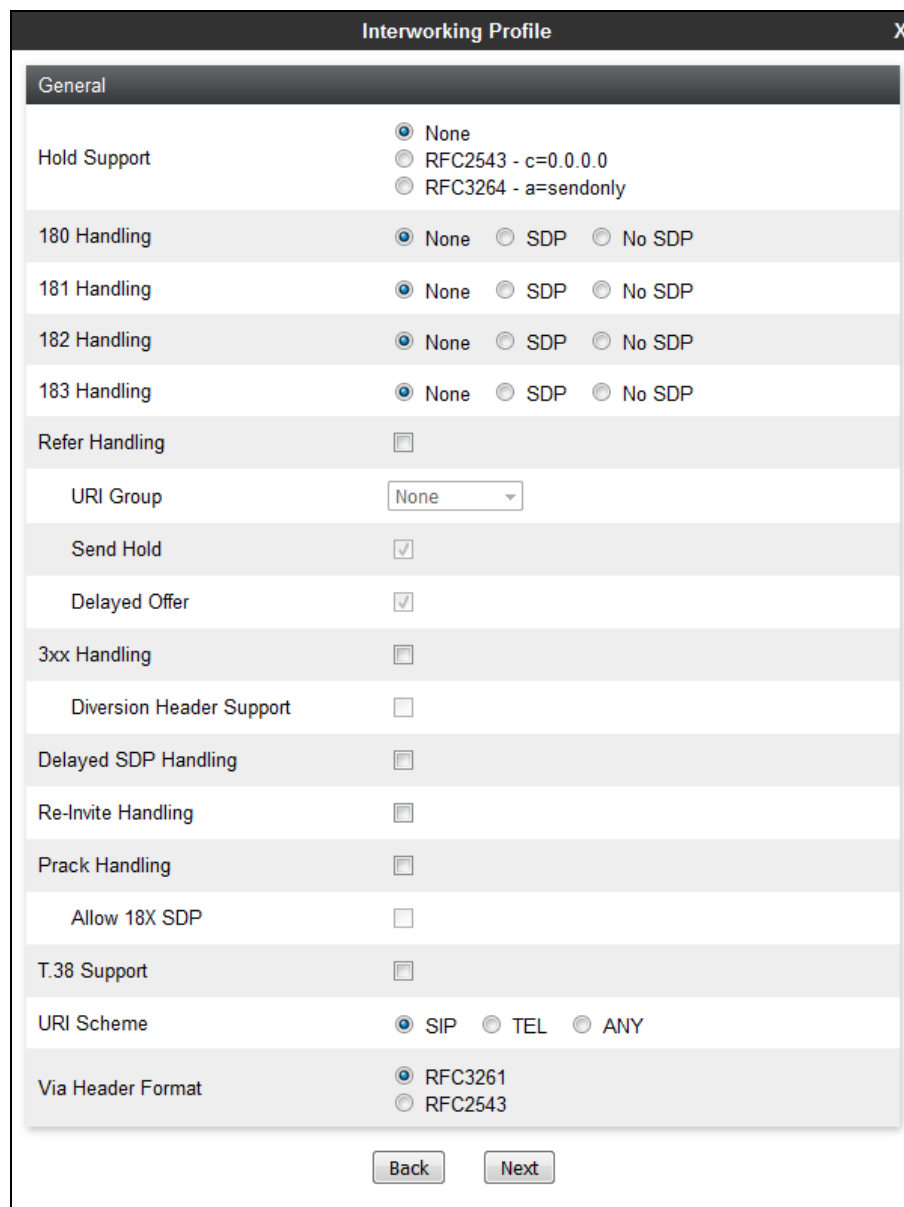
| | |
|--------------|---------|
| Hold Support | RFC3264 |
| 180 Handling | None |
| 181 Handling | None |

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



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Cardeasy". Below this field is a button labeled "Next".

The general settings are default for Interworking Profile:



The screenshot shows the "Interworking Profile" dialog box with the "General" tab selected. The settings are as follows:

| Setting | Value |
|--------------------------|--|
| Hold Support | <input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly |
| 180 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 181 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 182 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 183 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| Refer Handling | <input type="checkbox"/> |
| URI Group | None |
| Send Hold | <input checked="" type="checkbox"/> |
| Delayed Offer | <input checked="" type="checkbox"/> |
| 3xx Handling | <input type="checkbox"/> |
| Diversion Header Support | <input type="checkbox"/> |
| Delayed SDP Handling | <input type="checkbox"/> |
| Re-Invite Handling | <input type="checkbox"/> |
| Prack Handling | <input type="checkbox"/> |
| Allow 18X SDP | <input type="checkbox"/> |
| T.38 Support | <input type="checkbox"/> |
| URI Scheme | <input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY |
| Via Header Format | <input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543 |

At the bottom of the dialog, there are two buttons: "Back" and "Next". The "Next" button is highlighted.

