Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller 6.0 with Skype Connect R2.2 using TLS as the Transport Protocol – Issue 1.0

Abstract

These Application Notes describe the steps to configure the Avaya Aura® R6 SIP reference architecture with the Skype Connect SIP trunking service using TLS as the transport protocol.

Skype Connect allows Skype's registered user community to contact business users through click-to-call applications or by calling the Skype Names of business users associated with phone extensions on Avaya Aura® without the need for TDM media gateways and the associated maintenance costs. Skype Connect also provides a low-cost inbound and outbound PSTN calling service with DID and Caller ID support.

Testing was conducted in the Avaya Solution and Interoperability Test Lab, utilizing a Skype Manager account on the Skype Connect production service.

©2011 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
1.1. Design Principles and Assumptions 5
1.2. Interoperability Compliance Testing 5
1.3. Abbreviations 5
1.4. Known Limitations 6
1.5. Reference Configuration 7
1.6. Support 7
2. Equipment and Software Validated 8
3. Call Flows 9
3.1. Inbound from PSTN 9
3.2. Outbound to PSTN 10
3.3. Inbound from Skype Client 11
3.4. Outbound to Skype Client 12
4. Avaya Aura® Communication Manager 13
4.1. Administer System Parameters 13
4.2. Administer Dial Plan 14
4.3. Administer IP Network Parameters 15
4.4. Administer Signaling Group 17
4.5. Administer Trunk Group 18
4.6. Administer Automatic Route Selection 19
4.7. Administer Route Pattern 20
4.8. Administer Public Unknown Numbering 20
4.9. Administer Incoming Call Handling Treatment 21
5. Configuring Avaya Aura® Session Manager 22
5.1. Log in to Avaya Aura® Session Manager 22
5.2. Administer SIP Domain 24
5.3. Administer Locations 25
5.4. Administer SIP Entities 26
5.5. Administer Entity Links 28
5.6. Administer Time Ranges 29
5.7. Administer Routing Policies 30
5.8. Administer Dial Patterns 32
6. Configure Skype Manager 35
6.1. Log in to Skype Manager 35
6.2. Create SIP Profile 36
6.3. Administer Maximum Simultaneous Calls 37
6.4. Administer Online Numbers 40
6.5. Administer Caller ID 44
6.6. Create a Business User 46
6.7. Add Business User to SIP Profile 48
7. Configure Avaya Aura® Session Border Controller 51
7.1. Log in to Avaya Aura® Session Border Controller using the GUI 51
7.2. Administer SIP Domains 52

©2011 Avaya Inc. All Rights Reserved.

7.3. Administer TLS Certificate 56
7.4. Administer TLS on the outside interface 58
7.5. Administer Authentication 60
7.6. Administer Outbound SIP Header Manipulation Rules 61
7.7. Administer Inbound SIP Header Manipulation Rules 64
7.8. Administer SIP Header Rules for Topology Hiding 66
7.9. Save the Configuration 70
8. General Test Approach and Test Results 71
9. Verification Steps 71
9.1. Troubleshooting Tools 72
10. Conclusion 72
11. References 73
Appendix A – Skype Button 74
Appendix B – Avaya Aura® SBC Configuration File 76

©2011 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps to configure the Avaya Aura® R6 SIP reference architecture with the Skype Connect SIP trunking service. Skype Connect allows Skype's user community to contact business users through click-to-call applications or by calling the Skype Names of business users associated with phone extensions on Avaya Aura® without the need for TDM media gateways and the associated maintenance costs. Skype Connect also provides a low-cost inbound and outbound PSTN calling service with DID and Caller ID support.

The Avaya Aura® R6 SIP reference architecture consists of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® System Manager and Avaya Aura® Session Border Controller. Avaya Aura® Communication Manager controls the Avaya H.323, digital, and analog endpoints, normalizes the called and calling numbers for both incoming and outgoing calls to/from Skype Connect and provides telephony features such as Call Forward, Transfer and Call Pickup. The role of the Avaya Aura® Session Manager in the reference architecture is to act as a Registrar for Avaya SIP endpoints, SIP Proxy for outbound/inbound trunk calls while providing a centralized dial-plan for least-cost and time-of-day based routing. Avaya Aura® System Manager provides a web-based interface for the provisioning and maintenance of Avaya Aura® Session Manager while the Avaya Aura® Session Border Controller provides topology hiding without the need for Network Address Translation (NAT), SIP header manipulation and SIP signaling and media channel conversion services.

©2011 Avaya Inc. All Rights Reserved.

1.1. Design Principles and Assumptions

The service offer described in these Application Notes is designed for business customers using Avaya Aura® Communication Manager and Avaya Aura® Session Manager on a private protected enterprise network who opt for routing their voice calls over the public Internet using the Skype Connect service. It is assumed that Skype Connect is used as first choice for outbound calls and that business customers will keep some of their existing TDM connections to the PSTN as Skype Connect does not support calls to emergency services. It is also assumed that the Avaya Aura® Session Border Controller acts as a peering host between the public Internet and the private enterprise network and provides Denial-of-Service (DoS), packet filtering and topology hiding without the need for an additional firewall or intrusion prevention system (IPS) on either the public or private side of the Avaya Aura® Session Border Controller. Although the Avaya Aura® Session Border Controller can be configured to provide intelligent call routing decisions, no dial-plan was provisioned on the Avaya Aura® Session Border Controller in the sample configuration as all the call routing and number modification logic is achieved by Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Hardware, software resilience and failover between the various Avaya components are not covered in these Application Notes.

1.2. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 3** for examples) and basic supplementary features between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya Aura® Session Border Controller and the Skype Connect service.

The compliance testing was based on a test plan provided by TekVizion, for the functionality required for certification as a solution supported on the Skype Connect network. The following features were tested as part of this effort:

- SIP trunking.
- Passing of DTMF events and their recognition by navigating automated menus.
- Supplementary features such as hold, resume, conference and transfer.

1.3. Abbreviations

The abbreviations used in this document include the following:

Abbreviation	Description
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
HQ	Headquarters
B2BUA	Back-to-back User Agent
PE	Processor Ethernet
P2P	Peer-to-peer
AOR	Address of record
DNIS	Dialed Number Identification Service

©2011 Avaya Inc. All Rights Reserved.

1.4. Known Limitations

The following limitations are noted for the reference configuration described in these Application Notes:

- Skype Connect is currently U.S. only. The service will be introduced in other regions at a later stage.
- Skype Connect does not support calls to the emergency service. Another PSTN trunk must be provisioned in Avaya Aura® Communication Manager to route calls to the emergency service.
- Porting of existing PSTN numbers (DIDs) to Skype Connect is not supported.
- Access to a broadband internet connection is required.
- Maximum of 300 simultaneous calls per SIP Profile. A company may have multiple SIP Profiles.
- SIP over TLS is currently supported by Skype Connect R2.2
- Call processing tones are locally generated by Avaya Aura® Communication Manager.
- Premium-rated numbers (1900, 1976) are blocked.
- This solution does not currently support outbound SIP calls to Skype names.
- DNS A and SRV records are supported for Skype Connect R2.2
- The SIP REFER request is not supported for call redirection/transfer.
- SIP 3xx Redirect Responses are not supported.
- SRTP is supported in Skype Connect R2.2 and was tested successfully on the SIP trunk towards the SBC public interface.
- IP TOS or DiffServ QoS markings are neither set nor honored; therefore Skype Connect cannot guarantee the end-to-end voice quality. Service Level Agreements (SLAs) are not available.
- Maximum 99 Online Numbers per SIP Profile. Sequential number block (DID) purchases will be introduced at a later stage.
- G.711A/mu-law, G.729 (Annex A and B) codecs are supported.
- For outbound calls (local, national and international) via Skype Connect the E.164 or International numbering format (00 + <country code>) must be used.
- For inbound calls Skype Connect delivers the called/calling number in the format <country code><national number>.
- T.38 fax is not supported.
- RTCP and RTCP XR are not handled by Skype Connect.
- Skype Connect calls are limited to 4 hours.
- High Availability with two physically separate Avaya Aura® Session Border Controllers is not supported in R6.0.
- Skype Connect is not guaranteed to work with credit card machines, franking (stamping) machines and alarm systems or other services which use a regular phone line with a modem connection.
- No RTP was received from Skype when calling an international number (448458444777). This issue is currently being investigated by Skype.

©2011 Avaya Inc. All Rights Reserved.

1.5. Reference Configuration

Figure 1 illustrates Avaya Aura® R6 SIP reference architecture used for Interoperability testing. The reference configuration is comprised of a sample enterprise HQ site connected via a Metro Ethernet link to the Internet. At the edge of the test HQ site an Avaya Aura® Session Border Controller acts as a B2BUA for SIP calls. The Avaya Aura® Session Border Controller terminates and re-originates calls using its own IP addresses thereby hiding the IP address range (topology) of the private network. Network security is provided by the DoS and packet filtering module of the Avaya Aura® Session Border Controller. The Avaya Aura® Session Border Controller converts the SIP signaling channel from TLS to TCP for inbound and vice-versa for outbound calls.

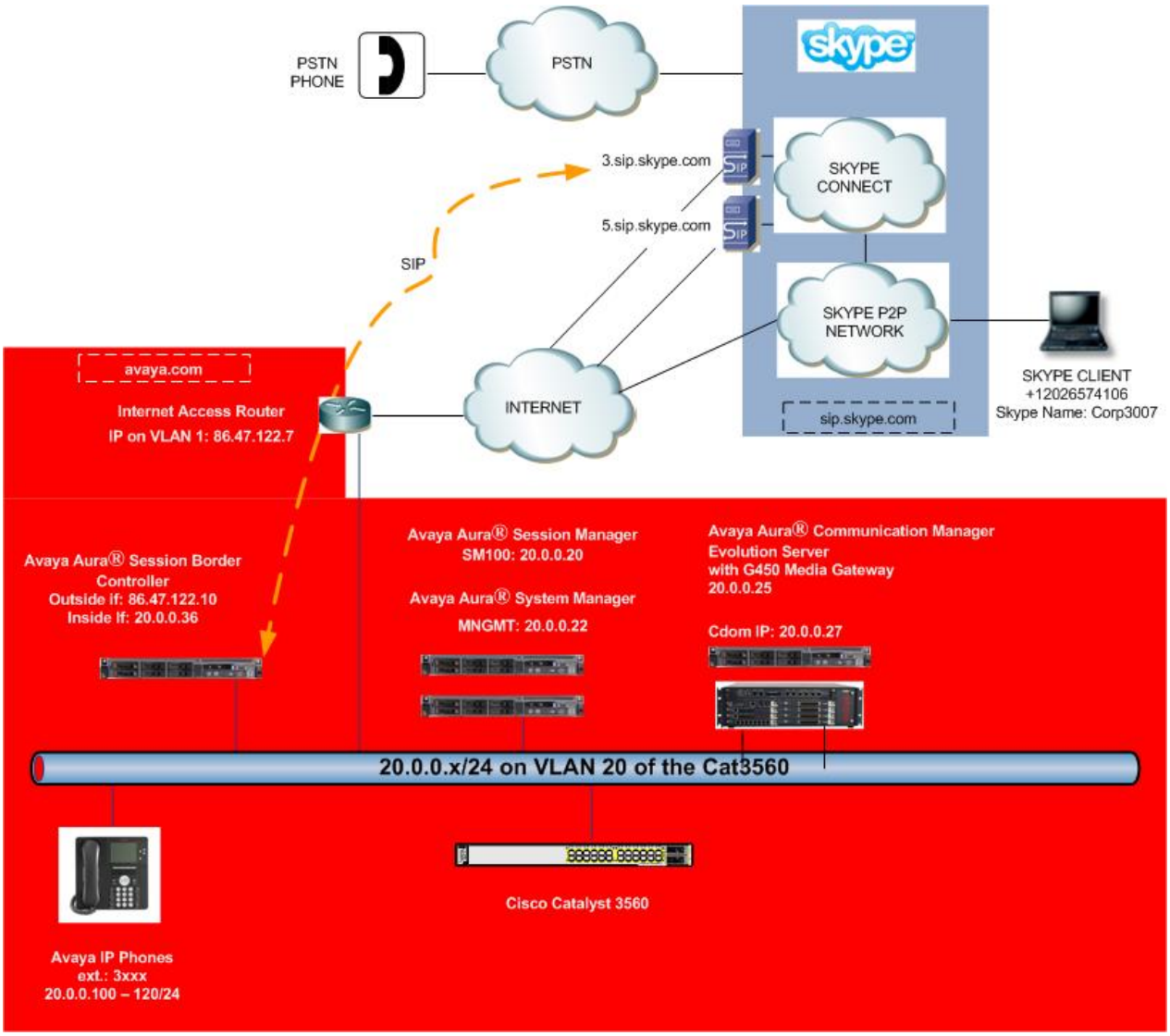


Figure 1: Avaya Interoperability Test Lab Reference Configuration

1.6. Support

For technical support on Avaya products described in these Application Notes visit
http://support.avaya.com

©2011 Avaya Inc. All Rights Reserved.

For technical support on the Skype Connect service visit http://www.skype.com/support

2. Equipment and Software Validated

The following equipment and software were used in the reference configuration.

Equipment	Software Version
Avaya S8800 Server	Avaya Aura® Session Manager – R6.1 Build R6.1.0.610012
Avaya S8800 Server	Avaya Aura® System Manager - R6.1 Build R6.1.0.610012
Avaya S8800 Server	Avaya Aura® Session Border Controller – R6.0.0.1.5 Build E36m3p4
Avaya S8800 Server	Avaya Aura® Communication Manager – Evolution Server - R016x.00.1.510.1
Avaya G430 Media Gateway	R30.10.4
Avaya 9650 H.323 Phone	R3.1.1
Avaya 9650 SIP Phone	R2.6.2.21
Test PC1	Microsoft Windows Vista with Avaya one-X® Communicator (H.323) R6.0.0.20
Test PC2	Skype Client v5.3.0.111
Skype Connect	R2.2 Build 3.6.0m3p4

Table 1: Equipment and Software Used in the Reference Configuration

©2011 Avaya Inc. All Rights Reserved.

3. Call Flows

To understand how inbound and outbound Skype Connect service calls are handled by Session Border Controller, Session Manager and Communication Manager, four general call flows are described in this section.

3.1. Inbound from PSTN

The first call scenario illustrated in **Figure 2** is an inbound call from a PSTN phone to the Online Number of a phone registered to Communication Manager on the enterprise network.

1. PSTN user dials the Skype Connect Online Number of the enterprise user (+12024703313).
2. The call is routed to the Skype Connect service network.
3. The Skype Connect service sends the call to the publicly routable IP address of the outside interface of the Session Border Controller.
4. The call is delivered to the Session Border Controller using SIP over TLS.
5. The Session Border Controller performs SIP header modifications, SDP modifications, transport protocol conversion (TLS to TCP) and routes the call to Session Manager.
6. Session Manager performs call routing based on the called number and the configured Network Routing Policies. In the sample configuration the Online Number is associated with the Communication Manager SIP Entity.
7. Communication Manager routes the call to a phone.

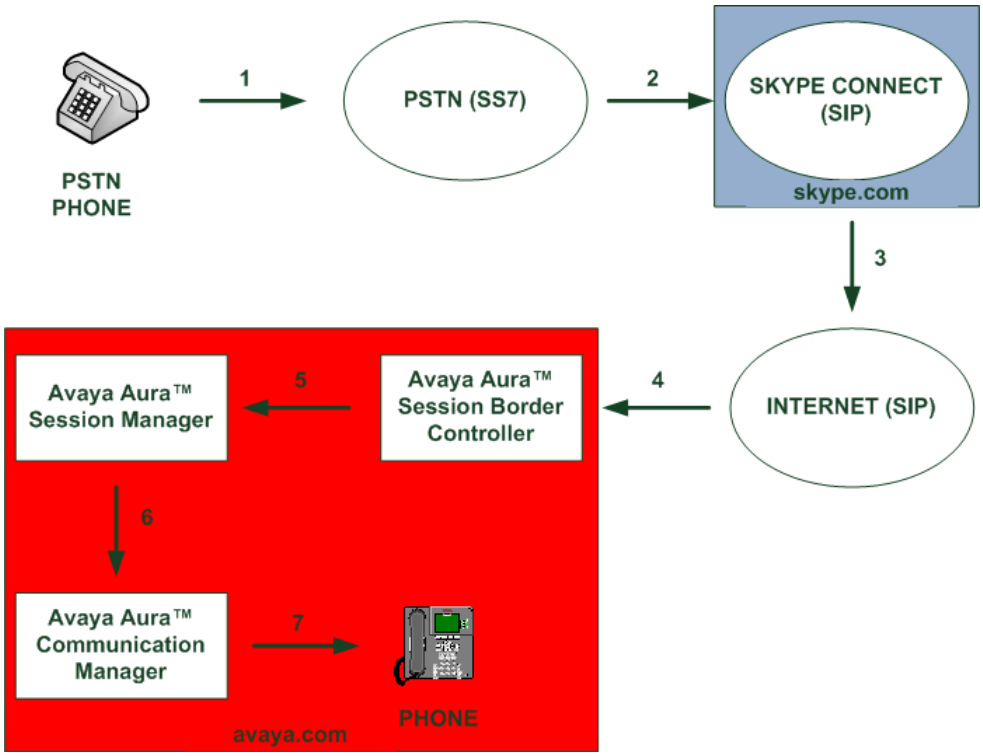


Figure 2 - Inbound PSTN to Skype Connect Call

Note: A single Session Border Controller was used in the sample configuration as High Availability is not supported in Release 6.0.

©2011 Avaya Inc. All Rights Reserved.

3.2. Outbound to PSTN

The second call scenario illustrated in **Figure 3** is an outbound call with CLIP that originates from a phone registered to Communication Manager on the enterprise network and terminates at the PSTN phone.

1. Avaya phone originates a call to a PSTN number.
2. Communication Manager converts the calling and called numbers to an E.164 format before it routes the call to Session Manager using SIP over TCP.
3. Based on the called number Session Manager sends the call to Avaya Aura® Session Border Controller.
4. Session Border Controller queries the public DNS server for "sip.skype.com". The public DNS server returns the IP address of the geographically closest Skype Connect peer in an SRV record. The call is sent using SIP over TLS through the Internet.
5. The SIP INVITE arrives to the public interface of the Skype Connect peer.
6. The Skype Connect network compares the contents of the PAI header with the Online Number of the caller's SIP Profile. If the two E.164 numbers match, the Caller ID gets set before the call breaks out to the PSTN. Otherwise the call is delivered to the PSTN with no Caller ID or a default Caller ID displayed for all outbound calls if one has been pre-configured in Skype Manager.
7. The call is routed to the PSTN phone.

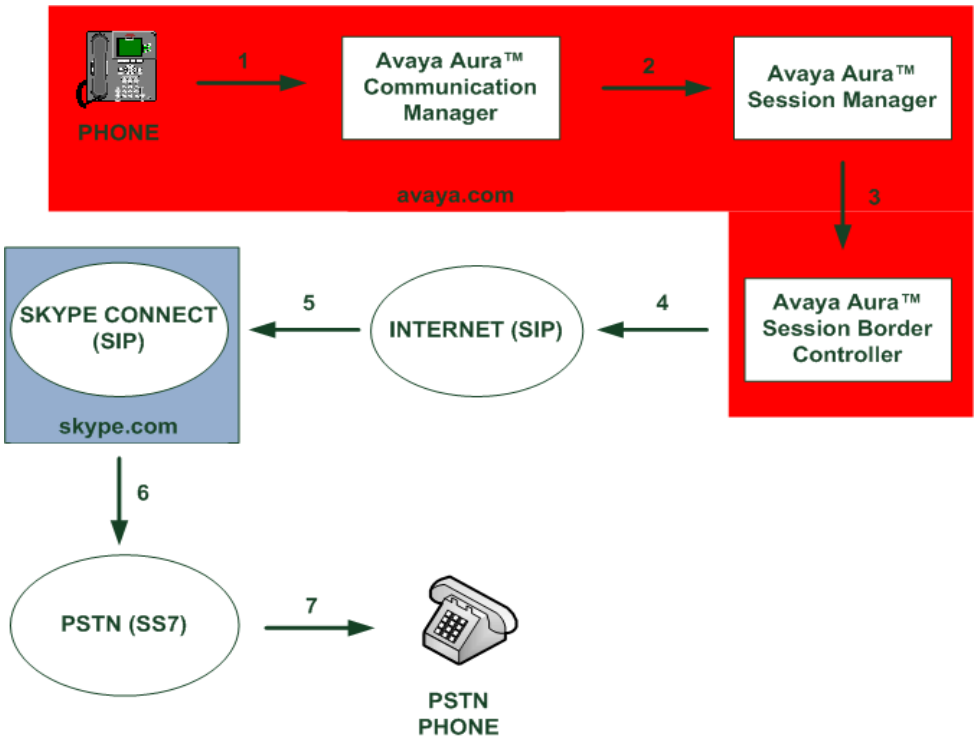


Figure 3: Outbound Skype Connect to PSTN call with CLIP

Note: Session Border Controller caches DNS SRV records until the TTL value expires.

©2011 Avaya Inc. All Rights Reserved.

3.3. Inbound from Skype Client

The third call scenario illustrated in **Figure 4** is an inbound call made from a Skype client to a phone registered to Avaya Aura® Communication Manager on the enterprise network. **Note:** The call stays within the skype.com service domain and does not break out to the PSTN.

1. Skype user initiates a call by double-clicking the Skype Name of the enterprise user associated with the SIP Profile.
2. The call is routed from the Skype P2P Network to the Skype Connect service network.
3. The Skype Connect service sends the call to the publicly routable IP address of the outside interface of the Avaya Aura® Session Border Controller.
4. The call is delivered to the Avaya Aura® Session Border Controller using SIP over TLS.
5. The Avaya Aura® Session Border Controller performs SIP header modifications, SDP modifications, transport protocol conversion (TLS to TCP) and routes the call to Avaya Aura® Session Manager.
6. Avaya Aura® Session Manager performs call routing based on the called number and the configured Network Routing Policies. In the sample configuration the Online Number is associated with the Avaya Aura® Communication Manager SIP Entity.
7. Avaya Aura® Communication Manager routes the call to a phone.

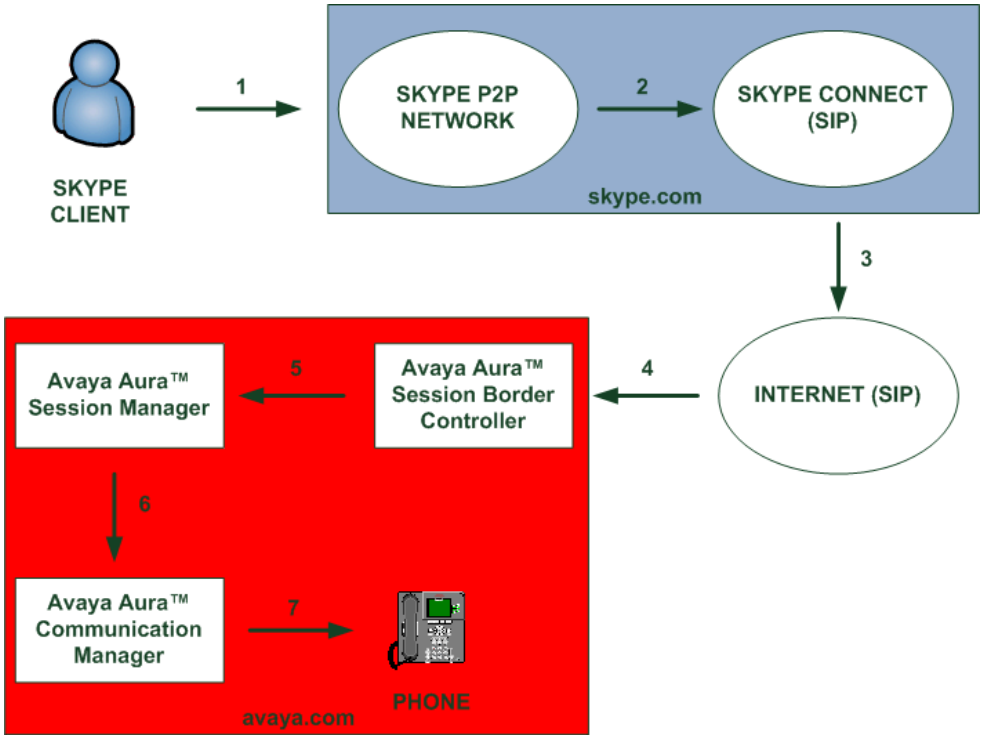


Figure 4: Inbound Skype P2P to Skype Connect call

©2011 Avaya Inc. All Rights Reserved.