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

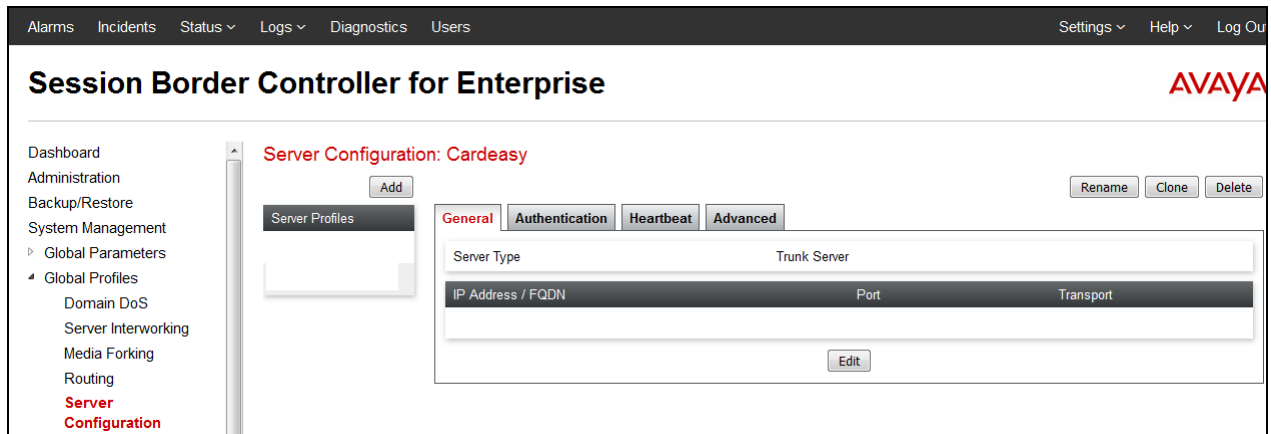
In the final dialogue box, leave the **Record Routes** at the default setting of **Both Sides** and ensure that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk. Click on **Finish**

Repeat the process to define **Server Interworking** for Session Manager using the same parameter settings.

6.5. Define Servers

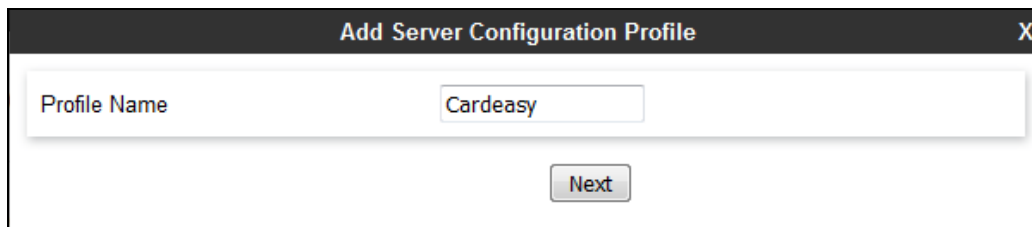
A server definition is required for each server connected to the Avaya SBCE. The CardEasy CPE is connected as a Trunk Server. Session Manager is connected as a Call Server.

To define the CardEasy CPE Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add**.



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Server Configuration' highlighted under 'Global Profiles'. The main content area is titled 'Server Configuration: Cardeasy' and features an 'Add' button. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a 'Server Type' dropdown set to 'Trunk Server'. Below this is a table with columns for 'IP Address / FQDN', 'Port', and 'Transport'. An 'Edit' button is located at the bottom right of the table. On the right side of the configuration area, there are buttons for 'Rename', 'Clone', and 'Delete'.

Enter an appropriate name in the pop-up menu.



The screenshot shows a pop-up dialog box 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 CPE 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**.

The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It contains the following fields and controls:

- Server Type**: A dropdown menu with "Trunk Server" selected.
- TLS Client Profile**: A dropdown menu with "None" selected.
- Add**: A button to add a new entry.
- Table**: A table with three columns: "IP Address / FQDN", "Port", and "Transport".

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 192.168.1.2 | 5060 | TCP |
- Delete**: A button to delete an entry.
- Back** and **Next**: Navigation buttons at the bottom.

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 CPE defined in **Section 6.4**.
- Leave the other fields at default settings.
- Click **Finish**.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains the following fields and controls:

- Enable DoS Protection**: A checkbox.
- Enable Grooming**: A checkbox.
- Interworking Profile**: A dropdown menu with "CardEasy" selected.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- Securable**: A checkbox.
- Enable FGDN**: A checkbox.
- TCP Failover Port**: A text box with "5060" entered.
- TLS Failover Port**: A text box with "5061" entered.
- Back** and **Finish**: Navigation buttons at the bottom.

Use the following process described to define the Call Server configuration for Session Manager if not already defined.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box (not shown).
- Ensure that the Interworking Profile defined for Session Manager in **Section 6.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box (not shown).

The following screenshots show the **General** and **Advanced** tabs of the completed Server Configuration:

Server Configuration: SM_31

Buttons: Add, Rename, Clone, Delete

Server Profiles: DT, **SM_31**

General | Authentication | Heartbeat | Advanced

Server Type: Call Server

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 10.10.9.31 | 5060 | TCP |

Edit

Server Configuration: SM_31

Buttons: Add, Rename, Clone, Delete

Server Profiles: DT, **SM_31**

General | **Advanced** | Authentication | Heartbeat

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile: Session_Manager

Signaling Manipulation Script: None

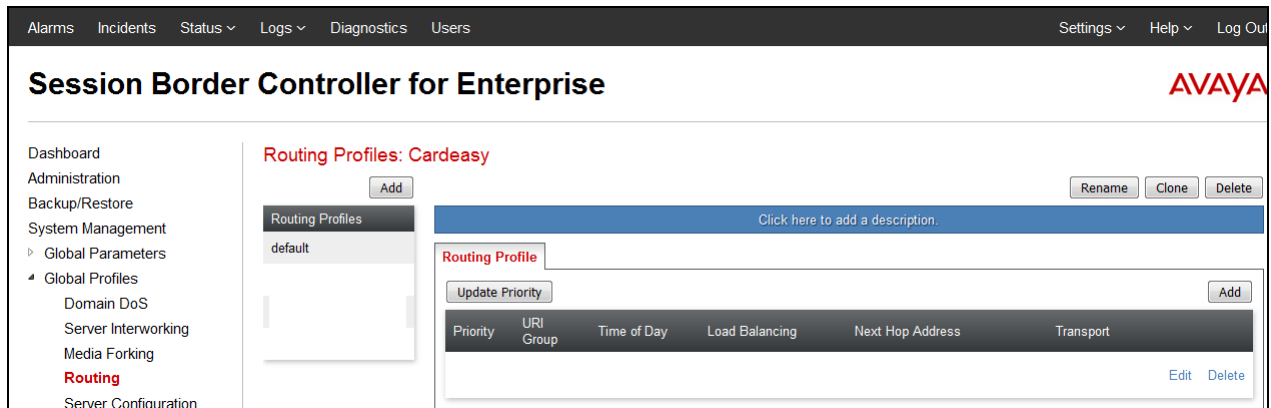
Securable ☐

Enable FGDN ☐

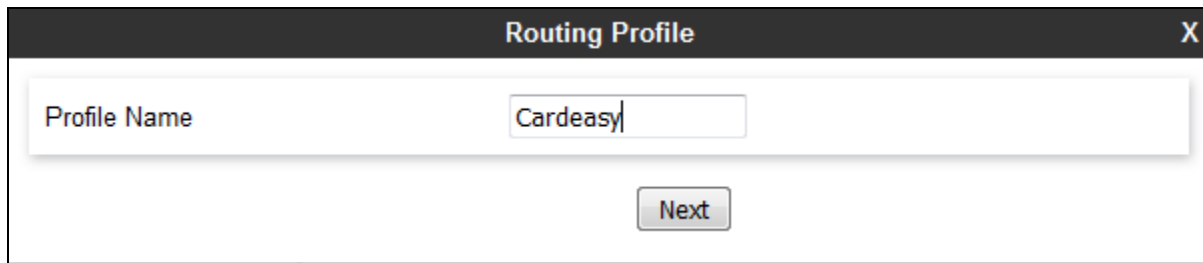
Edit

6.6. Define Routing

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



Enter an appropriate name in the dialogue box.



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 **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window. It has a title bar with 'Routing Profile' and a close button 'X'. The main area contains several fields: 'URI Group' with a dropdown showing '*', 'Time of Day' with a dropdown showing 'default', 'Load Balancing' with a dropdown showing 'Priority', 'NAPTR' with an unchecked checkbox, 'Transport' with a dropdown showing 'None', 'Next Hop Priority' with a checked checkbox, 'Next Hop In-Dialog' with an unchecked checkbox, 'Ignore Route Header' with an unchecked checkbox, 'ENUM' with an unchecked checkbox, and 'ENUM Suffix' with an empty text field. Below these fields is an 'Add' button. At the bottom, there is a table with columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The table contains one row with values: '1', 'Custom', '10.10.10.10', and 'None'. To the right of this row is a 'Delete' button. Below the table are 'Back' and 'Finish' buttons.

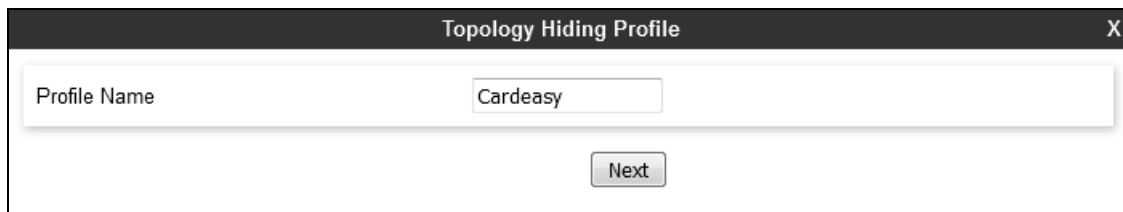
Repeat the process for the Routing Profile for Session Manager. The following screenshot shows the completed configuration:

The screenshot shows the 'Routing Profiles: SM_31' configuration window. It has a title bar with 'Routing Profiles: SM_31'. On the left, there is a sidebar with a list of routing profiles: 'default', 'SM_31' (highlighted in red), and 'DT'. Above the list is an 'Add' button. On the right, there are buttons for 'Rename', 'Clone', and 'Delete'. The main area has a blue header with the text 'Click here to add a description.'. Below this is a 'Routing Profile' section with an 'Update Priority' button and an 'Add' button. Below these buttons is a table with columns: 'Priority', 'URI Group', 'Time of Day', 'Load Balancing', 'Next Hop Address', and 'Transport'. The table contains one row with values: '1', '*', 'default', 'Priority', '10.10.9.31', and 'UDP'. To the right of this row are 'Edit' and 'Delete' buttons.

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.

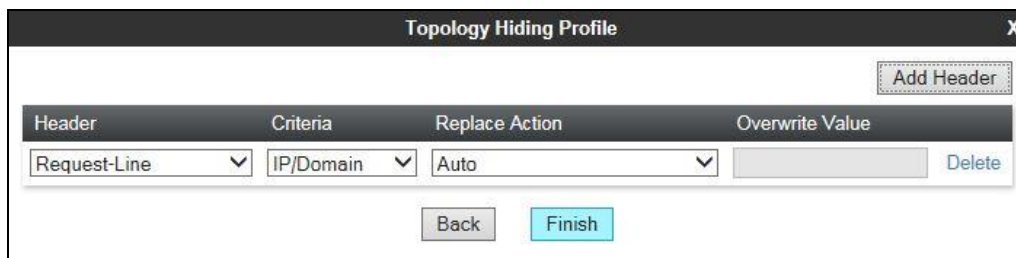
To define Topology Hiding for CardEasy, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Click on **Add** (not shown) to bring up a dialogue box, assign an appropriate name and click on **Next** to configure Topology Hiding for each header as required:



The screenshot shows a dialog box titled "Topology Hiding Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Cardeasy". Below this field is a button labeled "Next".

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

- Click on **Add Header** and select 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 the "Topology Hiding Profile" dialog box with the "Add Header" button in the top right corner. Below this button is a table with four columns: "Header", "Criteria", "Replace Action", and "Overwrite Value". The first row of the table has the following values: "Request-Line" in the "Header" column, "IP/Domain" in the "Criteria" column, "Auto" in the "Replace Action" column, and an empty field in the "Overwrite Value" column. To the right of the "Overwrite Value" field is a "Delete" button. Below the table are two buttons: "Back" and "Finish".

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

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

Topology Hiding Profiles:

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco_th_profile

SM_31

Cardeasy

Click here to add a description.

Topology Hiding

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

Edit

To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for CardEasy CPE. Do this by highlighting the profile defined for CardEasy and clicking on **Clone**. Enter an appropriate name for Session Manager and click on **Next** (not shown). Make any changes where required, in the test environment the settings were left at the same values.

Topology Hiding Profiles:

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco_th_profile

SM_31

Click here to add a description.

Topology Hiding

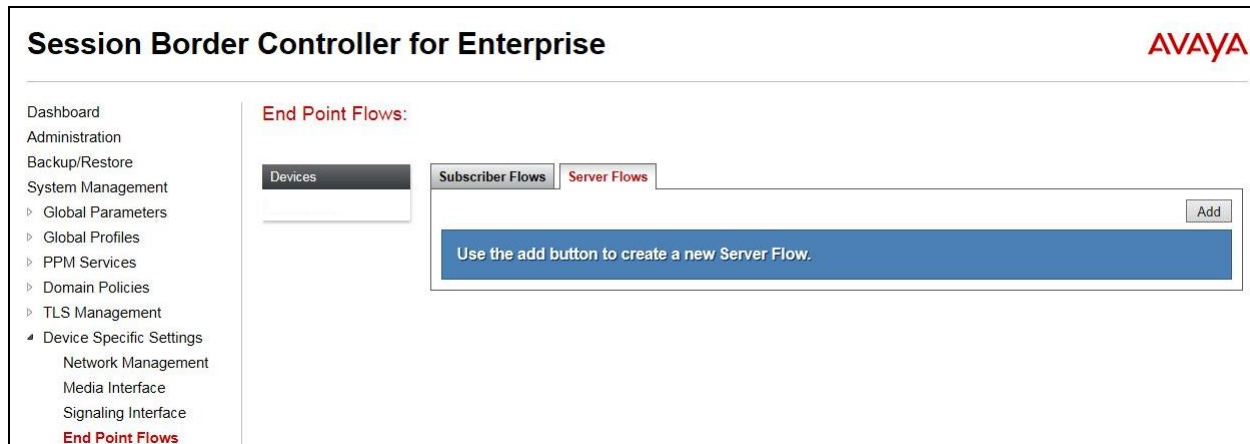
| Header | Criteria | Replace Action | Overwrite Value |
|--------------|-----------|----------------|-----------------|
| Referred-By | IP/Domain | Auto | --- |
| To | IP/Domain | Auto | --- |
| Via | IP/Domain | Auto | --- |
| Request-Line | IP/Domain | Auto | --- |
| SDP | IP/Domain | Auto | --- |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

Edit

6.8. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the CardEasy CPE. This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the CardEasy CPE and vice versa.

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



Define the Server flow for the CardEasy CPE as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for the CardEasy CPE, in the test environment **CardEasy_In** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the 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 **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 CPE defined in **Section 6.7** and click **Finish**.

| Edit Flow: Cardeasy_In | |
|-------------------------------|-------------|
| Flow Name | Cardeasy_In |
| Server Configuration | Cardeasy |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | Internal |
| Signaling Interface | External |
| Media Interface | External |
| Secondary Media Interface | None |
| End Point Policy Group | default-low |
| Routing Profile | SM 31 |
| Topology Hiding Profile | Cardeasy |
| Signaling Manipulation Script | None |
| Remote Branch Office | Any |
| <div>Finish</div> | |

Define a Server Flow for Session Manager as follows:

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

The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a corresponding input field or dropdown menu. The fields are as follows:

| Field Label | Value |
|-------------------------------|----------------|
| Flow Name | SM_Call_Server |
| Server Configuration | SM_31 |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | External |
| Signaling Interface | Internal |
| Media Interface | Internal |
| Secondary Media Interface | None |
| End Point Policy Group | default-low |
| Routing Profile | Cardeasy |
| Topology Hiding Profile | SM_31 |
| Signaling Manipulation Script | None |
| Remote Branch Office | Any |

At the bottom of the window, there is a "Finish" button.