3.4. Outbound to Skype Client

The fourth call scenario illustrated in **Figure 5** is an outbound call made from a phone registered to Avaya Aura® Communication Manager on the enterprise network to the Online Number of a Skype Client. **Note:** The call stays within the skype.com service domain and does not break out to the PSTN.

1. Avaya phone originates a call to the Online Number of the Skype Client.
2. Avaya Aura® Communication Manager converts the calling and called numbers to an E.164 format before it routes the call to Avaya Aura® Session Manager using SIP over TCP.
3. Based on the called number Avaya Aura® Session Manager sends the call to Avaya Aura® Session Border Controller.
4. Avaya Aura® Session Border Controller queries the public DNS server for "sip.skype.com". The public DNS server returns the IP address of the geographically closest Skype Connect peer in an SRV record. The call is sent using SIP over TLS through the Internet.
5. The SIP INVITE arrives to the public interface of the Skype Connect peer.
6. The Skype Connect network recognizes that the called number belongs to a Skype Client (Online Number) and routes the call to the Skype P2P Network.
7. The call is delivered to the Skype Client.

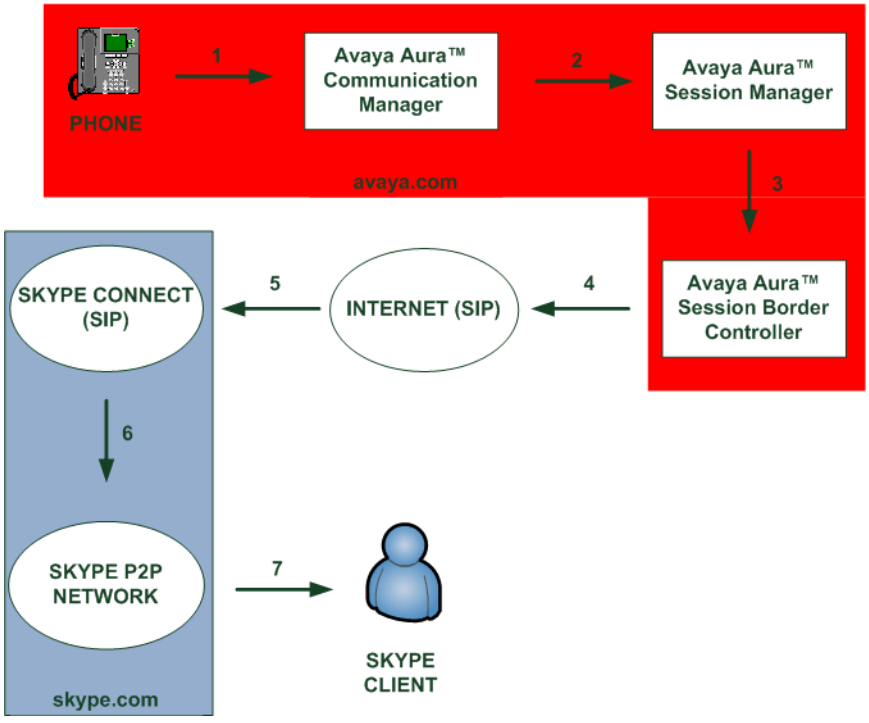


Figure 5: Outbound Skype Connect to Skype P2P Client call

©2011 Avaya Inc. All Rights Reserved.

4. Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager and includes the following items:

- Administer System Parameters
- Administer Dial Plan
- Administer IP Network Parameters
- Administer Signaling Group
- Administer Trunk Group
- Administer Automatic Route Selection
- Administer Route Pattern
- Administer Public Unknown Numbering
- Administer Incoming Call Handling Treatment

The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration, including stations, Processor Ethernet, etc, has already been performed.

4.1. Administer System Parameters

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes. For required licenses that are not enabled in the steps that follow, contact an authorized Avaya account representative to obtain the licenses. Enter the **display system-parameters customer-options** command. On **Page 2** of the **system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 8000  0
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                      Maximum Administered SIP Trunks: 5000  250
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                            Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

       (NOTE: You must logoff & login to effect the permission changes.)
```


©2011 Avaya Inc. All Rights Reserved.

On **Page 4** of the **system-parameters customer-options** form, verify that the **IP Trunks** field in the following screenshot is set to **y**.

```
display system-parameters customer-options                    Page   4 of  11
                              OPTIONAL FEATURES

   Emergency Access to Attendant? Y                             IP Stations? Y
            Enable 'dadmin' Login? Y
            Enhanced Conferencing? Y                     ISDN Feature Plus? Y
                   Enhanced EC500? Y      ISDN/SIP Network Call Redirection? N
    Enterprise Survivable Server? N                        ISDN-BRI Trunks? Y
       Enterprise Wide Licensing? N                              ISDN-PRI? Y
              ESS Administration? N              Local Survivable Processor? N
          Extended Cvg/Fwd Admin? Y                   Malicious Call Trace? N
     External Device Alarm Admin? N                 Media Encryption Over IP? N
  Five Port Networks Max Per MCC? N   Mode Code for Centralized Voice Mail? N
                  Flexible Billing? N
   Forced Entry of Account Codes? N                 Multifrequency Signaling? Y
      Global Call Classification? N        Multimedia Call Handling (Basic)? Y
             Hospitality (Basic)? Y     Multimedia Call Handling (Enhanced)? Y
 Hospitality (G3V3 Enhancements)? N              Multimedia IP SIP Trunking? N
                       IP Trunks? Y

            IP Attendant Consoles? N
```

4.2. Administer Dial Plan

Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings administered below:

- 3-digit dial access codes (indicated with a **Call Type** of **dac**) beginning with * – Trunk Access Codes (TACs) defined for trunk groups in this reference configuration conform to this format.
- 4-digit extensions with a **Call Type** of **ext** beginning with the digits **30** – local extensions for Communication Manager stations in this reference configuration conform to this format.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) beginning with the digit **9** – access code for outbound ARS dialing.

```
Change dialplan analysis                                      Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                 Location:  all          Percent Full:    2
      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
    *           3    dac
    30          4    ext
    9           1    fac
```


©2011 Avaya Inc. All Rights Reserved.

4.3. Administer IP Network Parameters

These Application Notes assume that the appropriate IP network regions and IP codec sets have already been administered to support internal calls. For simplicity in this reference configuration, all Communication Manager elements - stations, PE interface, G430 Media Gateway - within the Avaya site are assigned to a single IP network region (region 1) and all internal calls use a single IP codec set. This section describes the steps for administering an additional IP network region to represent the Skype Connect service, and another IP codec set for external calls. Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g. **2**). This IP codec set will be used for off-net calls to Skype Connect. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown below.

```
change ip-codec-set 2                                          Page   1 of   2

                         IP Codec Set
    Codec Set: 2

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.729             n          2        20
 2: G.711MU           n          2        20
 3: G.711A            n          2        20
```

On **Page 2** of the **ip-codec-set** form, set **FAX** Mode to **off**.

```
change ip-codec-set 2                                          Page   2 of   2
                         IP Codec Set
                             Allow Direct-IP Multimedia? N
                   Mode                Redundancy
    FAX            off                  0
    Modem          off                  0
    TDD/TTY        off                  0
    Clear-channel  n                    0
```


©2011 Avaya Inc. All Rights Reserved.

Enter the change **ip-network-region 1** command. This IP network region is used for on-net calls. Enter **avaya.com** for the **Authoritative Domain** parameter.

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:               Authoritative Domain:avaya.com
    Name: Skype
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? N
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? Y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? Y
        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
```

Enter the **change ip-network-region 2** command. This IP network region will be used to represent the SIP Trunk to Skype Connect. Enter **2** for the **Codec Set** parameter.

```
change ip-network-region 2                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain:
    Name: Skype
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? N
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? Y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? Y
        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
```

On **Page 4** of the form enter **2** for the **Codec Set** parameter for connections to destination region 1.

```
change ip-network-region 2                                    Page   4 of  19

 Source Region: 2    Inter Network Region Connection Management     I       M
                                                                    G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    2     y    NoLimit                                          n
```


©2011 Avaya Inc. All Rights Reserved.

4.4. Administer Signaling Group

This section describes the steps for administering a single signaling group, shared by both outbound and inbound calls. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **100**), and provision the following:

- **Group Type** Set to **sip**
- **Transport Method** Set to **tcp**
- **Near-end Node Name** Set to the node name of the Processor Ethernet interface
- **Far-end Node Name** Set to the node name of Session Manager SM100 ip address
- **Near-end Listen Port** Set to **5060**
- **Far-end Listen Port** Set to **5060**
- **Far-end Network Region** Set to IP network region **2**

```
add signaling-group 100
                               SIGNALING GROUP

 Group Number: 100            Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? n                                Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



 Near-end Node Name: procr                 Far-end Node Name: asmr61
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                           Far-end Network Region: 2

Far-end Domain:
                                            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
```


©2011 Avaya Inc. All Rights Reserved.

4.5. Administer Trunk Group

Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. **100**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** Set to **sip**
- **Group Name** Enter a descriptive name
- **TAC** Enter a trunk access code that is consistent with the dial plan
- **Service Type** Set to **public-ntwrk**
- **Signaling Group** Set to the number of the signaling group administered in the previous step
- **Number of Members** Enter the maximum number of simultaneous calls permitted on this trunk group

```
add trunk-group 100                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 100                    Group Type: sip           CDR Reports: y
  Group Name: SkypeConnect              COR: 1        TN: 1        TAC: *22
   Direction: both       Outgoing Display? n
 Dial Access? n                                    Night Service:
                                Auth Code? n
Service Type: public-ntwrk
                                                     Signaling Group: 100
                                                   Number of Members: 20
```

On **Page 3** of the **Trunk Group** form:

- Set **Numbering Format** to **public**

```
add trunk-group 100                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y
                      Numbering Format: public
                                                  UUI Treatment: service-provider

                                                   Replace Restricted Numbers? n
                                                  Replace Unavailable Numbers? n
 Show ANSWERED BY on Display? y
```


©2011 Avaya Inc. All Rights Reserved.

4.6. Administer Automatic Route Selection

Use the **change feature-access-codes** command to specify **9** as the access code for external dialing.

```
change feature-access-codes                                    Page   1 of   9
                                FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial – Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) – Access Code 1: 9     Access Code 2:
                  Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:     All:     Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                   CDR Account Code Access Code:
                         Change COR Access Code:
                    Change Coverage Access Code:
             Conditional Call Extend Activation:        Deactivation:
                    Contact Closure   Open Code:          Close Code:
```

Use the **change ars analysis** command to specify the called number patterns which are dialed following the ARS access code. In the reference configuration, outbound calls are placed to international numbers.

```
change ars analysis 0                                    Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    0
         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
    00                   10   18    100      pubu         n
```


©2011 Avaya Inc. All Rights Reserved.

4.7. Administer Route Pattern

Use the **change route-pattern** command to define the trunk group administered in **Section 4.5**.

```
change route-pattern 100                                          Page   1 of   3
                  Pattern Number: 68  Pattern Name:toasmr61
                           SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                        DCS/ IXC
    No          Mrk Lmt List Del  Digits                          QSIG
                           Dgts                                   Intw
 1: 100   0                                                         n   user
```

4.8. Administer Public Unknown Numbering

For Calling Line Identification Presentation (CLIP) to work on outbound calls, Skype Connect expects to receive one of the online or landline numbers associated with the SIP Profile. The calling number is converted to an E.164 format by the public-unknown-numbering table and is inserted into the From and PAI headers of the outgoing INVITE request. Enter the **change public-unknown-numbering 0** command to specify the calling party numbers that are to be sent to the PSTN through Skype Connect. In the **public-unknown-numbering** form, for each local extension assigned to Avaya Aura® Communication Manager provision an entry as follows:

- **Ext Len** Enter the total number of digits in the local extension range.
- **Ext Code** Enter enough leading digits to identify the local extension or extension range.
- **Trk Grp(s)** Enter the number of the outbound trunk group to Skype Connect.
- **CPN Prefix** Enter the online or Skype Connect E.164 verified landline numbers that are associated with the SIP Profile in Skype Manager minus the "+" as this will be added automatically by Communication Manager for calls that use a public trunk. In **Section 6.5** the Caller ID is set to +12024703313 in Skype Manager.
- **CPN Len** Enter the total number of digits to be sent to Session Manager.

```
change public-unknown-numbering 0                                 Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk       CPN           CPN
Len Code          Grp(s)    Prefix        Len
                                                  Total Administered: 2
                                                  Maximum Entries: 9999
 5  3001         100       12024703313   11
```


©2011 Avaya Inc. All Rights Reserved.

4.9. Administer Incoming Call Handling Treatment

In the reference configuration Skype Connect delivers 11 digit Online Numbers to the enterprise network. Avaya Aura® Communication Manager converts the incoming 11 digit Online Number to a 4 digit extension using the Incoming Call Handling Treatment table. In **Section 6.4** the Online Number is set to +12024703313 in Skype Manager but it should be noted that in the request-uri that Skype sends, the "+" is omitted.

```
change inc-call-handling-trmt trunk-group 100                  Page   1 of  30
                        INCOMING CALL HANDLING TREATMENT

 Service/      Number   Number      Del Insert
 Feature        Len      Digits

 public-ntwrk    11 12024703313      11  3001
```


©2011 Avaya Inc. All Rights Reserved.

5. Configuring Avaya Aura® Session Manager

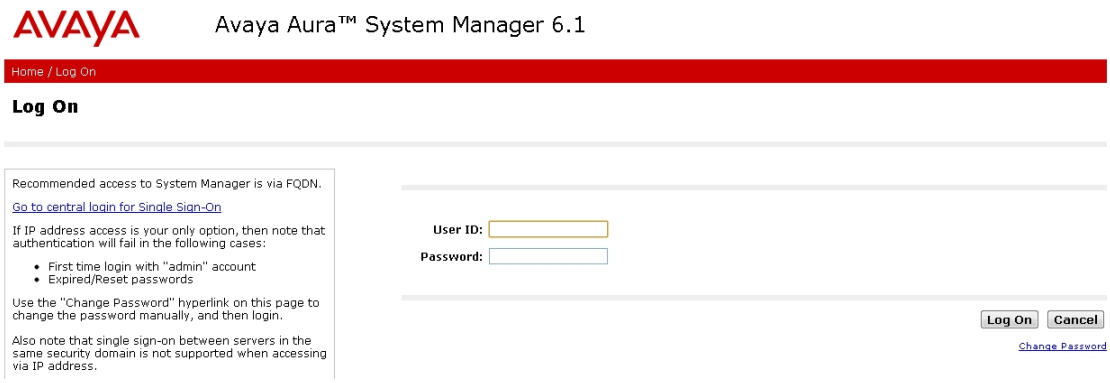
This section provides the procedures for configuring Session Manager. For further information on Session Manager, please consult with references **[1]-[3]**. The procedures include the following areas:

- Log in to Avaya Aura® Session Manager
- Administer SIP domain
- Administer Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns

The administration of Avaya endpoints and Communication Manager is not covered in these Application Notes. Please consult reference **[4]**.

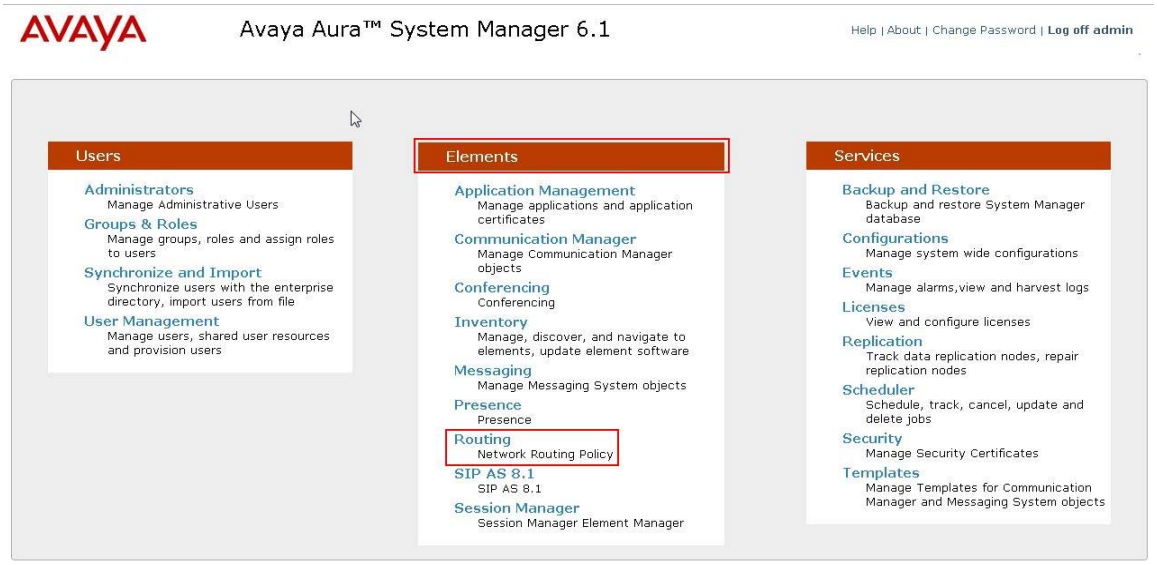
5.1. Log in to Avaya Aura® Session Manager

Access the System Manager using a Web Browser and entering ***http://<ip-address>/SMGR***, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials.

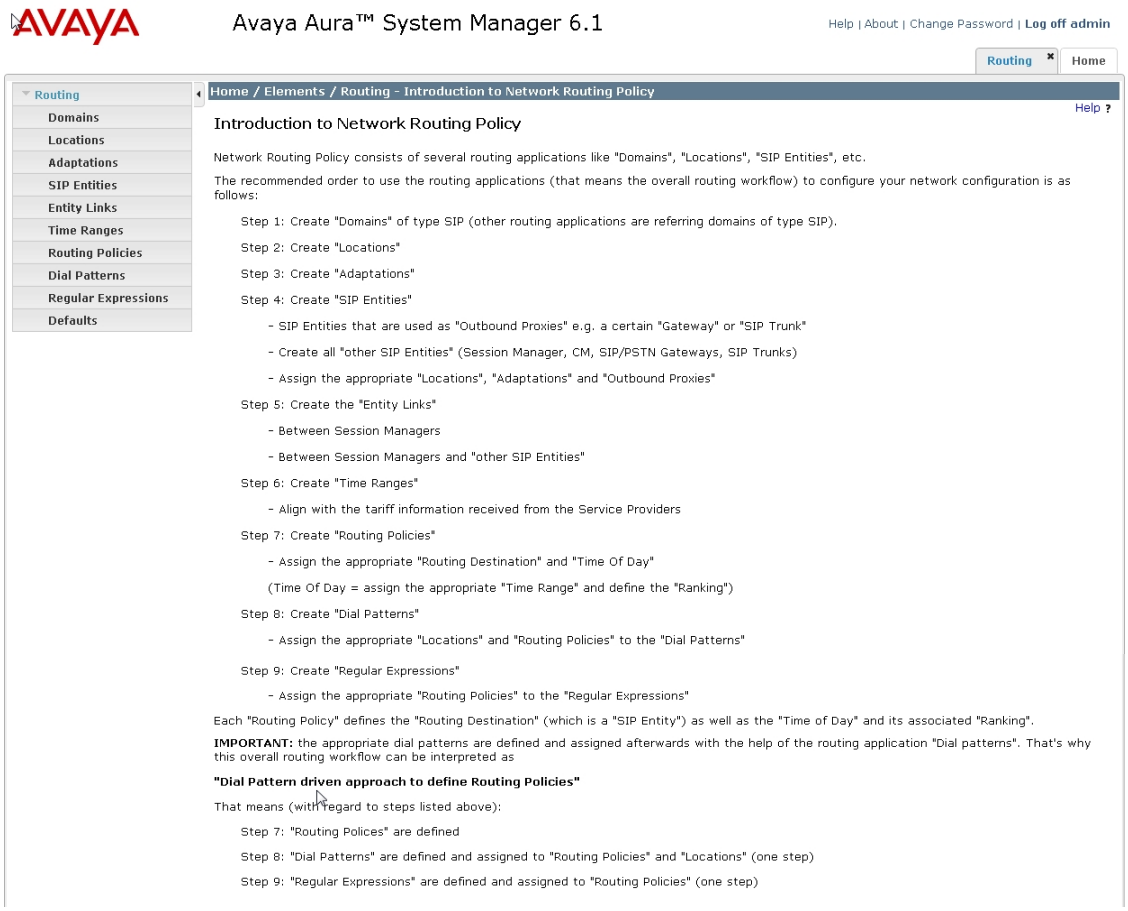


©2011 Avaya Inc. All Rights Reserved.

In the next screen under **Elements** column select **Routing**.



In the main panel, a short procedure for configuring Network Routing Policy is shown.



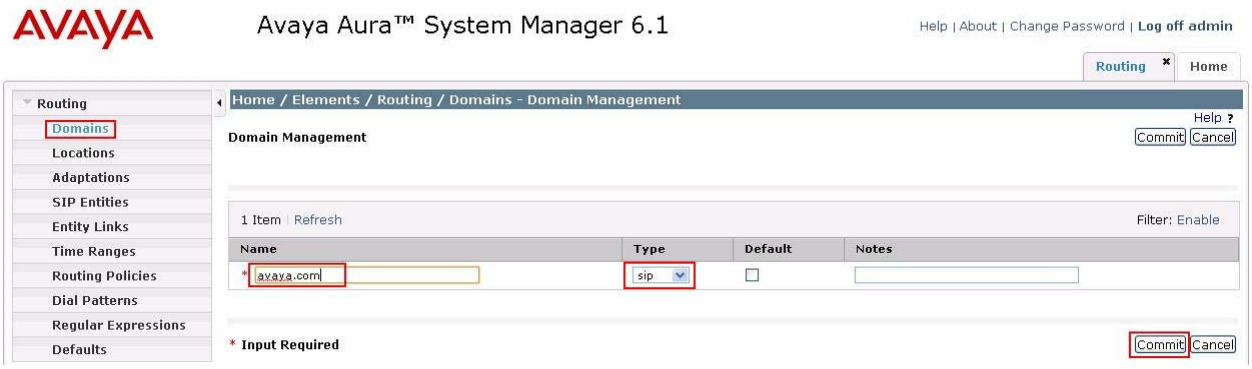
©2011 Avaya Inc. All Rights Reserved.

5.2. Administer SIP Domain

Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting **Domains** on the left panel menu and clicking the **New** button (not shown) to create a new SIP domain entry. Complete the following options:

- **Name** The authoritative domain name (e.g., **avaya.com**)
- **Type** **SIP**
- **Notes** Description for the domain (optional)

Click **Commit** to save changes.



©2011 Avaya Inc. All Rights Reserved.