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar lists various system management options, with "End Point Flows" highlighted at the bottom. The main content area is titled "End Point Flows: Wilson1971SBCE7" and features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of server configurations. The table has columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. Two configurations are listed: "Cardeasy" and "SM77". Each configuration has a "View" link and a "Delete" link. The "Cardeasy" configuration has a "Clone" link, while the "SM77" configuration has a "Clone" link. The "Add" button is located at the top right of the table.

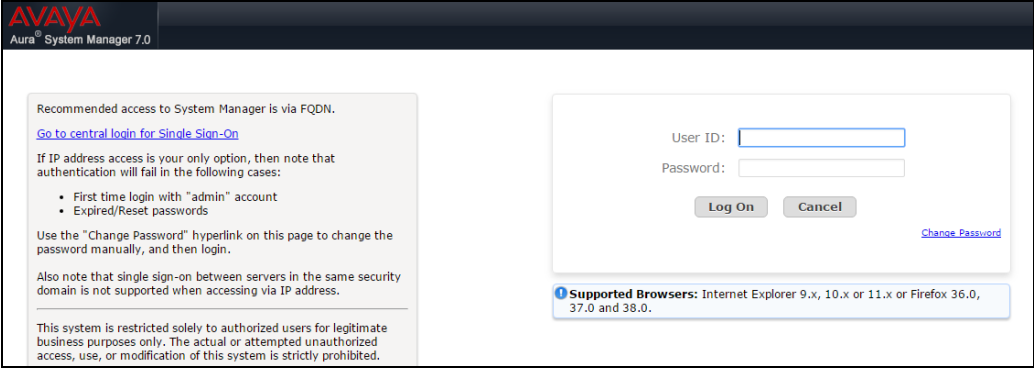
| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile | |
|----------|-------------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| 1 | Cardeasy_In | * | Internal_In | External_In | default-low | SM, 31 | View Clone Edit Delete |
| 1 | SM31_In | * | External_In | Internal_In | default-low | Cardeasy | View Clone Edit Delete |

7. Configure Avaya Aura® Session Manager

This section describes the steps required to configure Session Manager to connect to Avaya SBCE and forward calls to Communication Manager. It is assumed that Session Manager has been installed and configured for other connectivity and is out with the scope of this document. All configuration was done via the Avaya Aura® System Manager web interface.

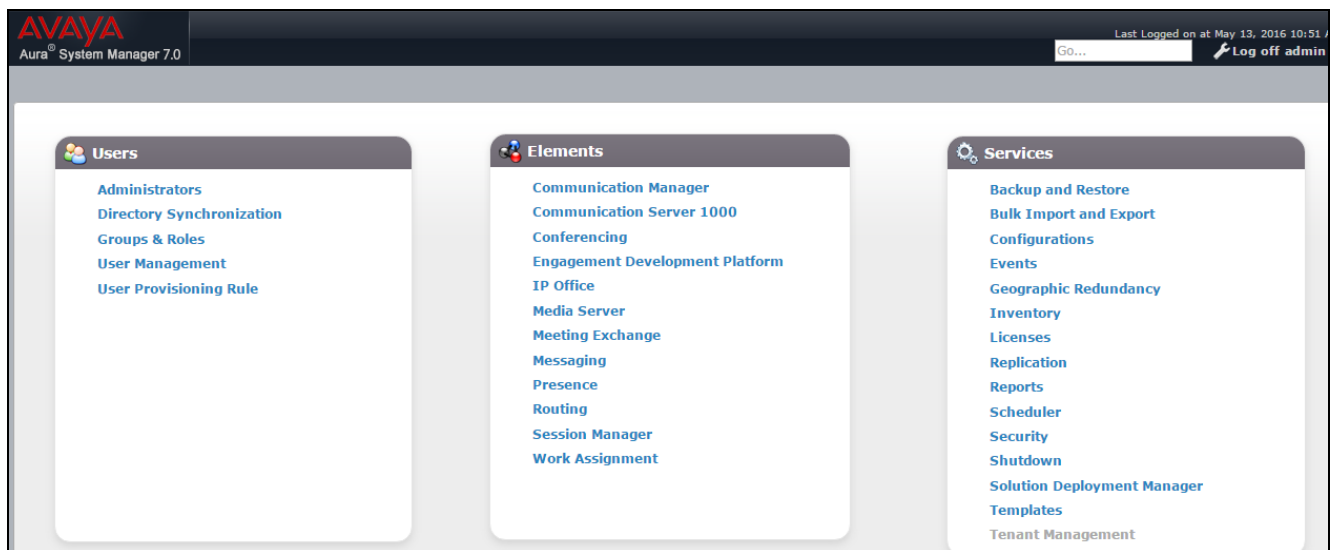
7.1. Log into System Manager

Using an internet browser go to **https://<system Manager IP>/SMGR**. Use valid credentials to log in.