5.3. Administer Locations

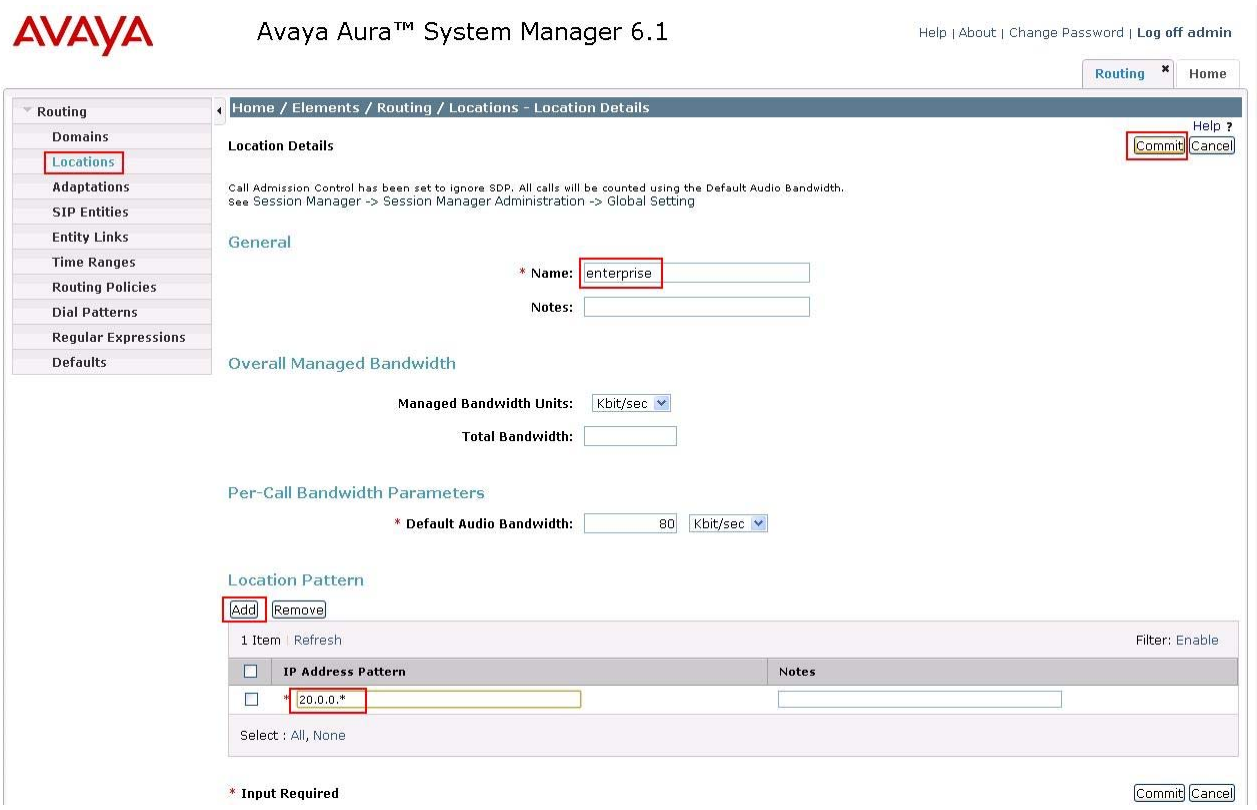
Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are dial patterns administered for specific locations. Locations are also used to limit the number of calls coming out of or going to a physical location. This is useful for those locations where the network bandwidth is limited. To add a Location, select **Locations** on the left panel menu and then click the **New** button (not shown). Enter the following for each **Location**:
Under **General:**

- **Name** An informative name (e.g. enterprise)

Under **Location Pattern:**

- **IP Address Pattern** An IP address pattern for this location

Select **Add** to add more locations. Click **Commit** to save changes.



©2011 Avaya Inc. All Rights Reserved.

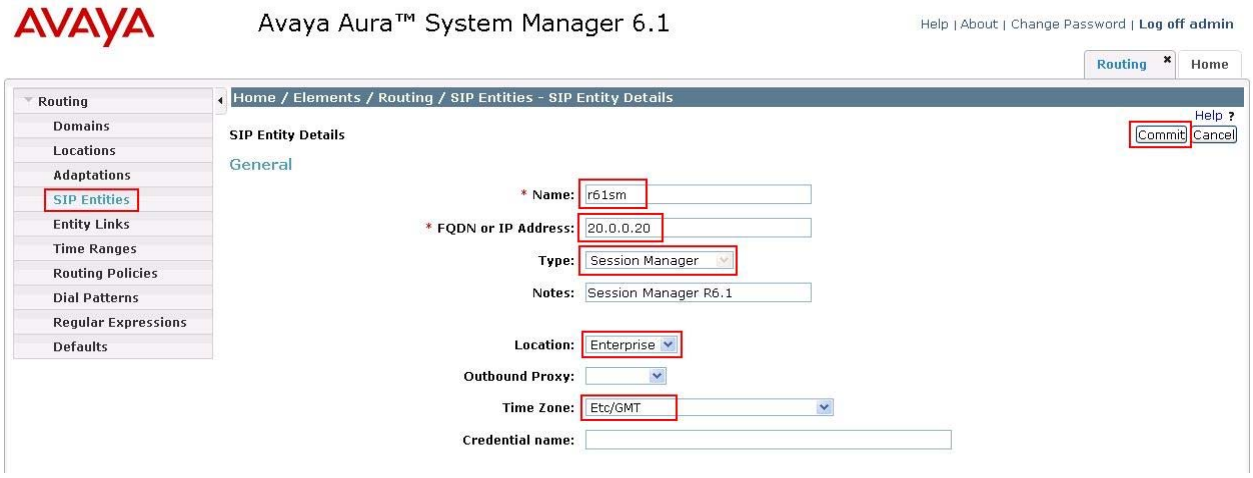
5.4. Administer SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by a SIP Trunk. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). Enter the following for each SIP Entity:

Under **General:**

- **Name** An informative name (e.g., **r61sm**)
- **FQDN or IP Address** IP address of the signaling interface on the Session Manager, Communication Manager or SBC.
- **Type** **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for SBC.
- **Location** **enterprise**
- **Time Zone** Time zone for this location

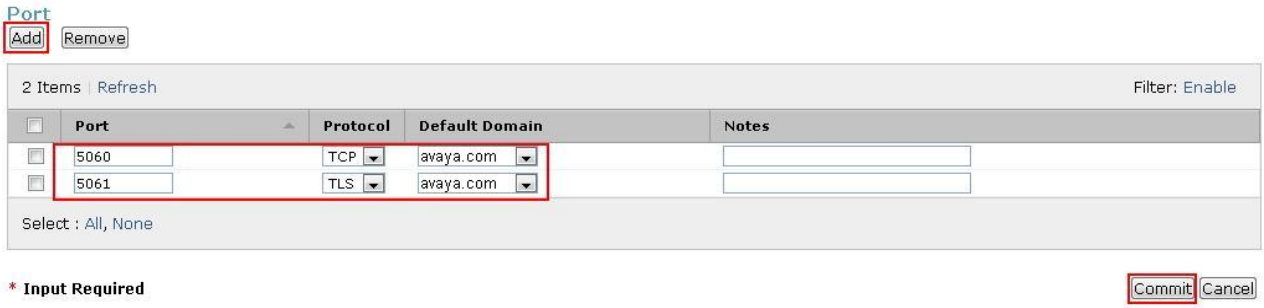
The following screen shows the SIP Entity for Session Manager.



Under **Port**, click **Add,** and then edit the fields in the resulting new row.

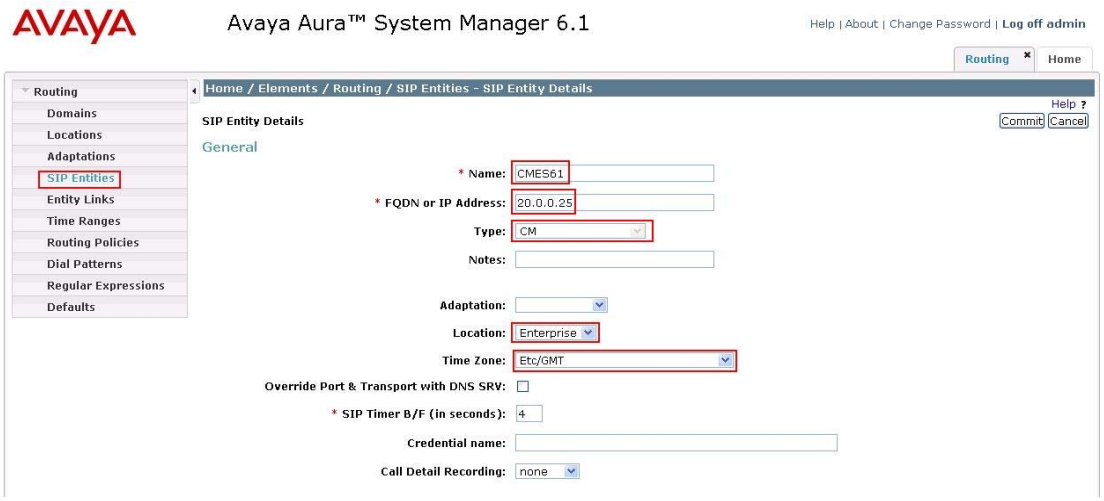
- **Port** Port number on which the system listens for SIP requests
- **Protocol** Transport protocol to be used to send SIP requests

The following screen shows the Port definitions for the Session Manager SIP Entity. Click **Commit** to save changes.

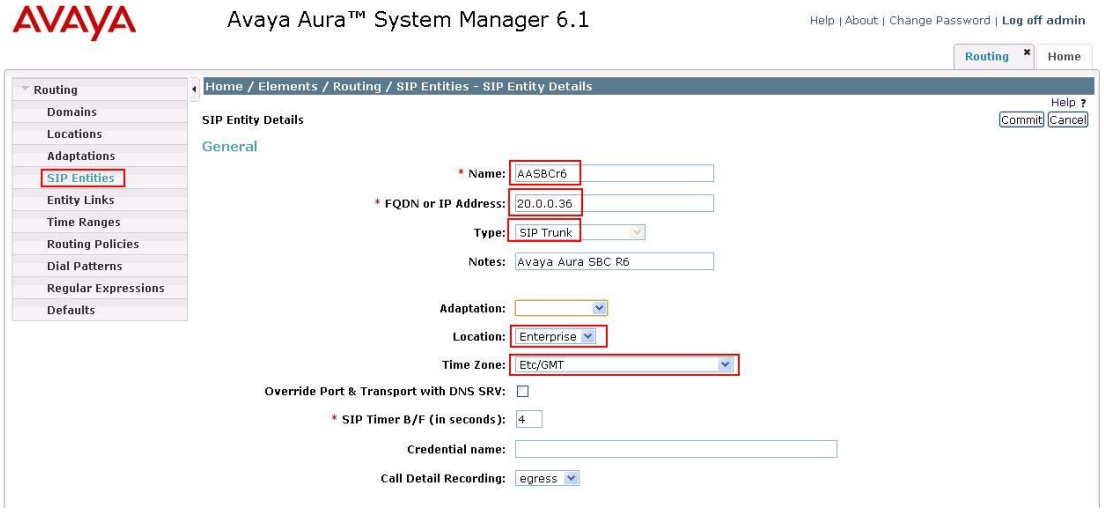


©2011 Avaya Inc. All Rights Reserved.

The following screen shows the SIP Entity for Communication Manager.



The following screen shows the SIP Entity for SBC.



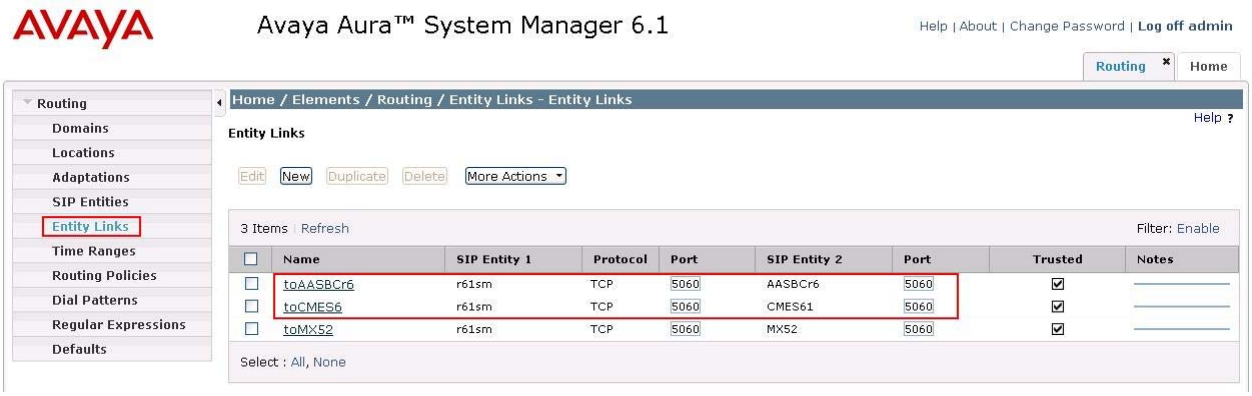
©2011 Avaya Inc. All Rights Reserved.

5.5. Administer Entity Links

A SIP trunk between a Session Manager and a telephony system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- **Name** An informative name
- **SIP Entity 1** Select **r61sm**
- **Port** Port number to which the other system sends its SIP requests
- **SIP Entity 2** The other SIP Entity for this link, created in **Section 5.4**
- **Port** Port number to which the other system expects to receive SIP requests
- **Trusted** Whether to trust the other system
- **Protocol** Transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in the sample network.



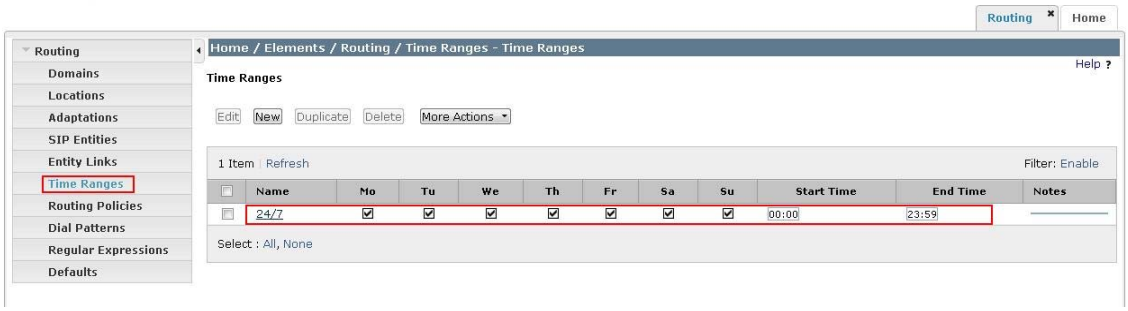
©2011 Avaya Inc. All Rights Reserved.

5.6. Administer Time Ranges

Before adding routing policies (see next step), time ranges must be defined during which the policies will be active. To add this time range, select **Time Ranges** from the left panel menu and then click **New** on the right. Fill in the following fields.

- **Name** An informative name (e.g. always)
- **Mo** through **Su** Check the box under each day of the week for inclusion
- **Start Time** Enter start time (e.g. **00:00** for start of day)
- **End Time** Enter end time (e.g. **23:59** for end of day)

In Session Manager, a default policy (**24/7**) is available that would allow routing to occur at anytime. This time range was used in the sample network.



©2011 Avaya Inc. All Rights Reserved.

5.7. Administer Routing Policies

Create routing policies to direct how calls will be routed to a system. Two routing policies must be added, one for Communication Manager (H.323 and Digital phones) and one for calls to Skype Connect numbers. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General:**

- Enter an informative **Name**

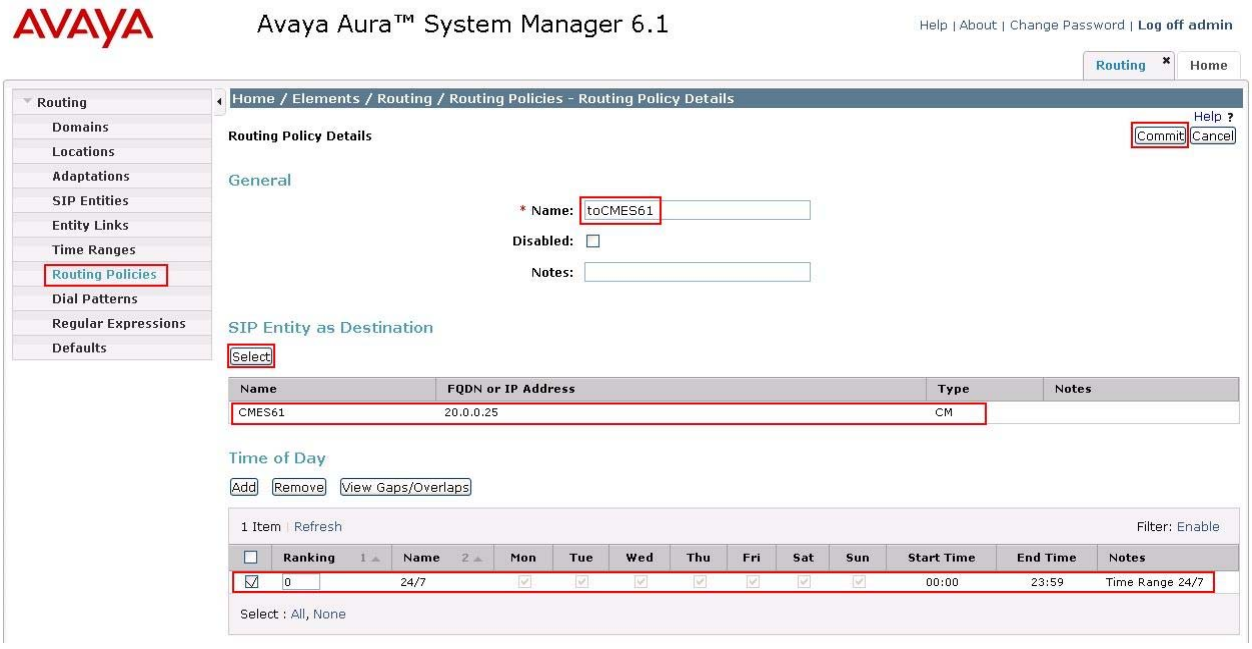
Under **SIP Entity as Destination:**

- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

Under **Time of Day:**

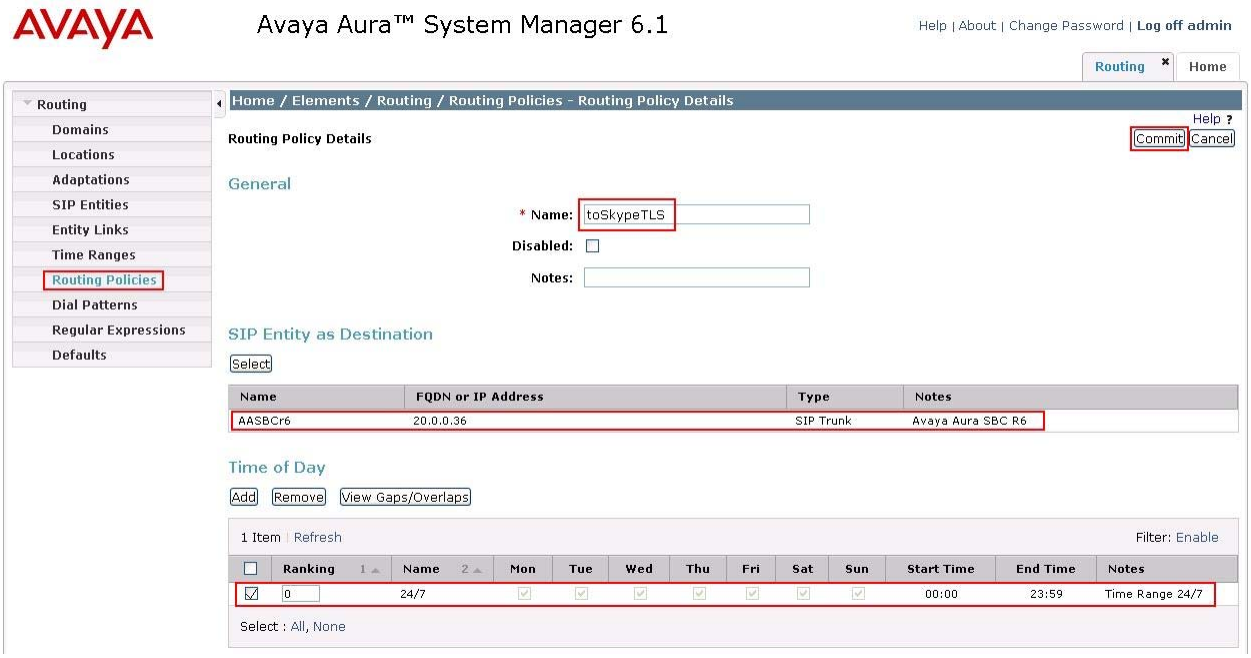
- Click **Add**, and then select the time range configured in the **Section 5.6.**

Click **Commit** to save changes. The following screen shows the **Routing Policy Details** for calls to Communication Manager.



©2011 Avaya Inc. All Rights Reserved.

The following is screen shows the **Routing Policy Details** for calls to Skype Connect numbers.



©2011 Avaya Inc. All Rights Reserved.

5.8. Administer Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, calls to 4-digit extensions on Communication Manager will begin with **300.** To configure the extension Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

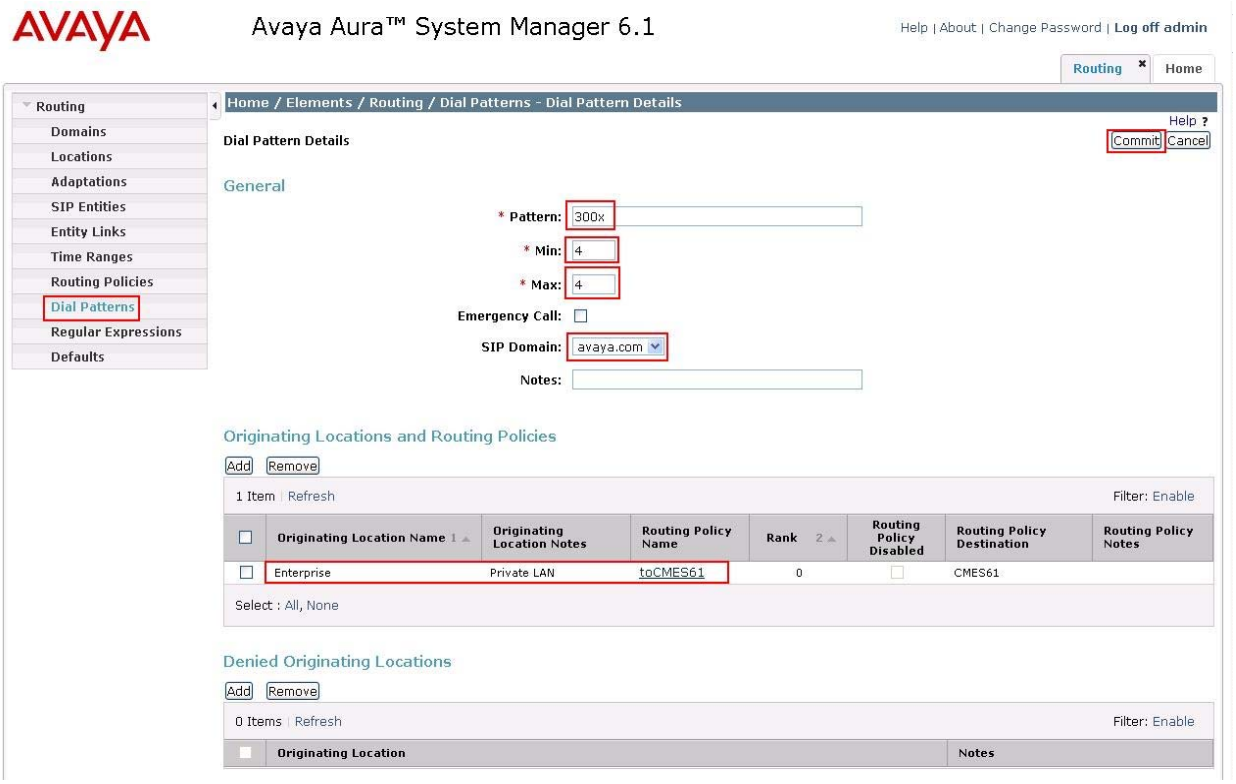
Under **General:**

- **Pattern** Dialed number or prefix
- **Min** Minimum length of dialed number
- **Max** Maximum length of dialed number
- **Notes** Comment on purpose of dial pattern
- **SIP Domain** Select the SIP Domain specified in **Section 5.2**

Under **Originating Locations and Routing Policy** select **Add** (not shown). Select the following entries:

- **Originating Location Name** Select the location created in **Section 5.3**
- **Routing Policies** Select the policy **toCMES61** created in **Section 5.7.**

Select **Commit** button to save.