The login page for Avaya Aura System Manager 7.0. It features a dark header with the Avaya logo and 'Aura System Manager 7.0'. The main content area is white. On the left, there is a text block with instructions: 'Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with "admin" account • Expired/Reset passwords. Use the "Change Password" hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address. This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.' On the right, there is a login form with fields for 'User ID:' and 'Password:', 'Log On' and 'Cancel' buttons, and a 'Change Password' link. At the bottom, a blue box lists 'Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.'

When logged in the Dashboard will be shown.



From the Dashboard select **Routing** from the **Elements** section. From the left hand menu Select **SIP Entities** and click on **New** (not shown).

- Set a Descriptive **Name**
- Enter the **FQDN or IP Address** of the Session Border Controller for Enterprise
- Set Type as **SIP Trunk**

Other entries can be default.

- Click on **Commit**.

| | |
|---------------------|---|
| Domains | <div><h2>SIP Entity Details</h2><div>Commit Cancel</div><div>General</div><div><div>* Name: SBCE60</div><div>* FQDN or IP Address: 10.10.16.60</div><div>Type: SIP Trunk</div><div>Notes:</div><div>Adaptation:</div><div>Location: SBCE60</div><div>Time Zone: Europe/Dublin</div><div>* SIP Timer B/F (in seconds): 4</div><div>Credential name:</div><div>Securable:</div><div>Call Detail Recording: egress</div></div><div>Loop Detection</div><div><div>Loop Detection Mode: On</div><div>Loop Count Threshold: 5</div><div>Loop Detection Interval (in msec): 200</div></div><div>SIP Link Monitoring</div><div><div>SIP Link Monitoring: Use Session Manager Configuration</div></div></div> |
| Locations | |
| Adaptations | |
| SIP Entities | |
| Entity Links | |
| Time Ranges | |
| Routing Policies | |
| Dial Patterns | |
| Regular Expressions | |
| Defaults | |
| | |
| | |
| | |
| | |
| | |
| | |

From the left hand menu select **Entity Links** and click on **New** (not shown).

- Enter a descriptive Name
- Set **SIP Entity 1** as the Session Manager used to forward calls to Communication Manager.
- Set **SIP Entity 2** as the Avaya SBCE added above.
- Set **Protocol** as **TCP** (port is set to **5060** automatically)
- Click on **Commit**

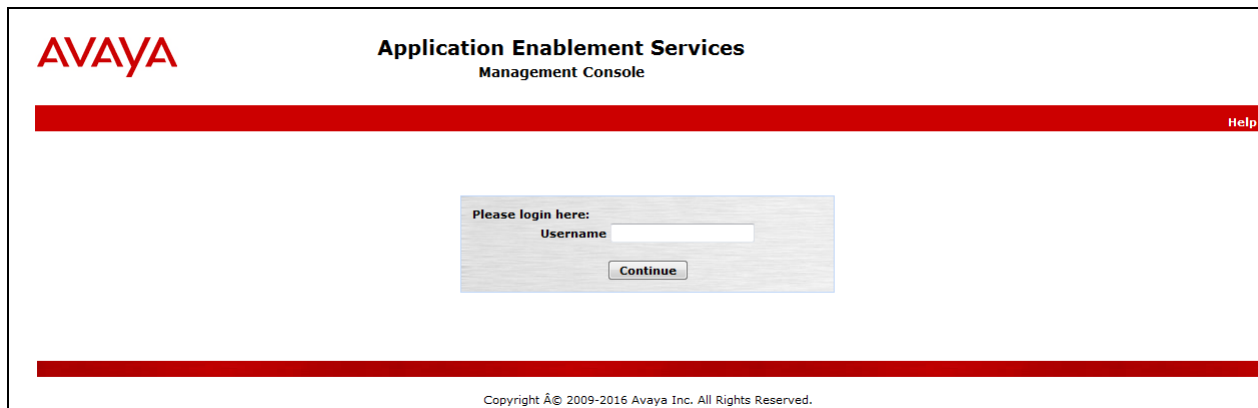
| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | DNS Override | Port |
|------------|--------------|----------|-------|--------------|--------------------------|-------|
| *SBCE60_EL | *Q SM71676 | TCP | *5060 | *Q SBCE60 | <input type="checkbox"/> | *5060 |

8. Configure Avaya Aura® Application Enablement Services

This section describes the configuration steps required to allow the CardEasy EPID application to send the Agent Identifier digits to the CardEasy CPE. It is assumed that the Application Enablement Services has been installed and configured for connectivity to Communication Manager.