©2011 Avaya Inc. All Rights Reserved.

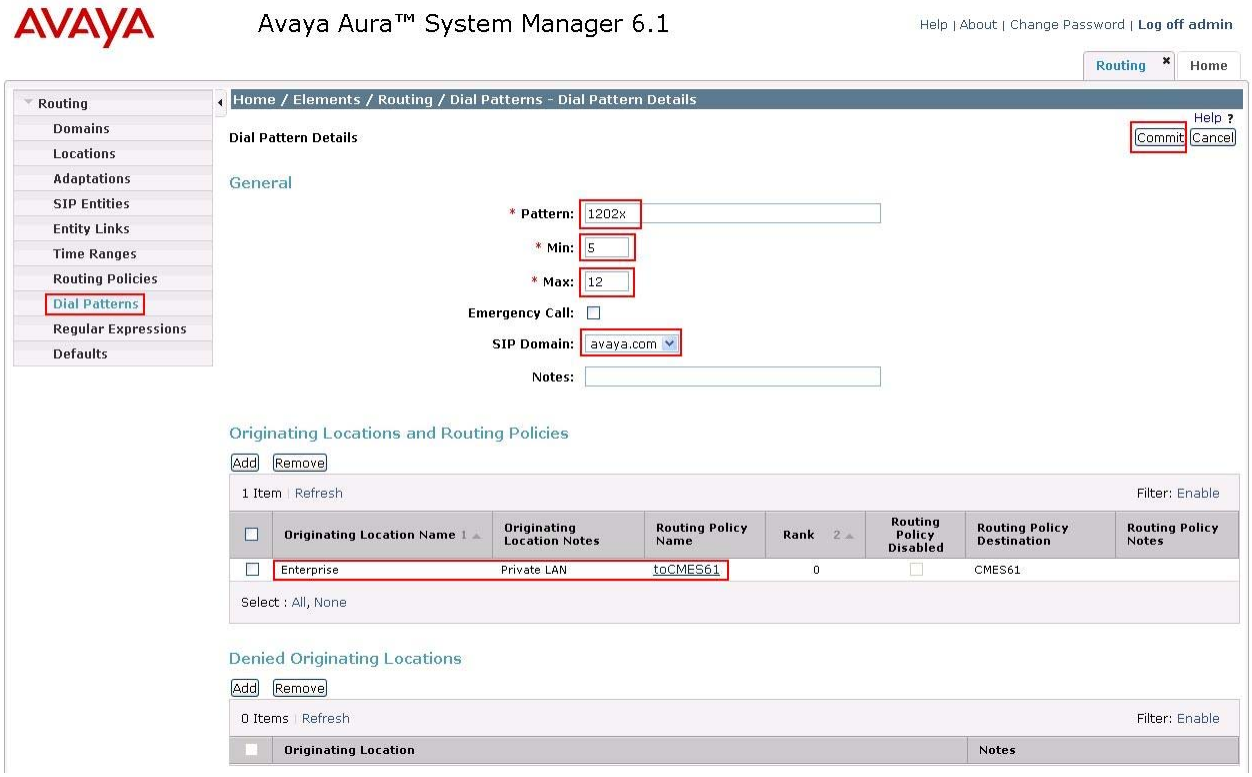
Inbound calls from Skype Connect will begin with **1202**. To configure the Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).
Under **General:**

- **Pattern** Dialed number or prefix
- **Min** Minimum length of dialed number
- **Max** Maximum length of dialed number
- **Notes** Comment on purpose of dial pattern
- **SIP Domain** Select the SIP Domain specified in **Section 5.2**

Under **Originating Locations and Routing Policy** select **Add** (not shown). Select the following entries:

- **Originating Location Name** Select the location created in **Section 5.3**
- **Routing Policies** Select the policy **toCMES61** created in **Section 5.7**

Select **Commit** button to save.



©2011 Avaya Inc. All Rights Reserved.

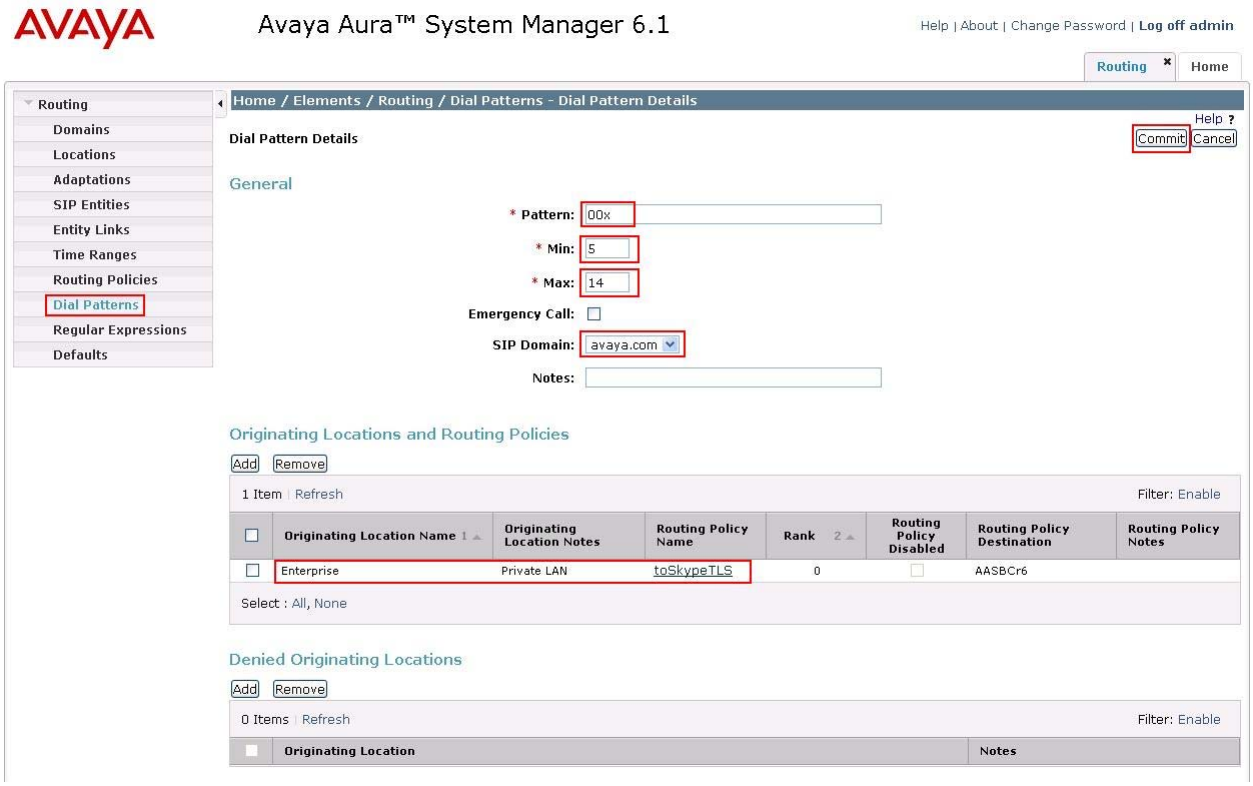
Outbound calls to Skype Connect numbers will begin with **00**. To configure the Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).
Under **General:**

- **Pattern** Dialed number or prefix
- **Min** Minimum length of dialed number
- **Max** Maximum length of dialed number
- **Notes** Comment on purpose of dial pattern
- **SIP Domain** Select the SIP Domain specified in **Section 5.2**

Under **Originating Locations and Routing Policy** select **Add** (not shown). Select the following entries:

- **Originating Location Name** Select the location created in **Section 5.3**
- **Routing Policies** Select the policy **toSkypeTLS** created in **Section 5.7**

Select **Commit** button to save.



©2011 Avaya Inc. All Rights Reserved.

6. Configure Skype Manager

This section provides the procedures for configuring Skype Manager and includes the following items:

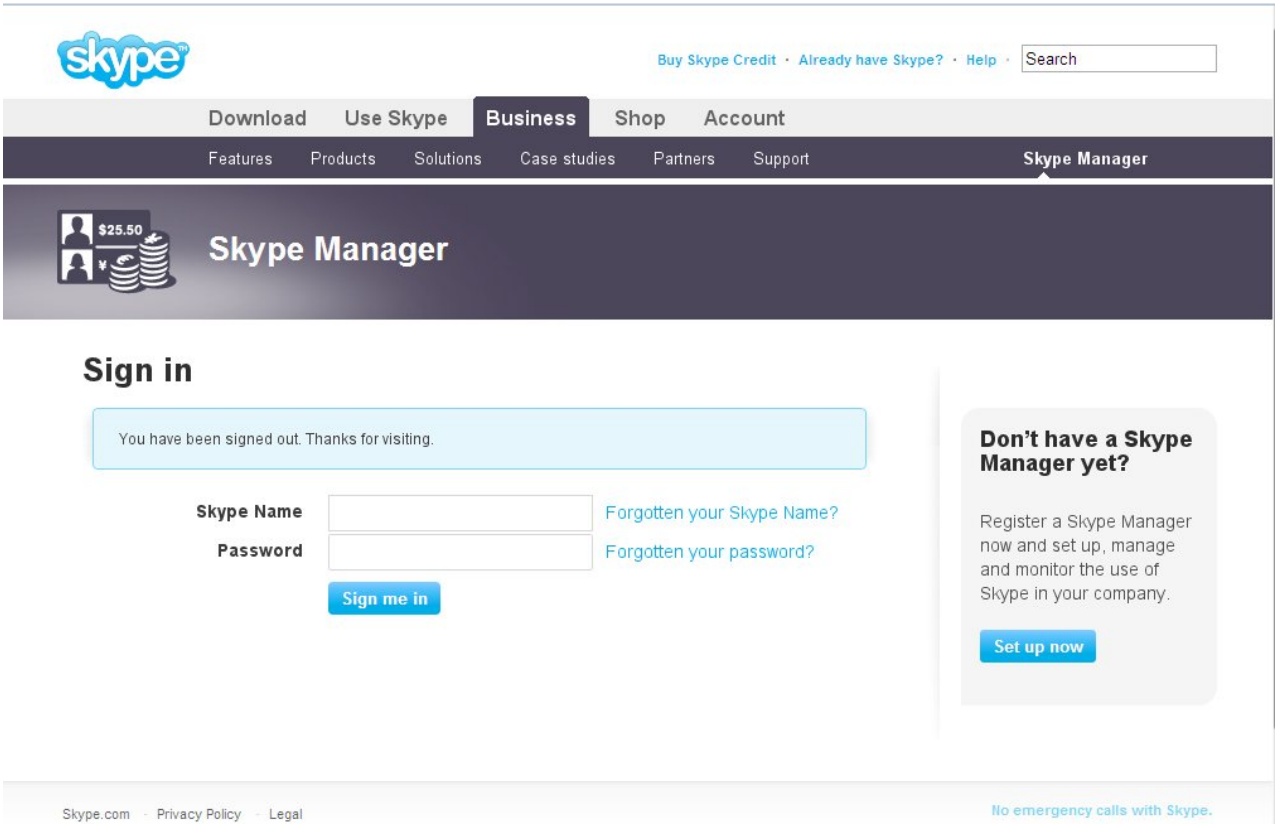
- Log in to Skype Manager
- Create SIP Profile
- Administer Maximum Simultaneous Calls
- Administer Online Numbers
- Administer Caller ID
- Create a Business User
- Add Business User to SIP Profile

These Application Notes assume that the Skype Manager account has enough credit allocated to create a new SIP Profile and associate Online Numbers with it.

Note – When Skype Connect R2.2 becomes Generally Available (GA), there will be an option (tick box) to select TLS/SRTP in Skype Manager. However, during interoperability testing with the Skype Connect R2.2, there was no Skype Manager provisioning required for TLS/SRTP.

6.1. Log in to Skype Manager

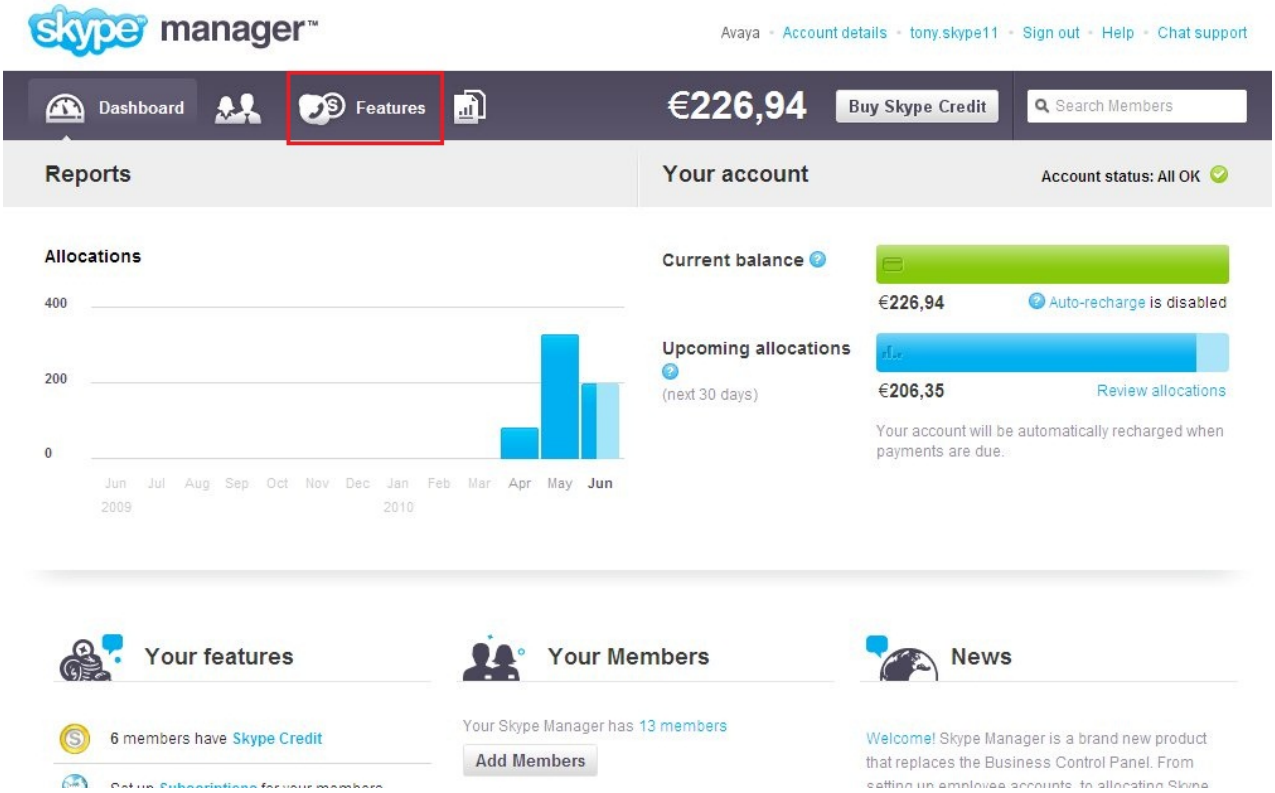
Configuration of a new SIP Profile and Business Users is accomplished by accessing the browser-based GUI of Skype Manager at **http://manager.skype.com**. Log in with the appropriate credentials.



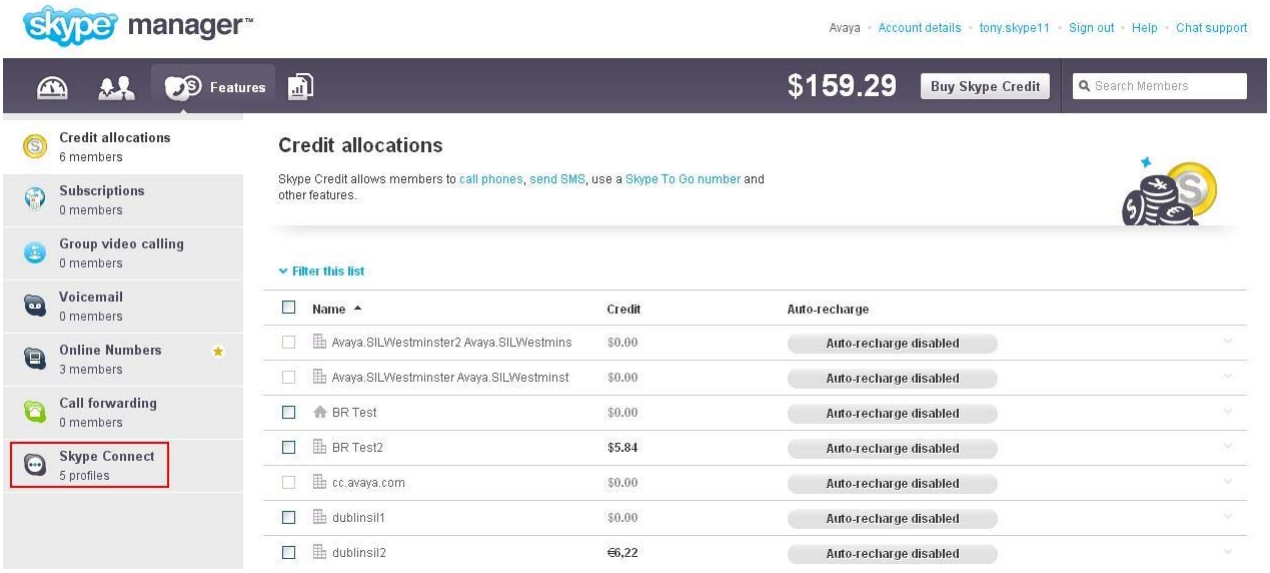
©2011 Avaya Inc. All Rights Reserved.

6.2. Create SIP Profile

The **Dashboard** page is displayed. Verify that enough credit is available in your company's account to create a new SIP Profile. The available total credit is shown on the toolbar below. Click **Features**.

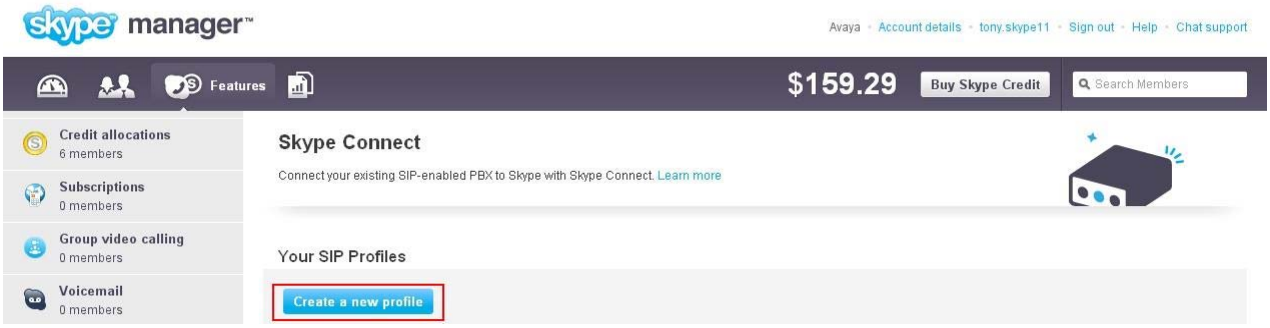


The **Features** page is displayed. Click **Skype Connect** on the left pane.

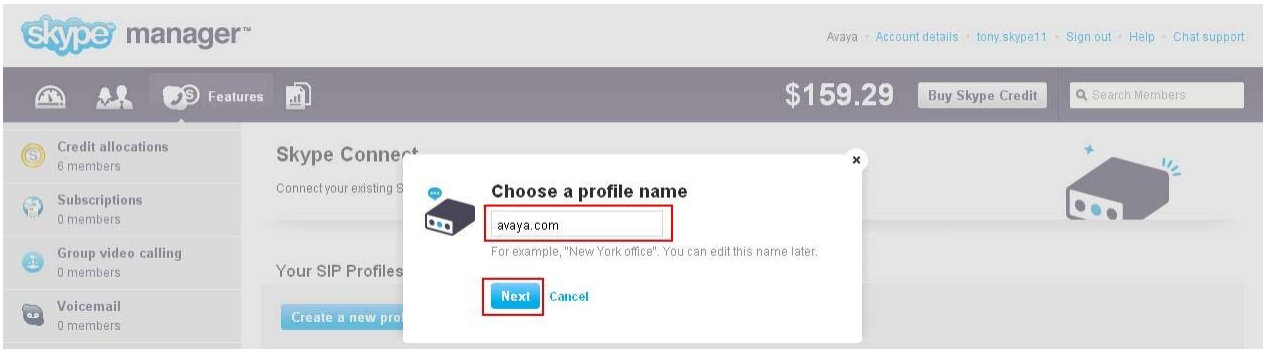


©2011 Avaya Inc. All Rights Reserved.

The **Skype Connect** page is displayed. Click **Create a new profile**.

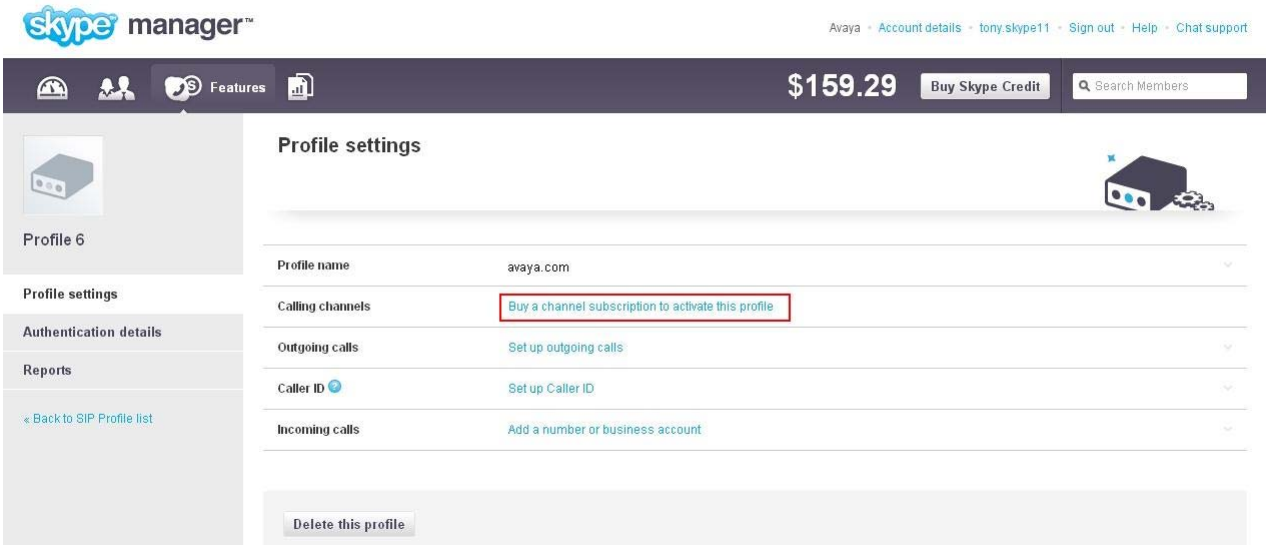


The **Choose a profile name** pop-up window is displayed. Type the name of your SIP Profile and click **Next**.



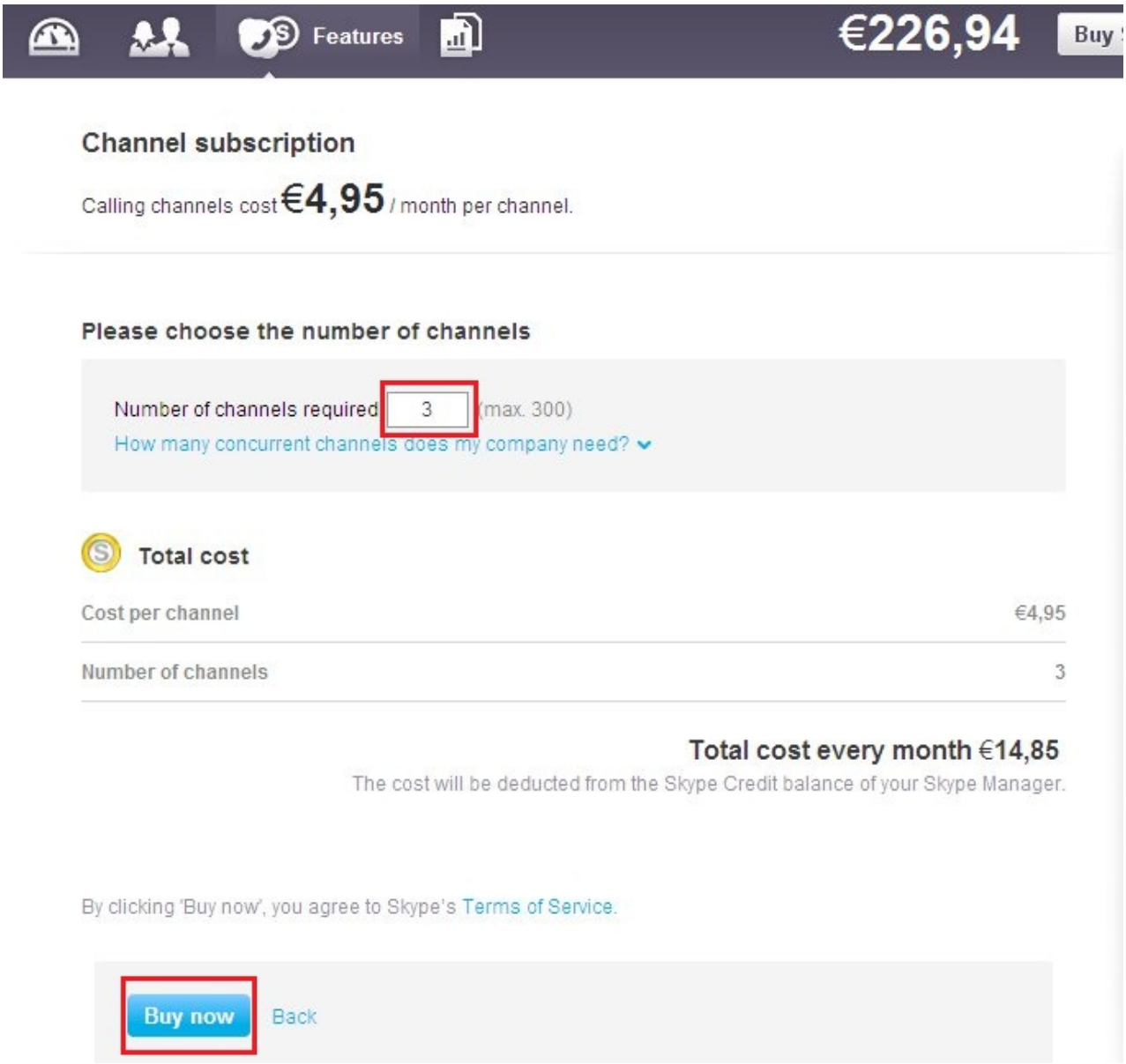
6.3. Administer Maximum Simultaneous Calls

The **Profile settings** page is displayed. Click **Buy a channel subscription to activate this profile**.



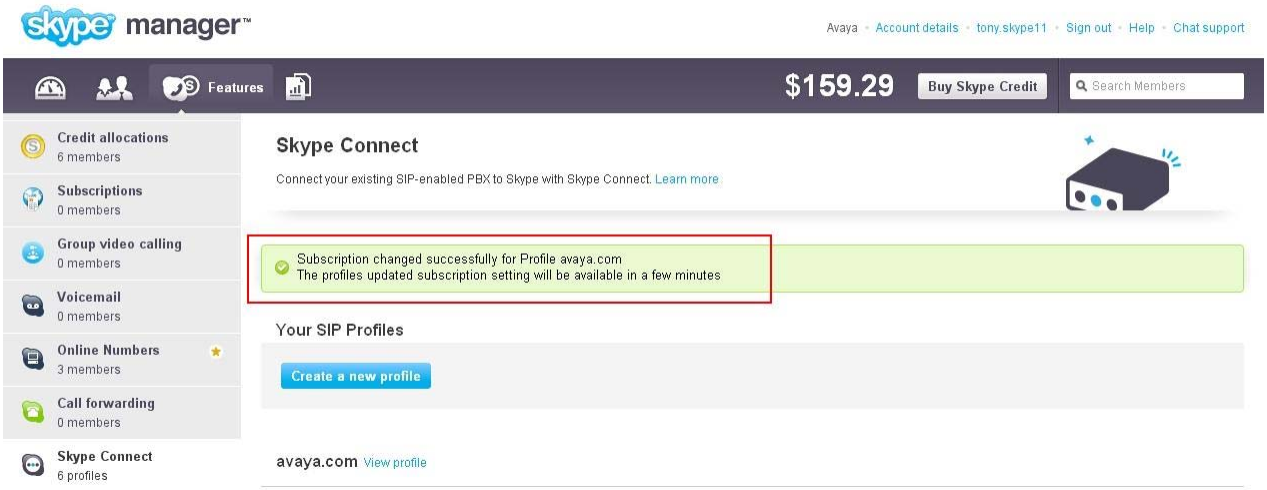
©2011 Avaya Inc. All Rights Reserved.

The **Channel subscription** page is displayed. Type the maximum number of simultaneous calls that your business users are expected to make. Click **Buy now**.

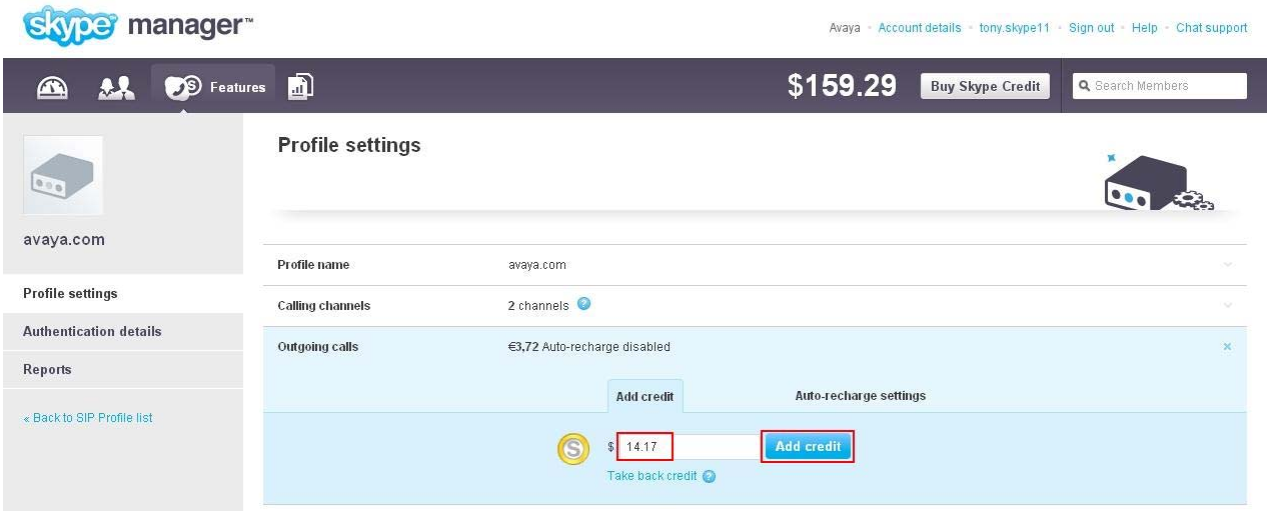


©2011 Avaya Inc. All Rights Reserved.

The below status message is displayed to confirm that the channel subscription was successful. Click **Set up outgoing calls** (not shown).



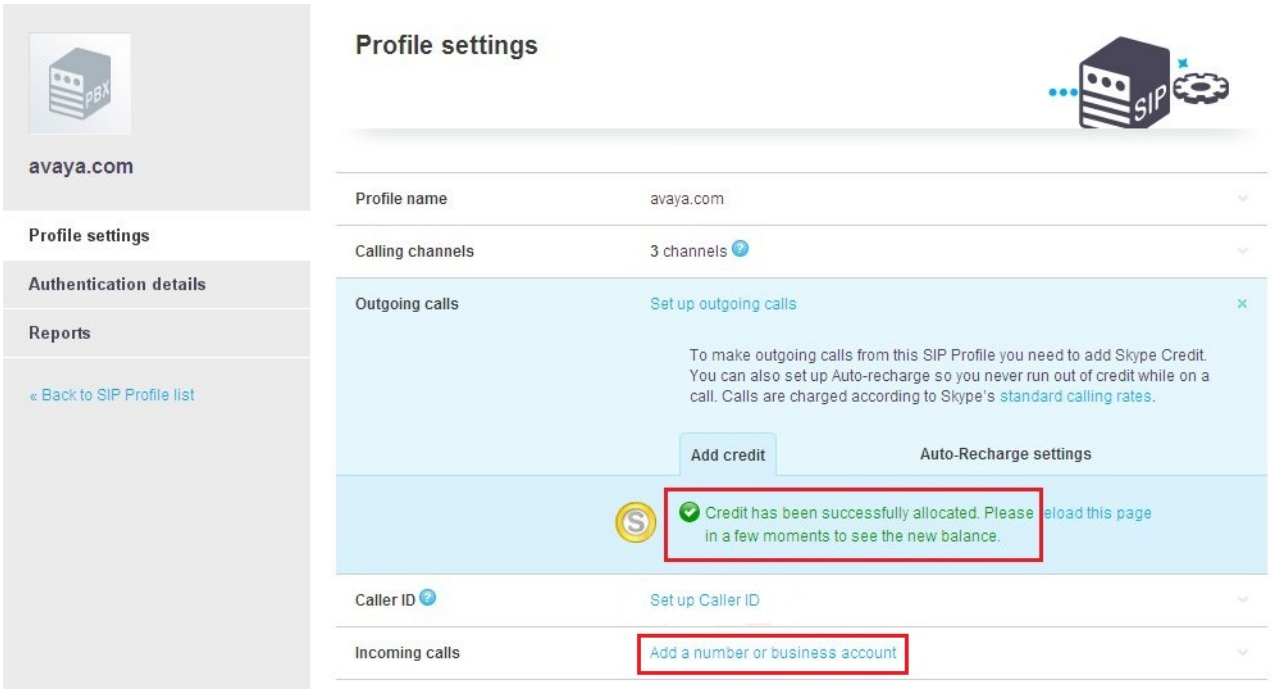
The **Profile settings** page is displayed. On the **Add credit** tab type the amount of credit you'd like to allocate for outbound calls. Note that calls to other SIP Profiles or Online Numbers of Skype Clients on the P2P network are free of charge.
Click **Add credit**.



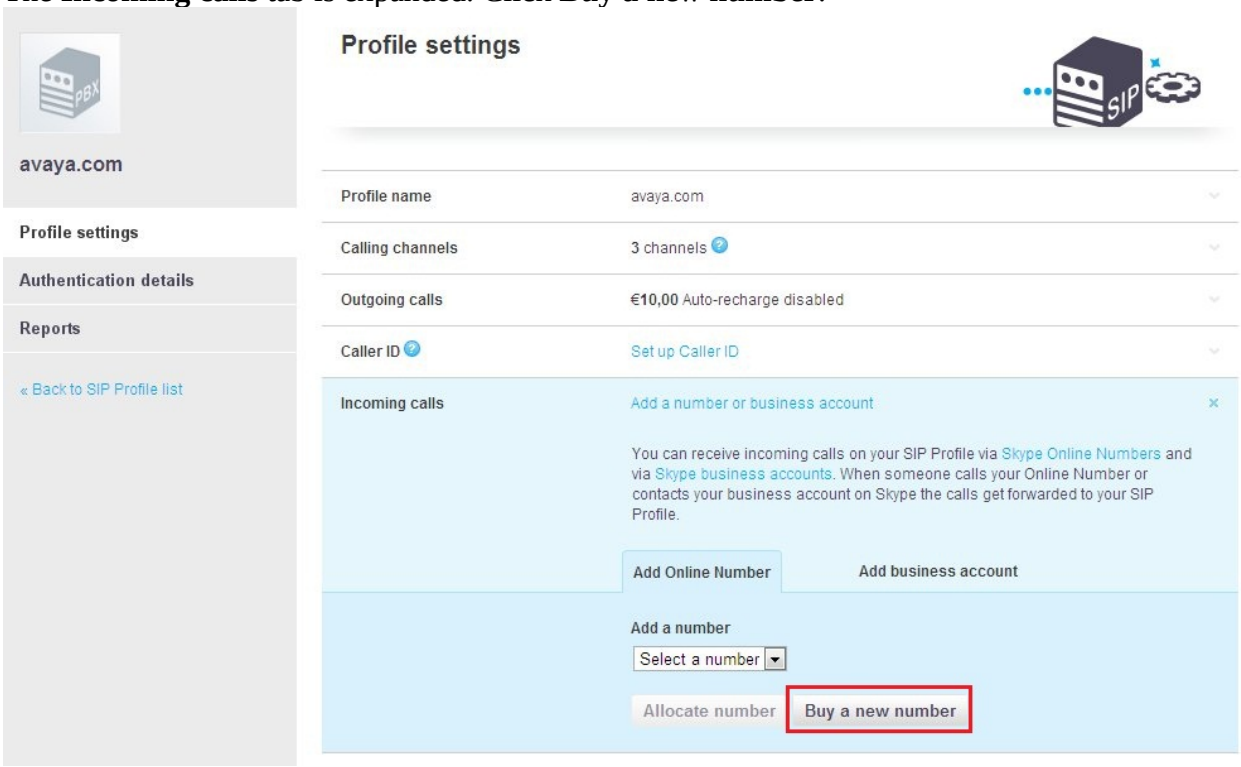
©2011 Avaya Inc. All Rights Reserved.

6.4. Administer Online Numbers

Online Numbers provide the same functionality as DID/DDIs in a traditional telephony environment. The below confirmation message is displayed once the credit allocation for outbound calls is complete. Click **Add a number or business account**.

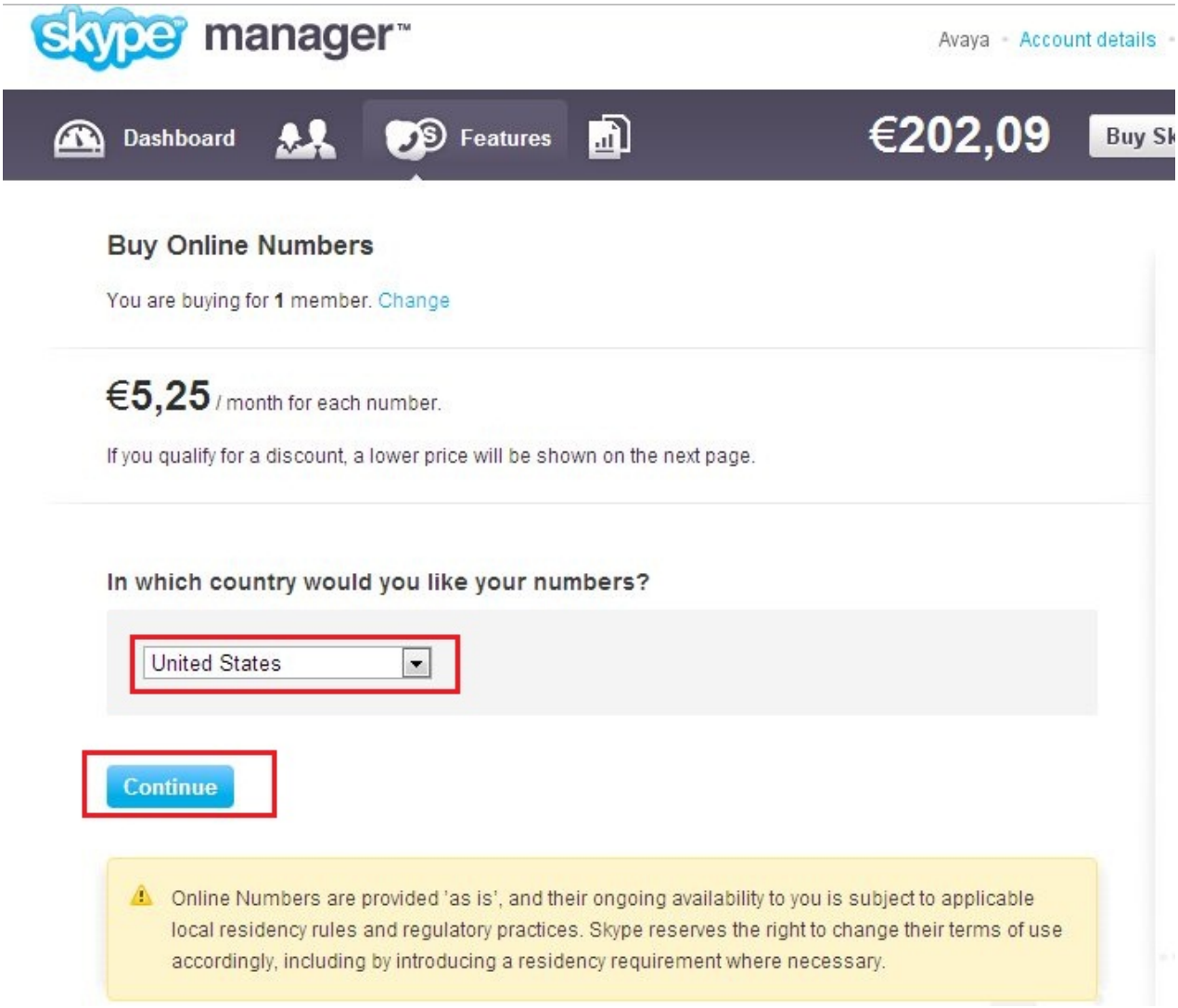


The **Incoming calls** tab is expanded. Click **Buy a new number**.



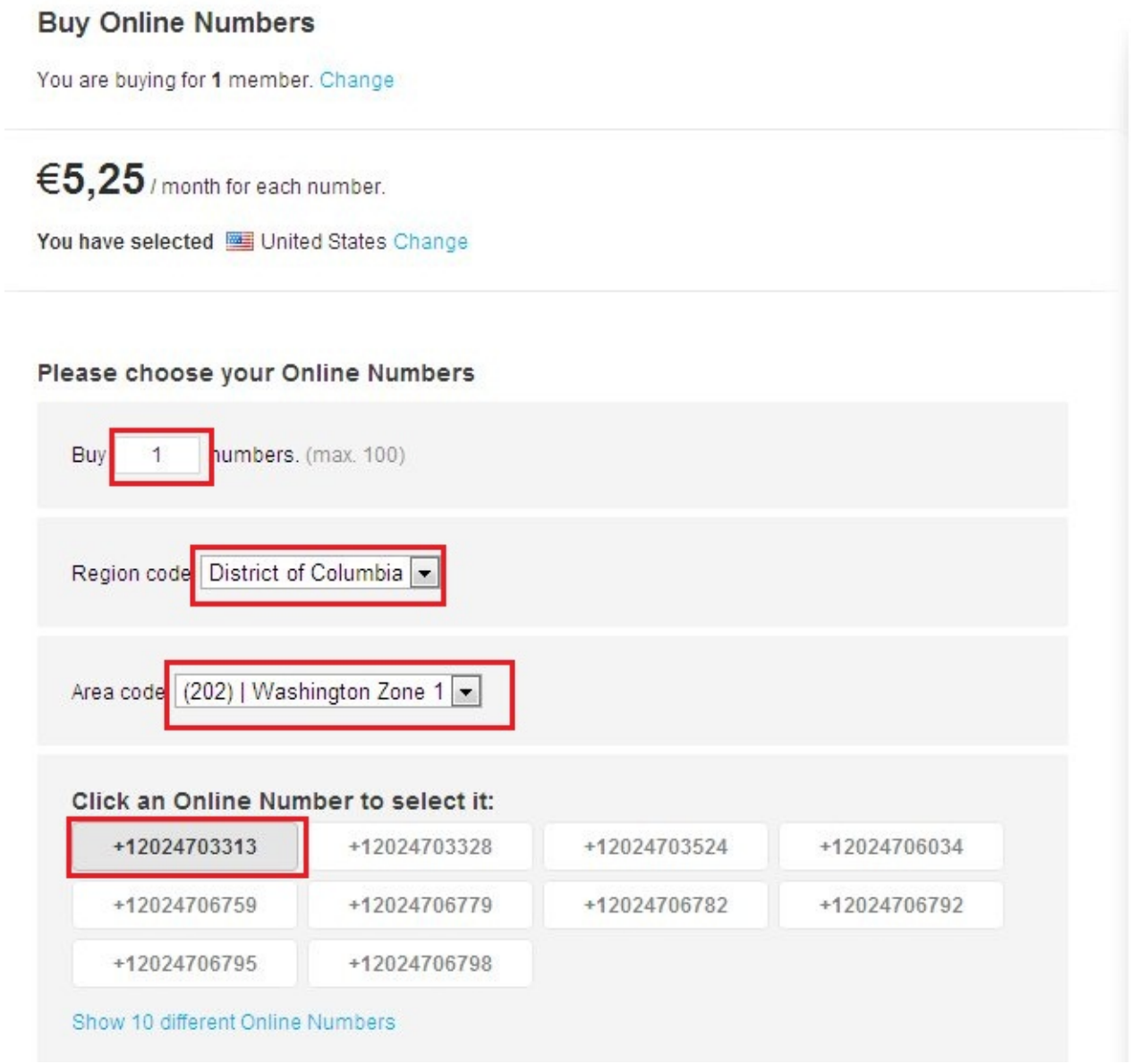
©2011 Avaya Inc. All Rights Reserved.

The **Buy Online Numbers** page is displayed. Select **a country** from the drop-down list box and click **Continue**.