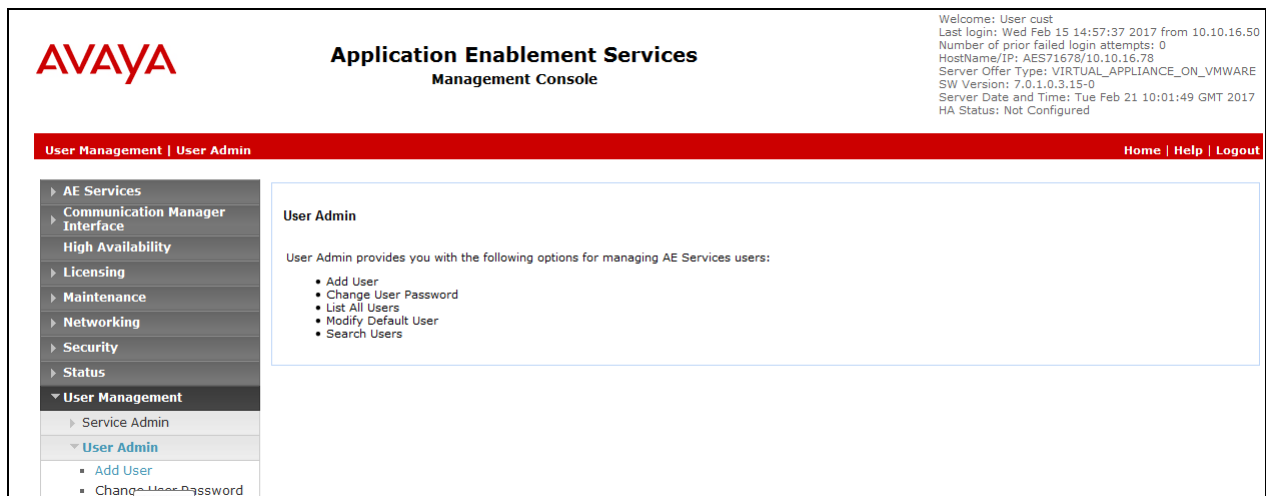
8.1. Log into Avaya Aura® Application Enablement Services

Using an internet browser go to **https://<application enablement server IP>**. Log in with the appropriate credentials.



8.2. Add CTI User

From the left hand menu select **User Management→User Admin→Add User**.



On the resultant screen enter:

- A descriptive **User Id**, **Common Name** and **Surname**.
- A **User Password** that will be used in the EPID Collection utility configuration.
- Set **CT User** to **Yes**.

Click on **Apply** (not shown) to save changes.


The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message: 'Welcome: User cust', 'Last login: Wed Feb 15 14:57:37 2017 from 10.10.16.50', 'Number of prior failed login attempts: 0', 'HostName/IP: AES71678/10.10.16.78', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.3.15-0', 'Server Date and Time: Tue Feb 21 10:04:46 GMT 2017', and 'HA Status: Not Configured'. The main navigation menu on the left includes 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', and 'User Management'. The 'User Management' menu is expanded, showing 'Service Admin', 'User Admin', and 'Add User'. The 'Add User' form is displayed, with fields for 'User Id', 'Common Name', 'Surname', 'User Password', 'Confirm Password', 'Admin Note', 'Avaya Role', 'Business Category', 'Car License', 'CM Home', 'CSS Home', and 'CT User'. The 'CT User' field is set to 'Yes'.

8.3. Apply CTI User Settings

From the left hand menu select **Security**→**Security Database**→**CTI Users**→**List All Users**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message: 'Welcome: User cust', 'Last login: Wed Feb 15 14:57:37 2017 from 10.10.16.50', 'Number of prior failed login attempts: 0', 'HostName/IP: AES71678/10.10.16.78', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.3.15-0', 'Server Date and Time: Tue Feb 21 10:06:39 GMT 2017', and 'HA Status: Not Configured'. The main navigation menu on the left includes 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', and 'User Management'. The 'Security' menu is expanded, showing 'Account Management', 'Audit', 'Certificate Management', 'Enterprise Directory', 'Host AA', 'PAM', 'Security Database', and 'CTI Users'. The 'Security Database' menu is expanded, showing 'Control', 'CTI Users', and 'List All Users'. The 'CTI Users' page is displayed, with a heading 'CTI Users' and a description: 'CTI Users provides you with the followings for managing users who are members of the Security Database:'. The page lists two options: 'List All Users' and 'Search Users'.

Select the user added in **Section 8.2** and click on **Edit**



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Wed Feb 15 14:57:37 2017 from 10.10.16.50
 Number of prior failed login attempts: 0
 HostName/IP: AES71678/10.10.16.78
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.1.0.3.15-0
 Server Date and Time: Tue Feb 21 10:07:35 GMT 2017
 HA Status: Not Configured

Security | Security Database | CTI Users | List All Users
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
 - List All Users
 - Search Users
 - Devices

CTI Users

| User ID | Common Name | Worktop Name | Device ID |
|---|-------------|--------------|-----------|
| <input checked="" type="radio"/> cardeasy | cardeasy | NONE | NONE |
| <input type="radio"/> pomcti | POM | NONE | NONE |
| <input type="radio"/> presence | presence | NONE | NONE |

Set the following and then click on **Apply Changes** to save changes.

- **Call and Device Control** to **Any**
- **Device Monitoring** to **Any**
- **Calls on a Device Monitoring** to **Any**
- **Select Call Monitoring**
- **Allow Routing on Listed Devices** to **Any**



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Wed Feb 15 14:57:37 2017 from 10.10.16.50
 Number of prior failed login attempts: 0
 HostName/IP: AES71678/10.10.16.78
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.1.0.3.15-0
 Server Date and Time: Tue Feb 21 10:10:26 GMT 2017
 HA Status: Not Configured

Security | Security Database | CTI Users | List All Users
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
 - List All Users

Edit CTI User

User Profile:

User ID
Common Name
Worktop Name
Unrestricted Access

cardeasy
cardeasy
NONE
☐

Call and Device Control:

Call Origination/Termination and Device Status

Any

Call and Device Monitoring:

Device Monitoring
Calls On A Device Monitoring
Call Monitoring

Any
Any
☒

Routing Control:

Allow Routing on Listed Devices

Any

9. Configure CardEasy CPE

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 describes the steps to show that the SIP trunk is operational.