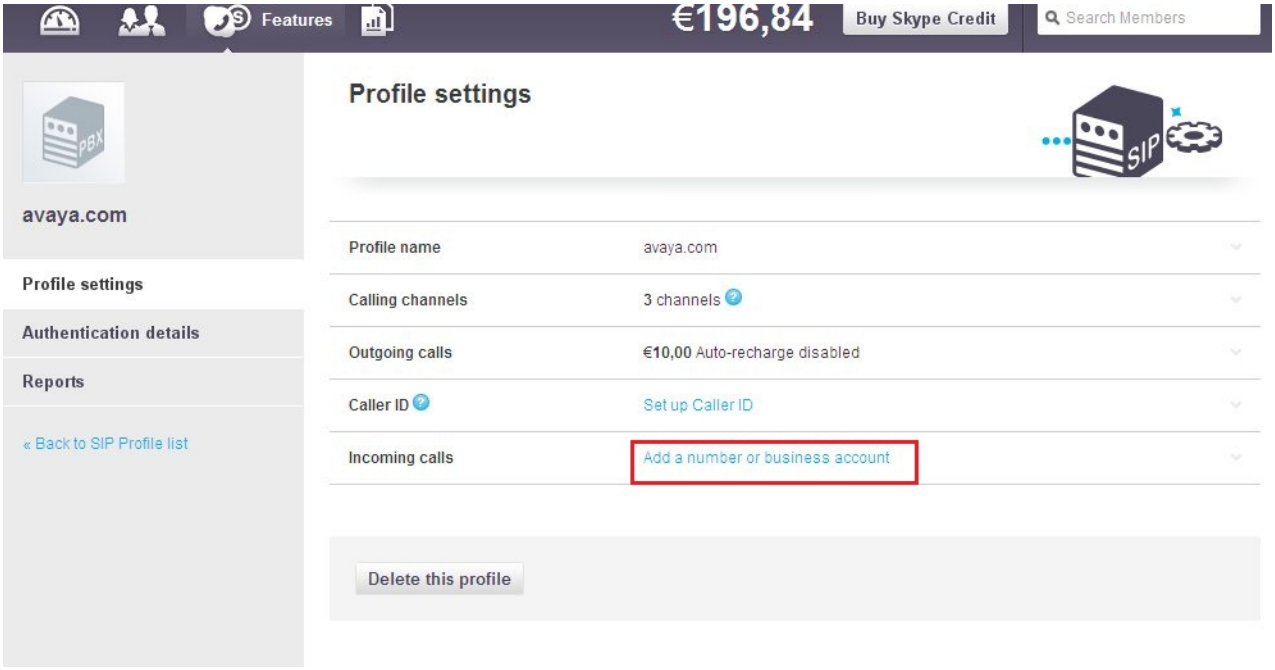
©2011 Avaya Inc. All Rights Reserved.

The **Buy Online Numbers** page is displayed. Under **Please choose your Online Numbers** type the number of required Online Numbers which are used as DIDs in conjunction with the SIP Profile. Select **a state or county** from the **Region Code** drop-down list box. Select an **area code** from the **Area code** drop-down list box. Under **Click an Online Number to select it:** Select a number. Scroll down and click **Buy now** (not shown).

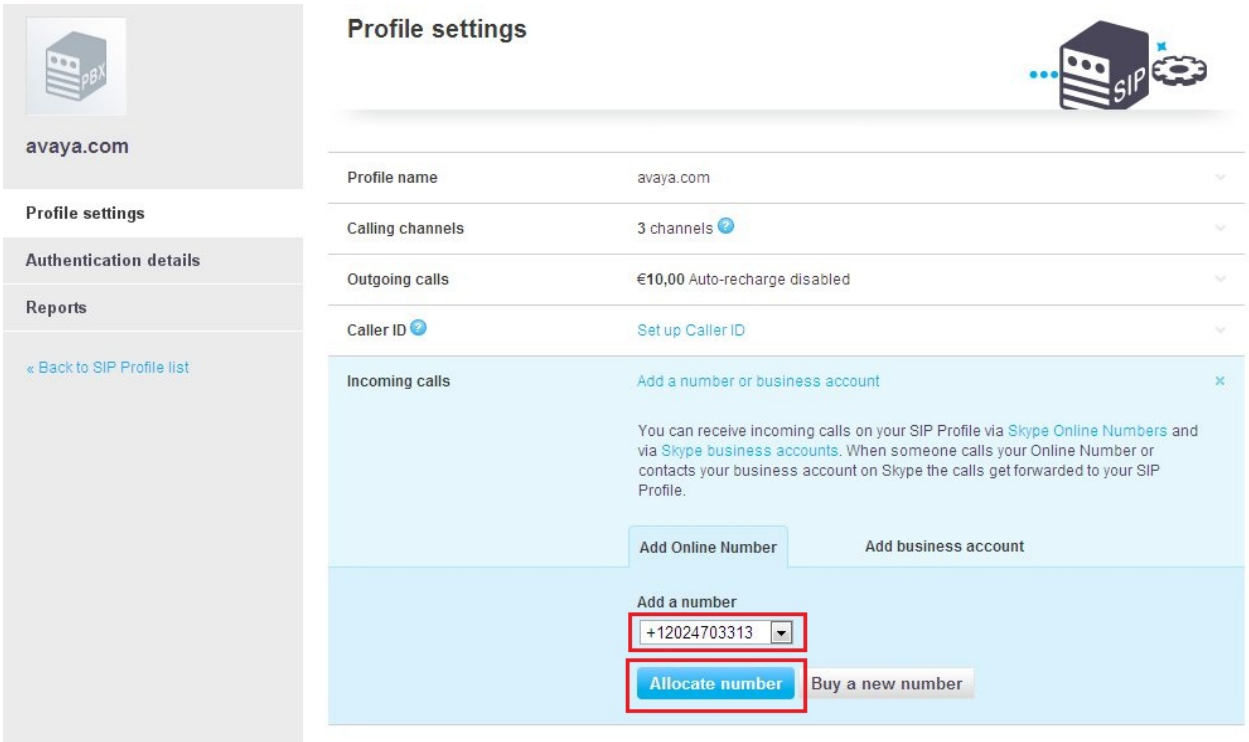


©2011 Avaya Inc. All Rights Reserved.

The **Profile settings** page is displayed. Click **Add a number or business account**.



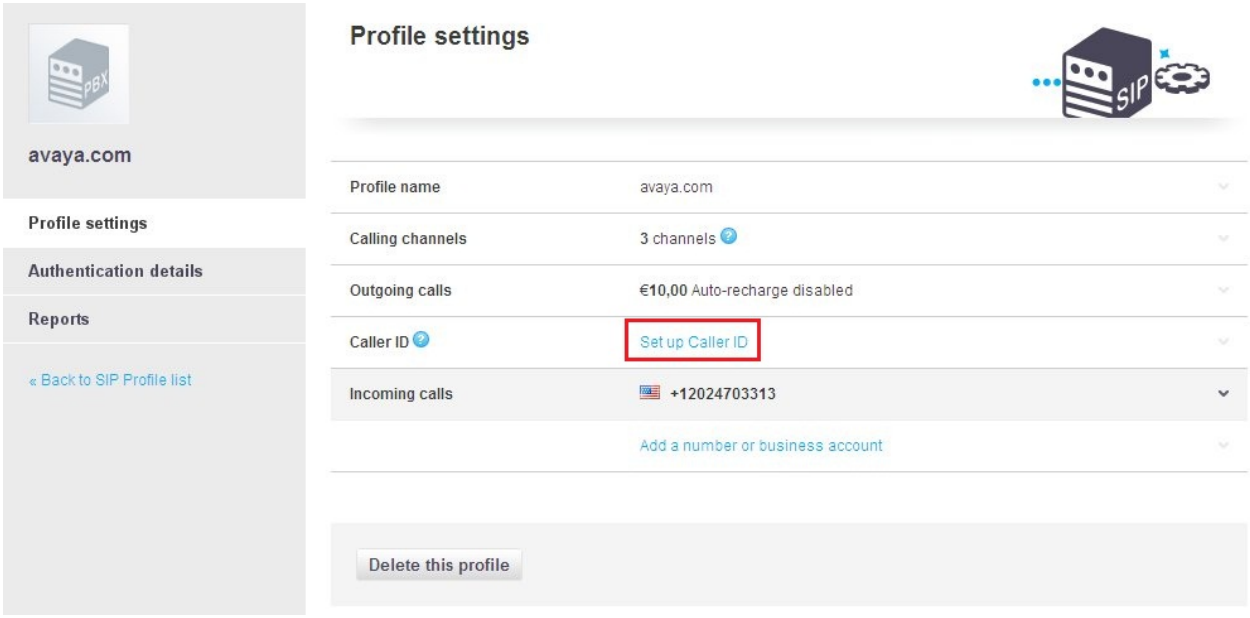
Select the newly purchased Online Number from the **Add a number** drop-down list box then click **Allocate number**.



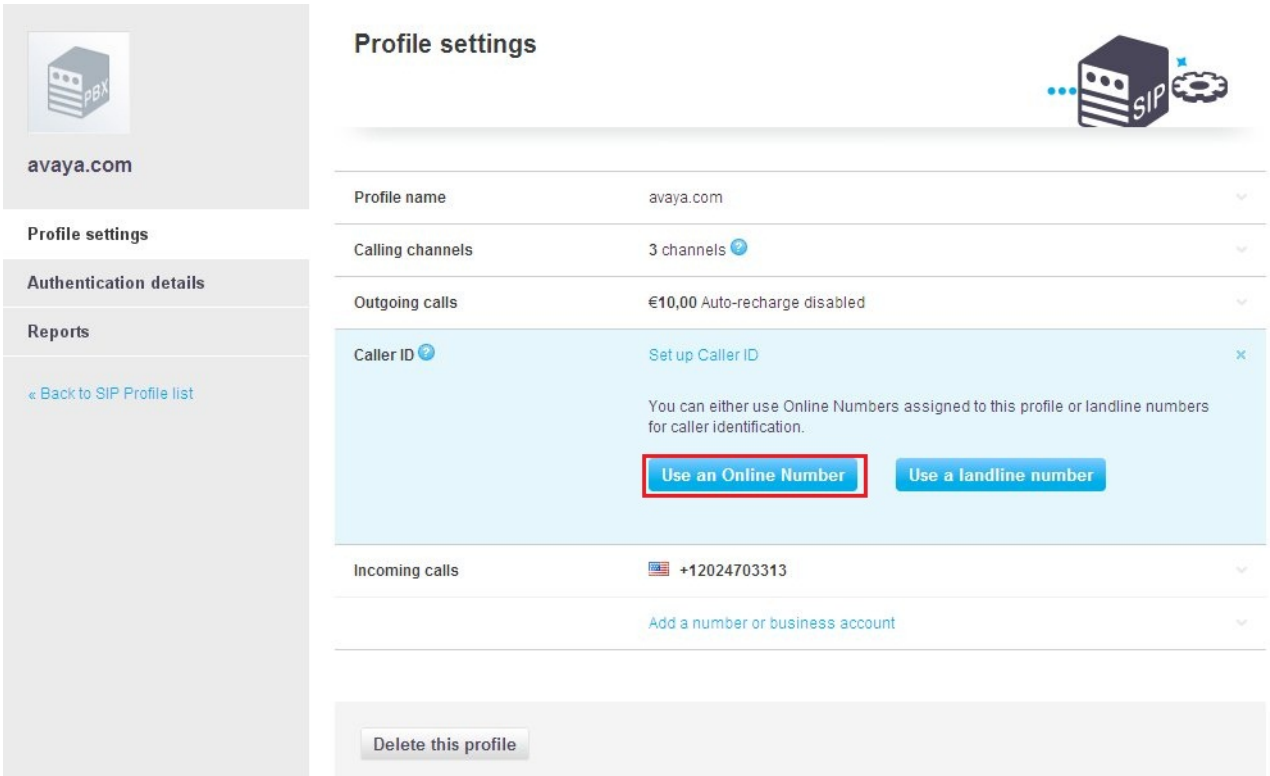
©2011 Avaya Inc. All Rights Reserved.

6.5. Administer Caller ID

The **Profile settings** page is displayed. Click **Set up Caller ID**.

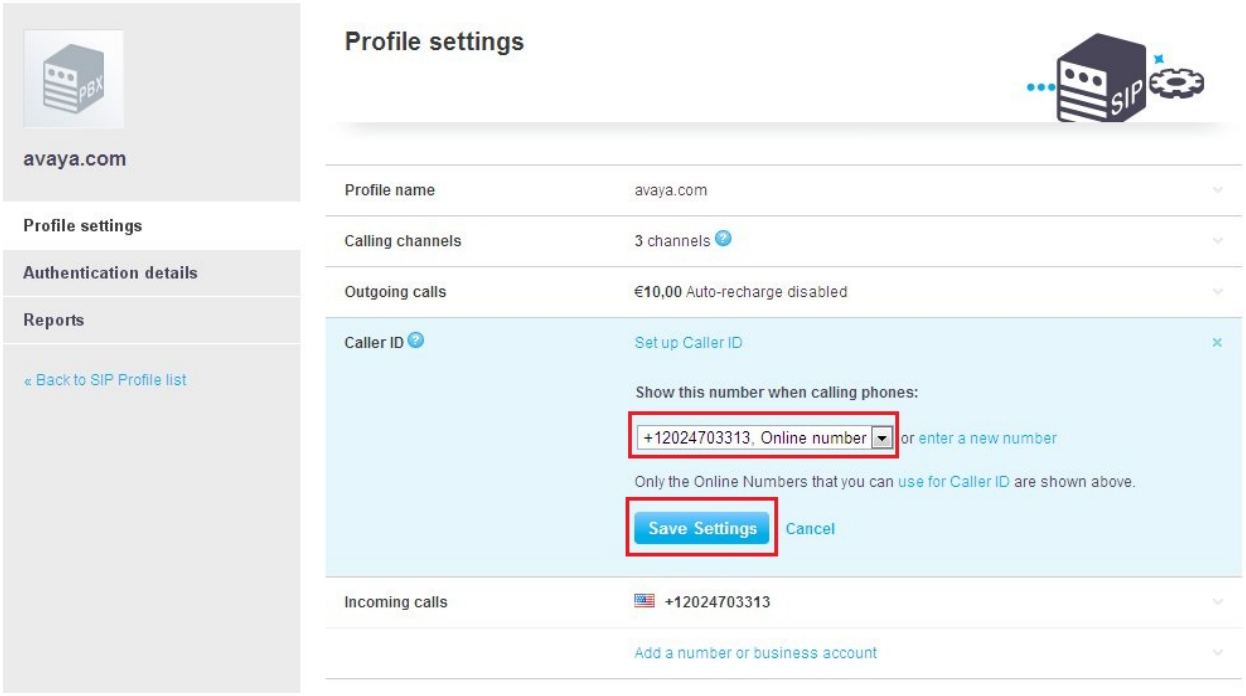


Click **Use an Online Number**.

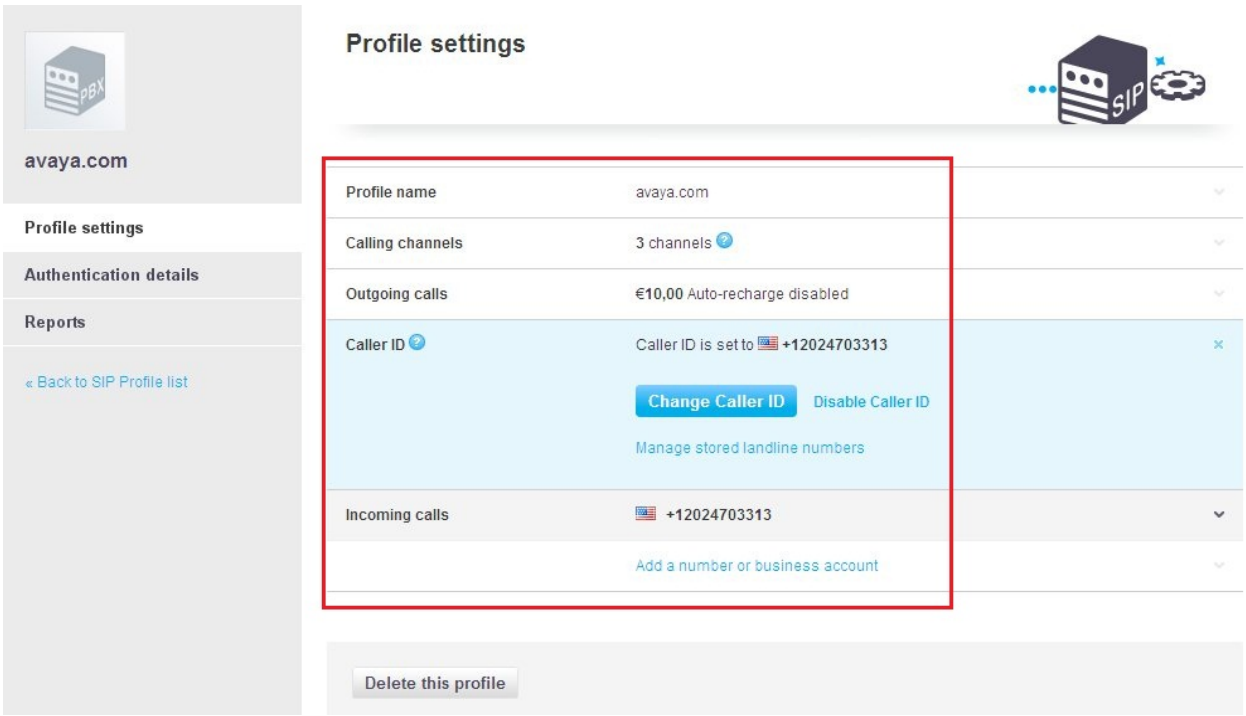


©2011 Avaya Inc. All Rights Reserved.

Select an Online Number from the **Show this number when calling phones:** drop-down list box than click **Save Settings**.



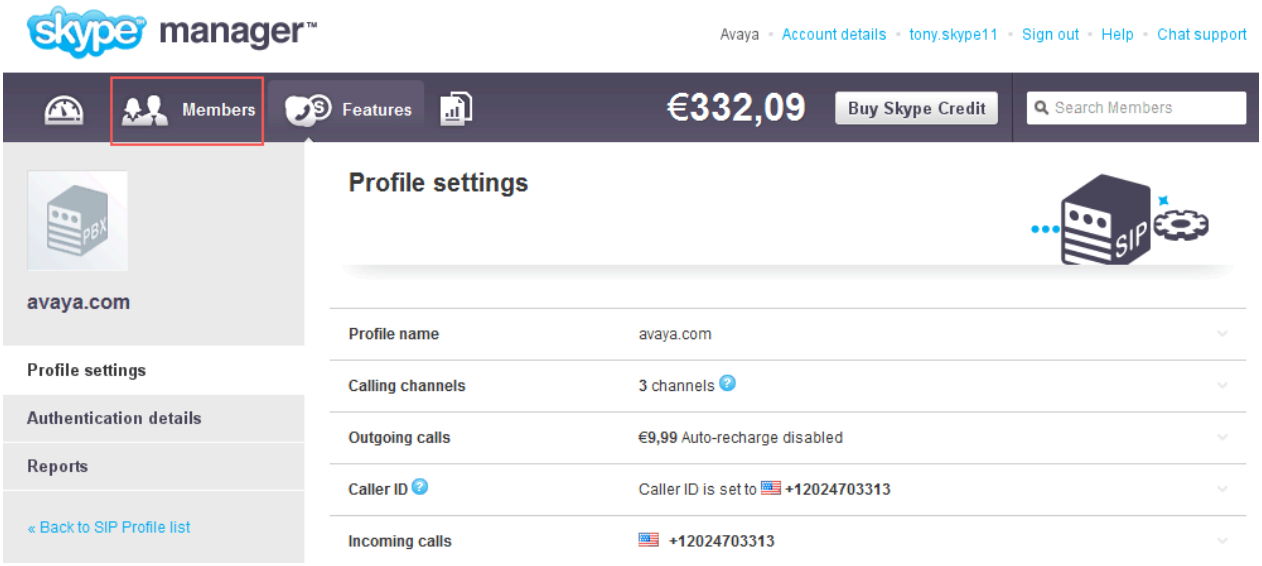
The following screenshot displays a sample Profile with both the Caller ID and the Incoming calls (DID) set to the same Online Number.



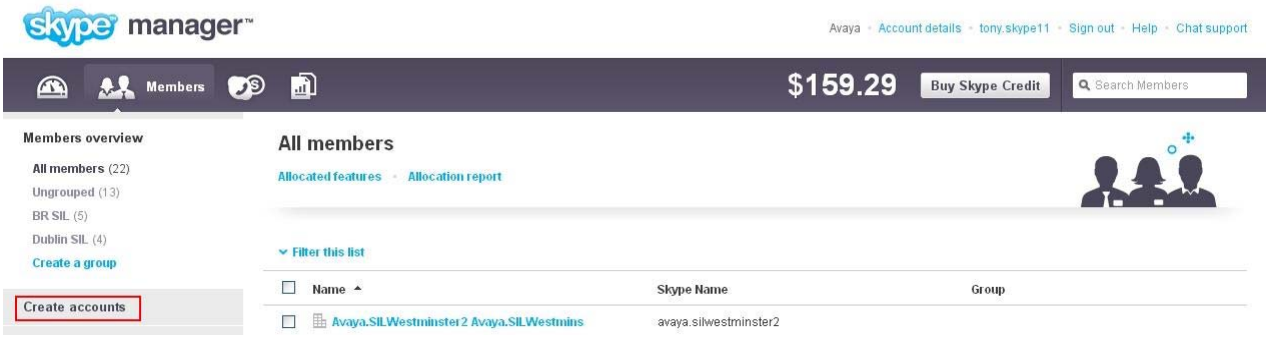
©2011 Avaya Inc. All Rights Reserved.

6.6. Create a Business User

A Business User with a unique Skype Name needs to be created and associated with the extension of the enterprise user (3001) for click-to-call functionality to work from the Skype P2P Network. Click **Members** on the toolbar.

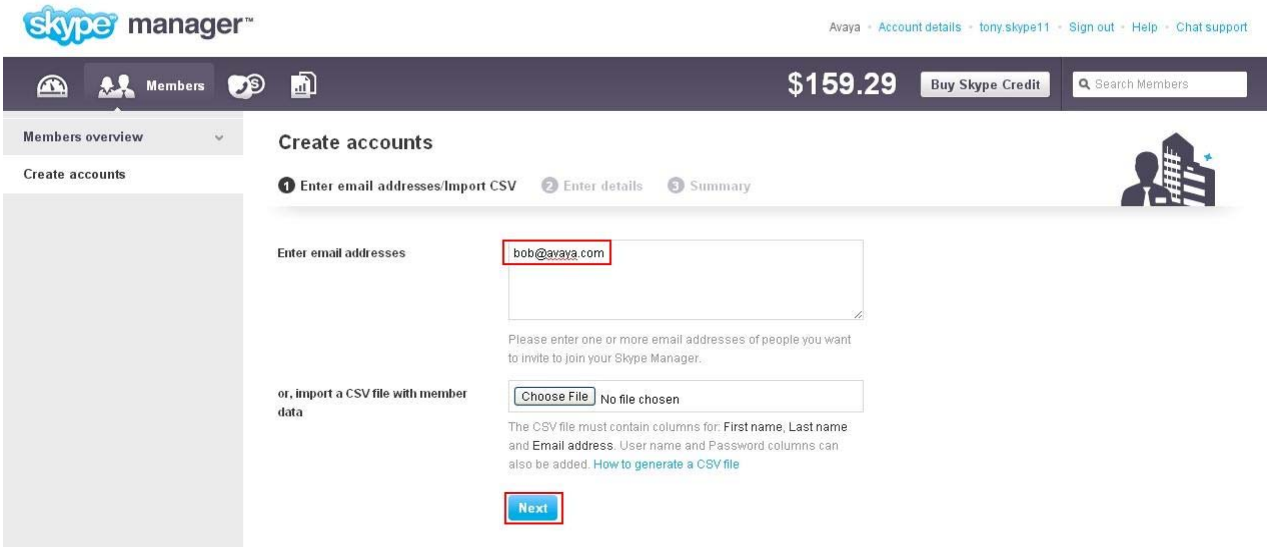


The **All Members** page is displayed. Click **Create accounts.**



©2011 Avaya Inc. All Rights Reserved.

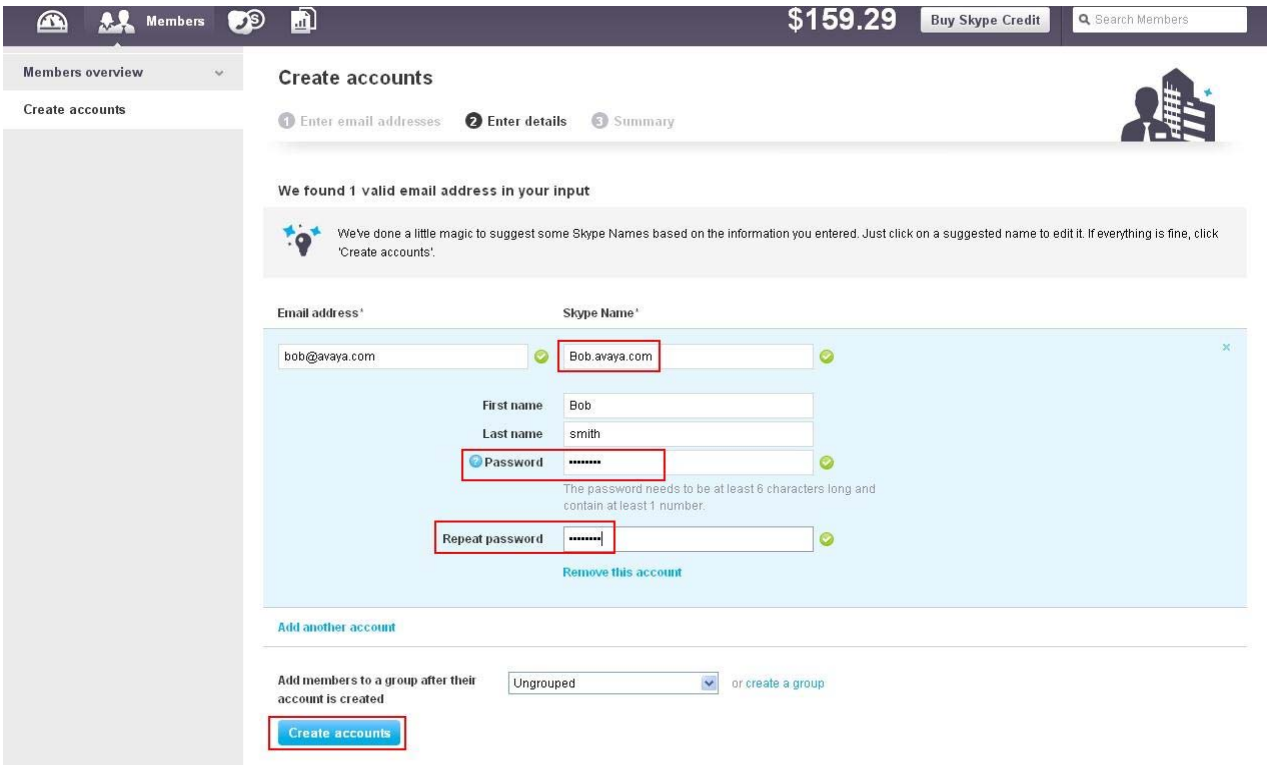
The **Create accounts** page is displayed. Enter an email address in the text field as Skype Manager sends an automated email once the new account is created. Click **Next**.



Under **Enter details** fill in the following fields:

- **Skype Name:** Type a unique name. Skype Client users will click on this Skype Name to initiate a call to the enterprise user with extension 3001.
- **Password:** Type a password.
- **Repeat Password:** Repeat the password.

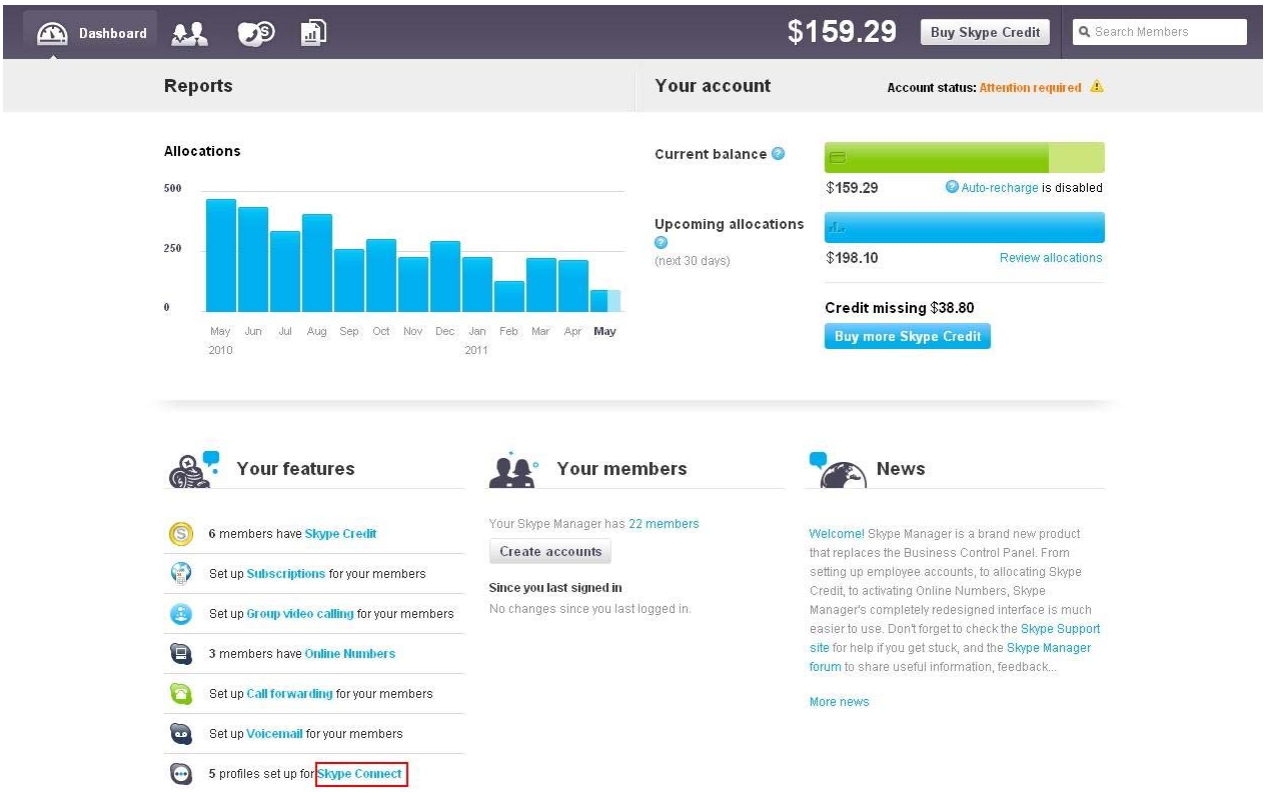
Click **Create accounts.**



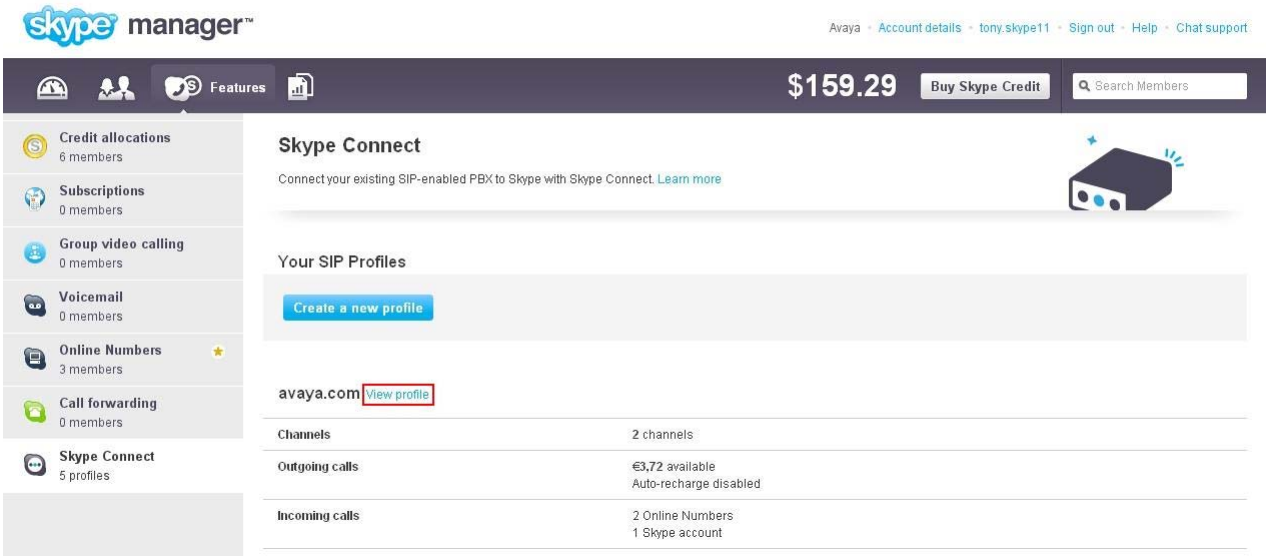
©2011 Avaya Inc. All Rights Reserved.

6.7. Add Business User to SIP Profile

Click **Dashboard** and scroll down and click **Skype Connect**.

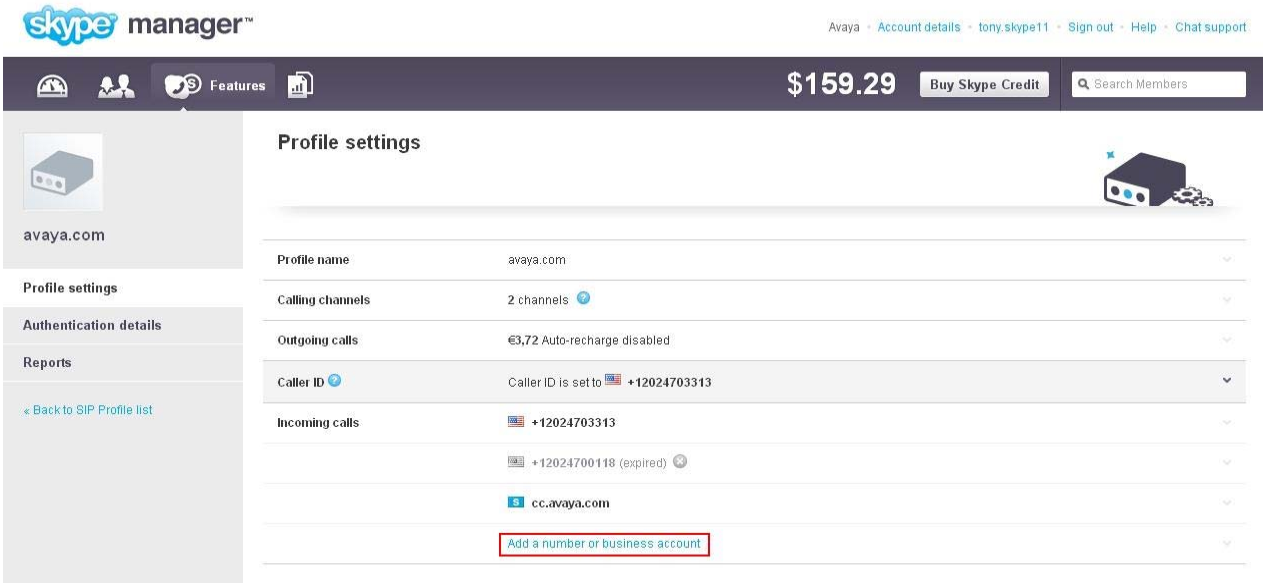


The **Skype Connect** page is displayed. Click **View profile**.

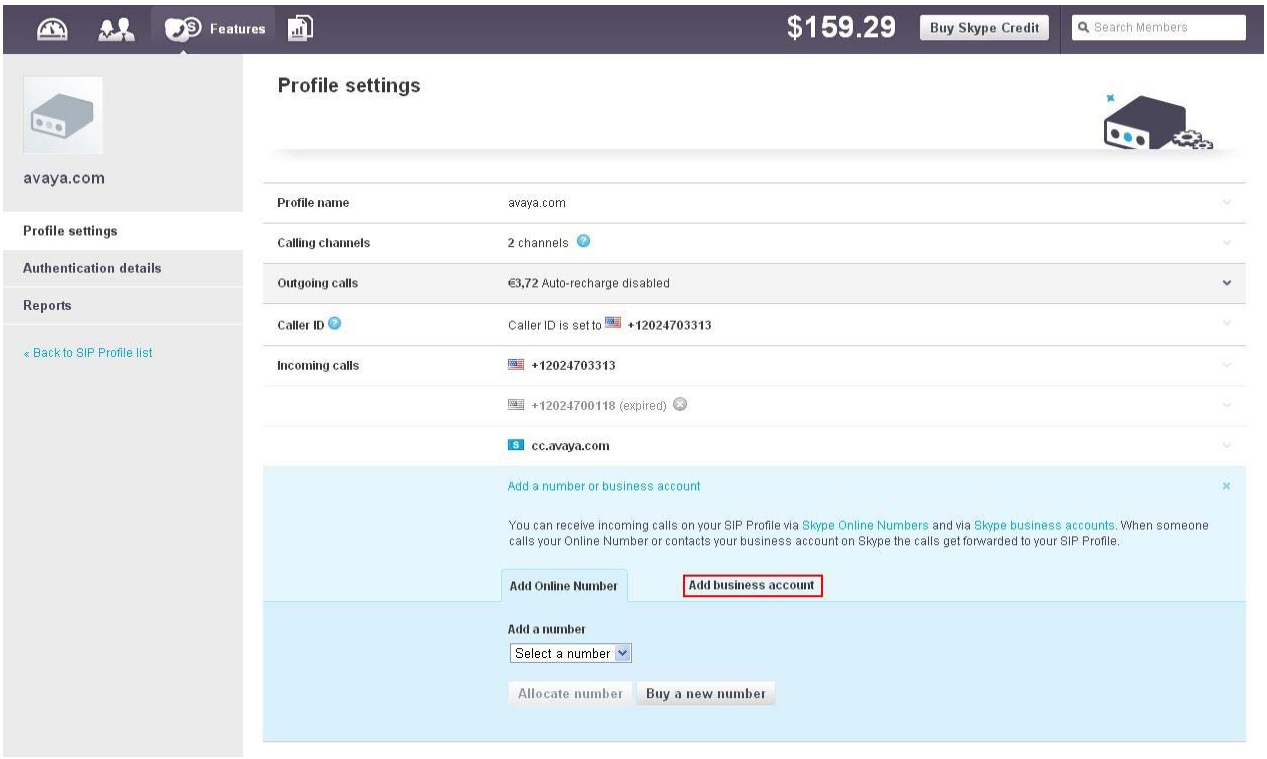


©2011 Avaya Inc. All Rights Reserved.

The **Profile settings** page is displayed. Click **Add a number or business account**.



The **Add Online Number** tab is displayed. Click **Add business account**.

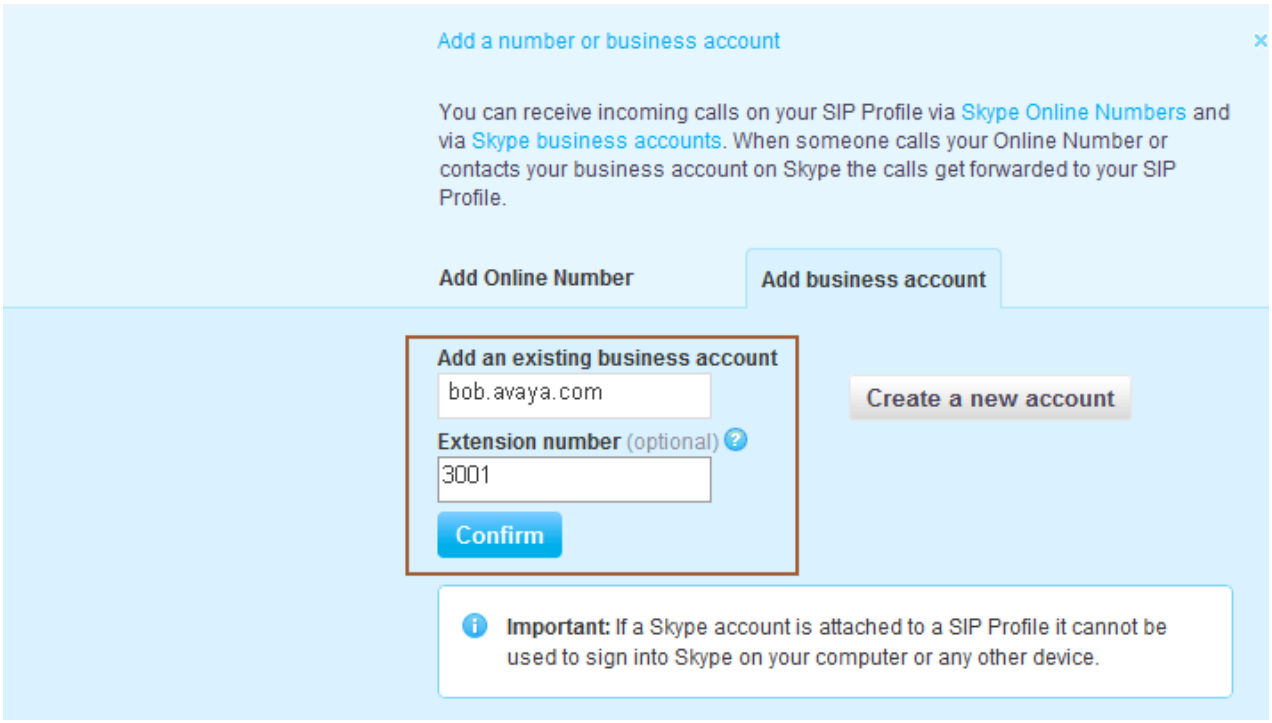


©2011 Avaya Inc. All Rights Reserved.

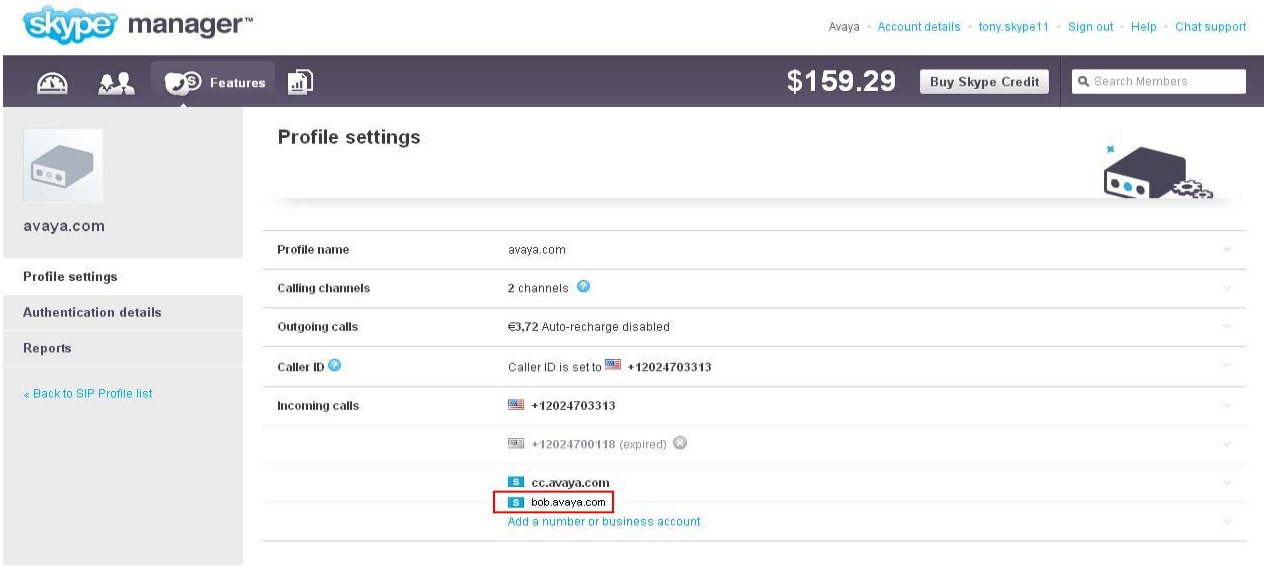
Under the **Add business account** tab fill in the following fields:

- **Add an existing business account:** Type a unique name. Skype Client users will click on the Skype Name to initiate a call to the enterprise user with extension 3001.
- **Extension number:** Type an extension.

Click **Confirm.**



The **Profile settings** page is displayed. Verify that the newly created Skype Name is displayed under the **Incoming calls** section.



©2011 Avaya Inc. All Rights Reserved.

7. Configure Avaya Aura® Session Border Controller

This section provides the procedures for configuring Avaya Aura® Session Border Controller and includes the following items:

- Log in to Avaya Aura® Session Border Controller using the GUI
- Administer SIP Domains
- Administer TLS Certificate
- Administer TLS on the Outside Interface
- Administer Authentication
- Administer Outbound SIP Header Manipulation Rules
- Administer Inbound SIP Header Manipulation Rules
- Administer SIP Header Rules for Topology Hiding
- Save the Configuration

Appendix B contains a sample configuration file in text form.

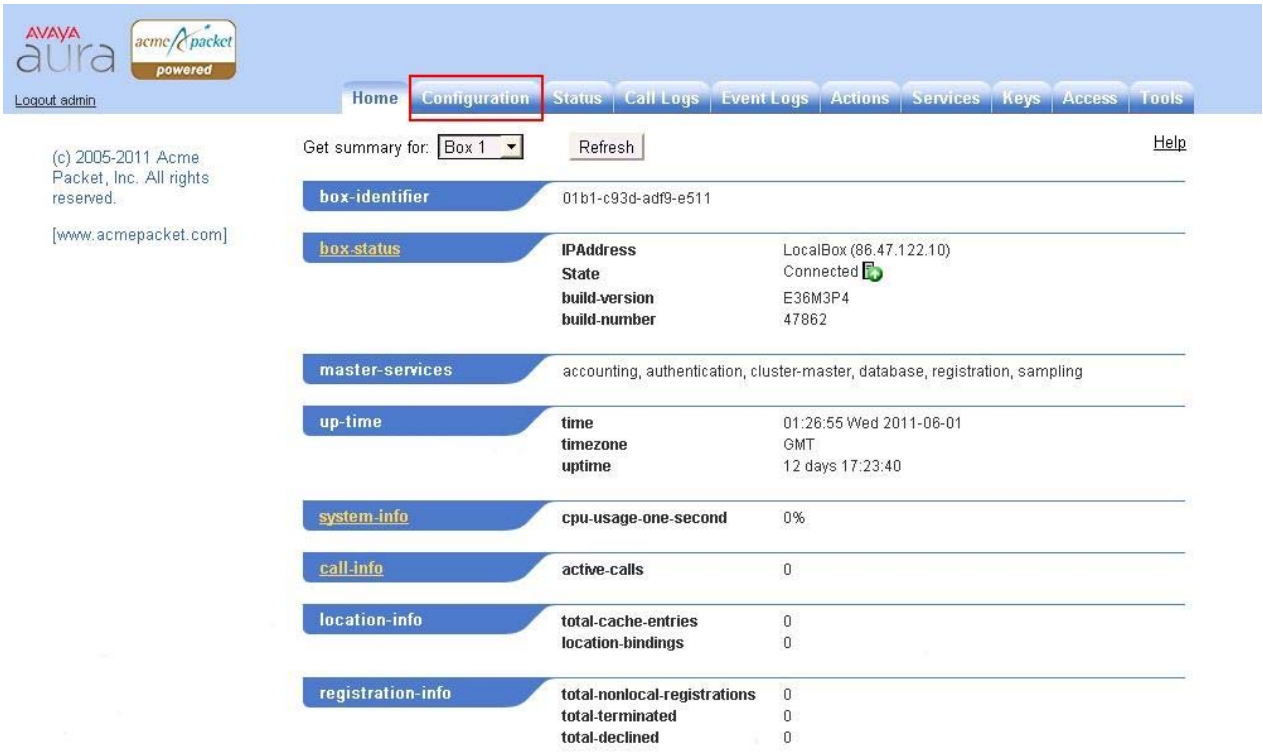
7.1. Log in to Avaya Aura® Session Border Controller using the GUI

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® Session Border Controller, using the URL "**https://<ip-address>**", where "<ip-address>" is the IP address of the inside interface of the Avaya Aura® Session Border Controller. Log in with the appropriate credentials.