11.1. Verify SIP Trunk on Communication Manager

Use the **status trunk n** where **n** is the SIP trunk number. Make sure that all trunks are showing as **in-service/idle**. Make a call into Communication Manager and make sure that the call can be answered.

| status trunk 11 | | | |
|--------------------|--------|-----------------|------------------------------|
| TRUNK GROUP STATUS | | | |
| Member | Port | Service State | Mtce Connected Ports Busy |
| 0011/001 | T00266 | in-service/idle | no |
| 0011/002 | T00267 | in-service/idle | no |
| 0011/003 | T00268 | in-service/idle | no |
| 0011/004 | T00269 | in-service/idle | no |
| 0011/005 | T00270 | in-service/idle | no |
| 0011/006 | T00271 | in-service/idle | no |
| 0011/007 | T00272 | in-service/idle | no |
| 0011/008 | T00273 | in-service/idle | no |
| 0011/009 | T00274 | in-service/idle | no |
| 0011/010 | T00275 | in-service/idle | no |

11.2. Verify CardEasy

During a call, process a credit card transaction and verify that an **Authorised** response is returned.

| Payment Response | | | | | | | | | | |
|------------------|--|--|-------|----------|----------|---------|--------------|----|---------|-----|
| BenignPAN: | 426397*****1307 | | | | | | | | | |
| response: | timestamp: 20170220110537 | | | | | | | | | |
| | merchantid: syntec | | | | | | | | | |
| | account: internet | | | | | | | | | |
| | orderid: 4hvw25cxpk2k | | | | | | | | | |
| | authcode: 12345 | | | | | | | | | |
| | result: 00 | | | | | | | | | |
| | cvnresult: M | | | | | | | | | |
| | avspostcoderesponse: M | | | | | | | | | |
| | avsaddressresponse: M | | | | | | | | | |
| | batchid: 398203 | | | | | | | | | |
| | message: [test system] Authorised | | | | | | | | | |
| | pasref: 1487588737517652 | | | | | | | | | |
| | timetaken: 0 | | | | | | | | | |
| | authtimetaken: 0 | | | | | | | | | |
| | cardissuer: | <table><tbody><tr><td>bank:</td><td>AIB BANK</td></tr><tr><td>country:</td><td>IRELAND</td></tr><tr><td>countrycode:</td><td>IE</td></tr><tr><td>region:</td><td>EUR</td></tr></tbody></table> | bank: | AIB BANK | country: | IRELAND | countrycode: | IE | region: | EUR |
| | bank: | AIB BANK | | | | | | | | |
| | country: | IRELAND | | | | | | | | |
| countrycode: | IE | | | | | | | | | |
| region: | EUR | | | | | | | | | |
| sha1hash: | 528cd7aaa58965efc2fe75673a176dbebded85b2 | | | | | | | | | |

11.3. Verify Avaya Aura® Application Enablement Services Connectivity

From the left hand menu select **Status**→**Status and Control**→**TSAPI Service Summary**. Click on **TLink Status**. The status should display **Talking** as shown below.

Welcome: User cust
Last login: Tue Feb 21 10:22:52 2017 from 10.10.16.50
Number of prior failed login attempts: 0
HostName/IP: AES71678/10.10.16.78
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Tue Feb 21 10:38:58 GMT 2017
HA Status: Not Configured

AVAYA Application Enablement Services Management Console

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

Left Hand Menu:

- AE Services
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
 - Alarm Viewer
 - Log Manager
 - Logs
 - Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - TSAPI Service Summary

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 |
|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| 1 | CM1627 | 1 | Talking | Thu Feb 16 11:09:27 2017 | Online | 17 | 6 | 15 | 15 | 30 |

Online Offline

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

TSAPI Service Status TLink Status User Status

From the left hand menu select **Status**→**Status and Control**→**TSAPI Service Summary**. Click on **User Status**. Set **CTI Users** to the user added in Section 8.2. Make sure **Open Streams** is set to **1** and an entry exists for the open stream.

Welcome: User cust
Last login: Wed Feb 15 14:57:37 2017 from 10.10.16.50
Number of prior failed login attempts: 0
HostName/IP: AES71678/10.10.16.78
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Tue Feb 21 10:12:41 GMT 2017
HA Status: Not Configured

AVAYA Application Enablement Services Management Console

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

Left Hand Menu:

- AE Services
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
 - Alarm Viewer
 - Log Manager
 - Logs
 - Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - TSAPI Service Summary

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users: cardeasy Submit

Open Streams: 1
Closed Streams: 0

Open Streams

| Name | Time Opened | Time Closed | Tlink Name |
|----------|---------------------------------|-------------|----------------------------|
| cardeasy | Thu 16 Feb 2017 12:39:38 PM GMT | | AVAYA#CM1627#CSTA#AES71678 |

Show Closed Streams Close All Opened Streams Back

Conclusion

These Application Notes describe the configuration required for Syntec CardEasy CPE to interoperate with Communication Manager using a SIP Trunk. All tests passed successfully with any observations notes in **Section 2.2**

12. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

[1] Administering Avaya Aura® Communication Manager, Release 7.0, August 2015, *Document Number 03-300509*, Issue 1.

[2] Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.0, August 2015, *Document Number 555-245-205*, Issue 1.

Product Documentation for Syntec CardEasy can be requested from support@syntec.co.uk.

©2017 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.