©2011 Avaya Inc. All Rights Reserved.

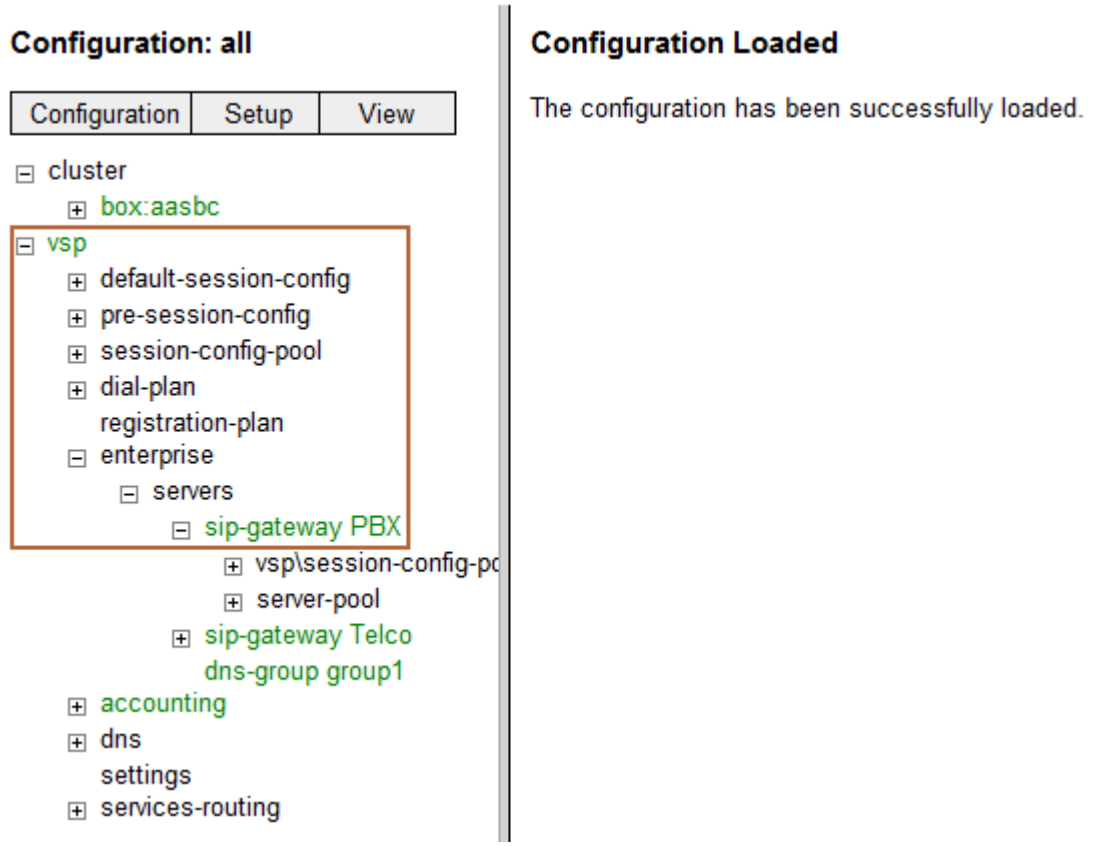
7.2. Administer SIP Domains

The Avaya Aura® Session Border Controller performs topology hiding by translating the private domain avaya.com to the public domain sip.skype.com for outbound calls and vice-versa for inbound calls. The following steps assign the domain names to the corresponding SIP Entities. The **Home** page is displayed. Select the **Configuration** tab on the toolbar.



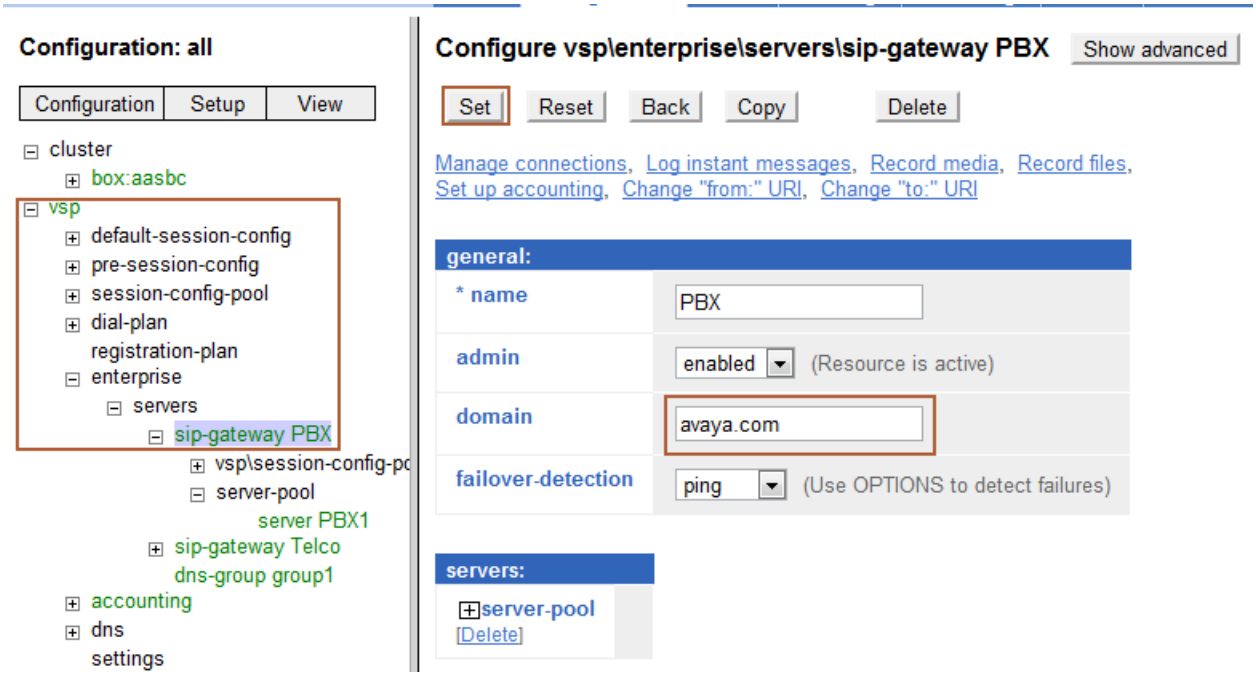
©2011 Avaya Inc. All Rights Reserved.

The **Configuration Loaded** page is displayed. Expand **vsp -> enterprise -> servers** and click on **sip-gateway PBX.**



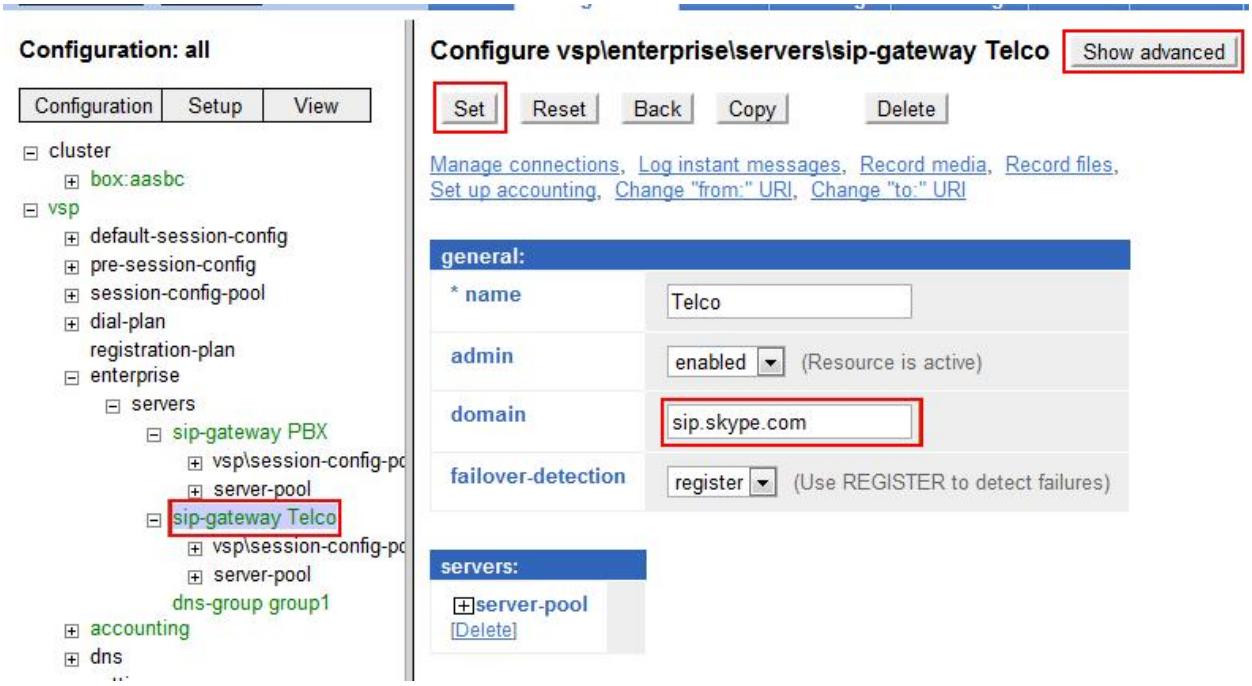
©2011 Avaya Inc. All Rights Reserved.

The **Configure vsp\enterprise\servers\sip-gateway PBX** page is displayed. Type **avaya.com** in the domain field then click **Set**.



©2011 Avaya Inc. All Rights Reserved.

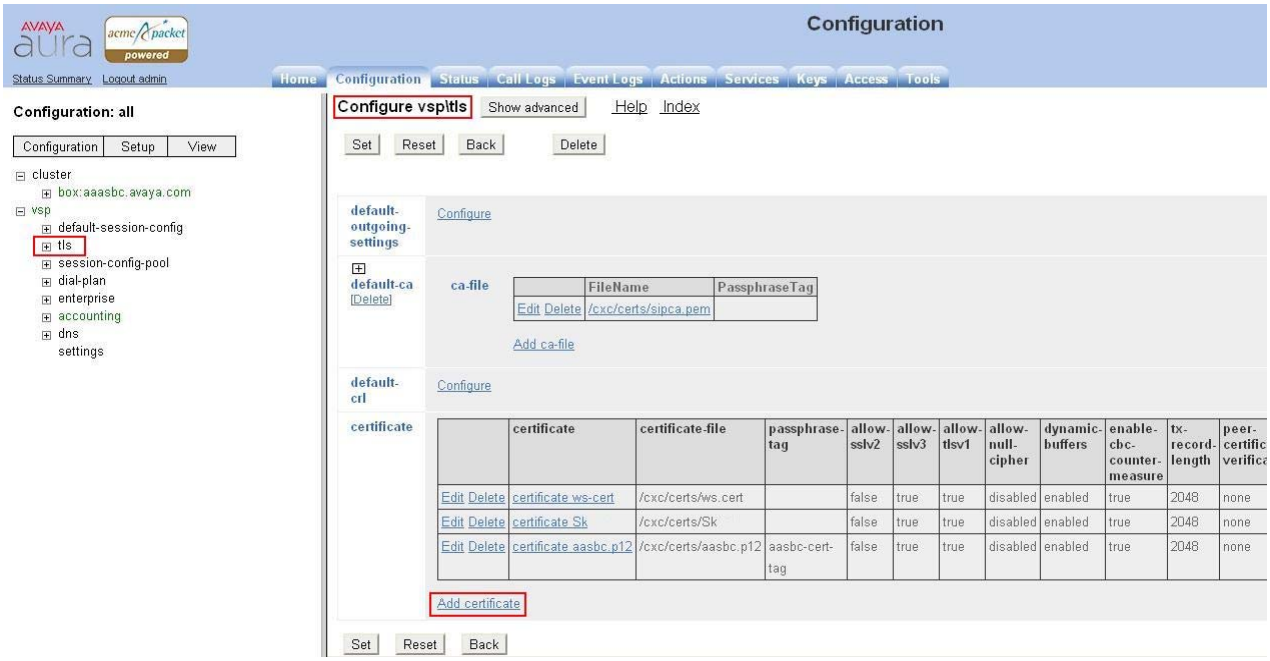
Select **sip-gateway Telco** on the left pane. The **Configure vsp\enterprise\servers\sip-gateway Telco** page is displayed. Type **sip.skype.com** in the **domain** field then click **Set**.



©2011 Avaya Inc. All Rights Reserved.

7.3. Administer TLS Certificate

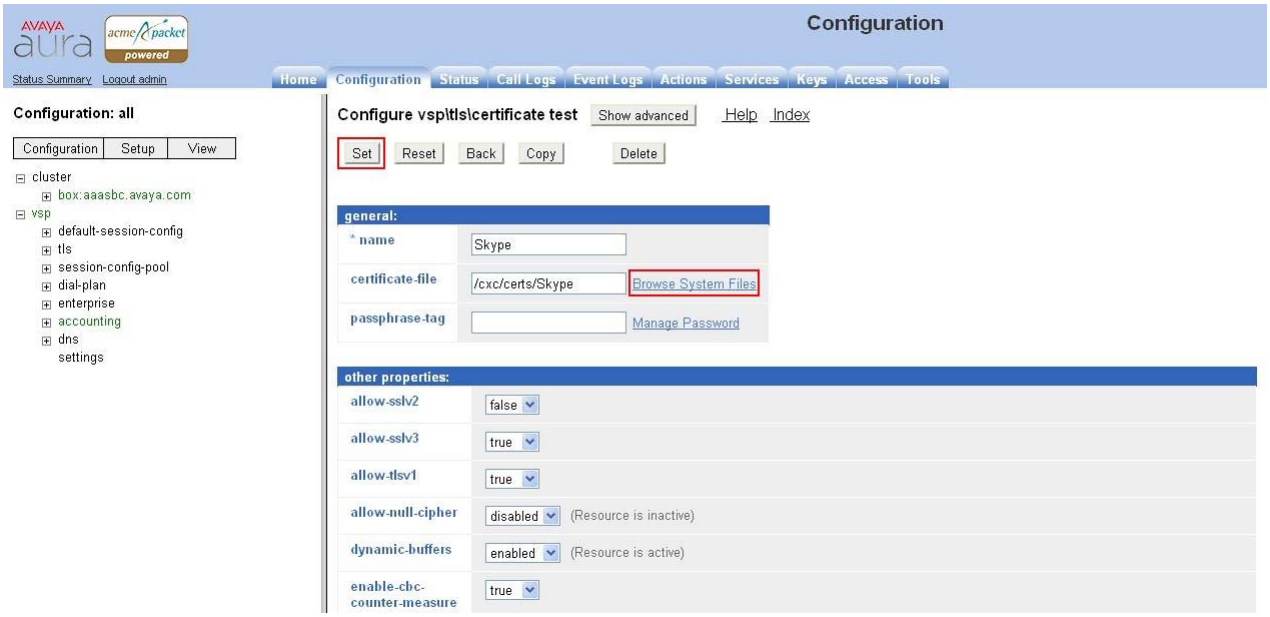
Select **tls** on the left pane. The **Configure vsp\tls** page is displayed. Select **Add certificate.**



In the next screen, enter a name and select **Create.**

©2011 Avaya Inc. All Rights Reserved.

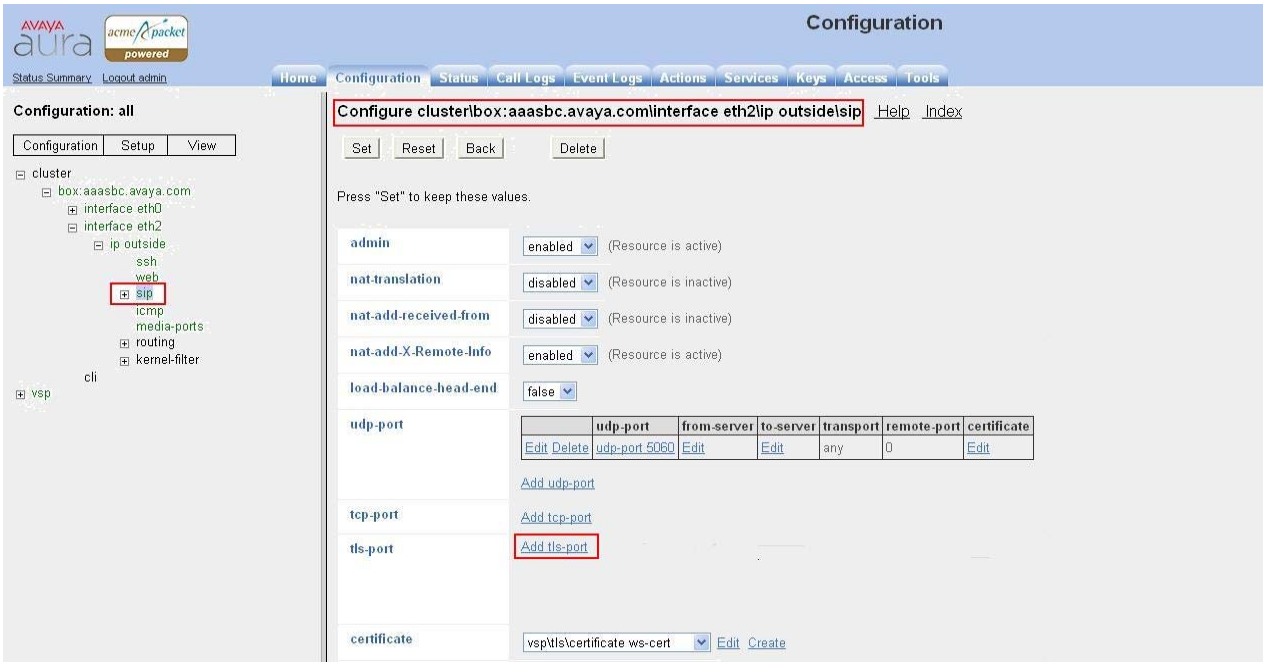
In the next screen select **Browse System Files** and select the Skype TLS certificate (not shown). Leave all other properties as default. Click **Set** to save.



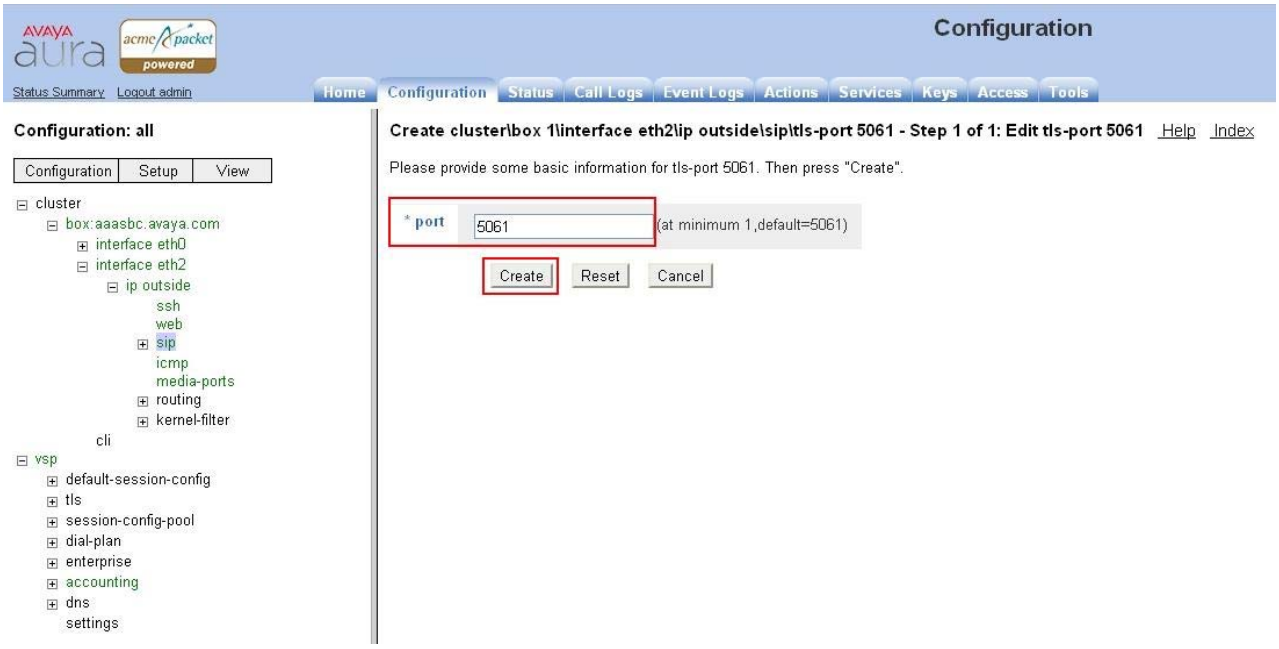
©2011 Avaya Inc. All Rights Reserved.

7.4. Administer TLS on the outside interface

Select **sip** on the left pane. The **Configure cluster\box:aaasbc.avaya.com\interface eth2\ip outside\sip** page is displayed. Select **Add-tls-port.**

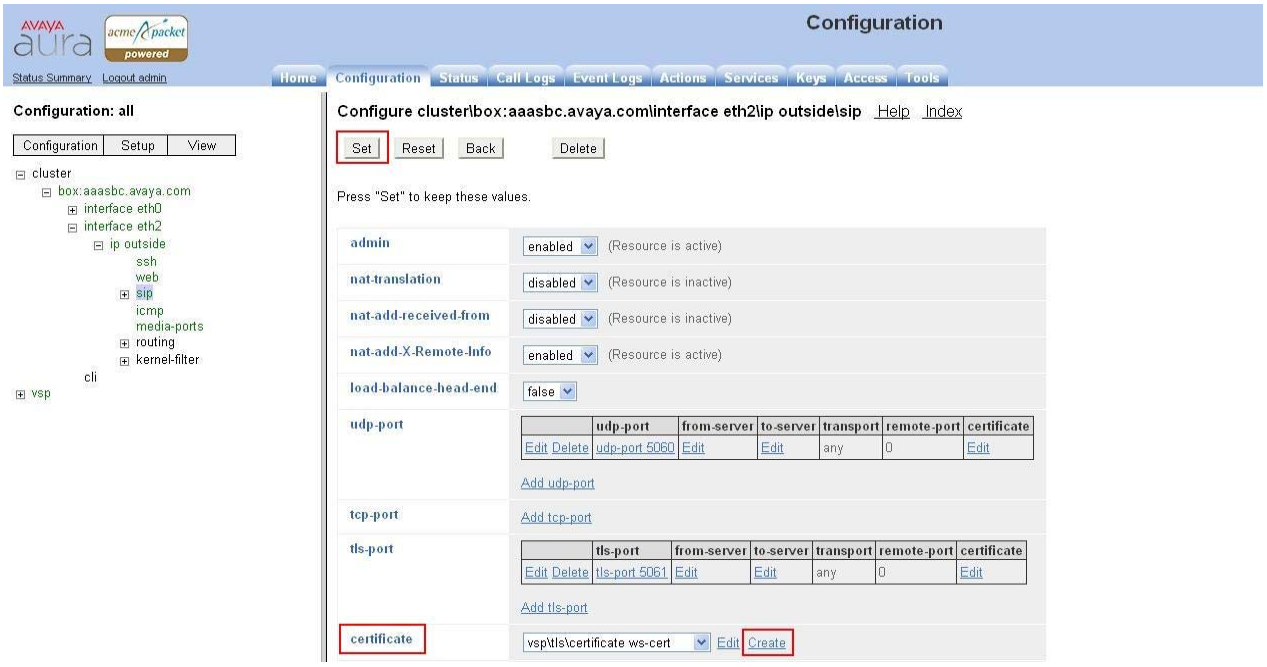


In the next screen, enter **5061** for the port number and select **Create**.

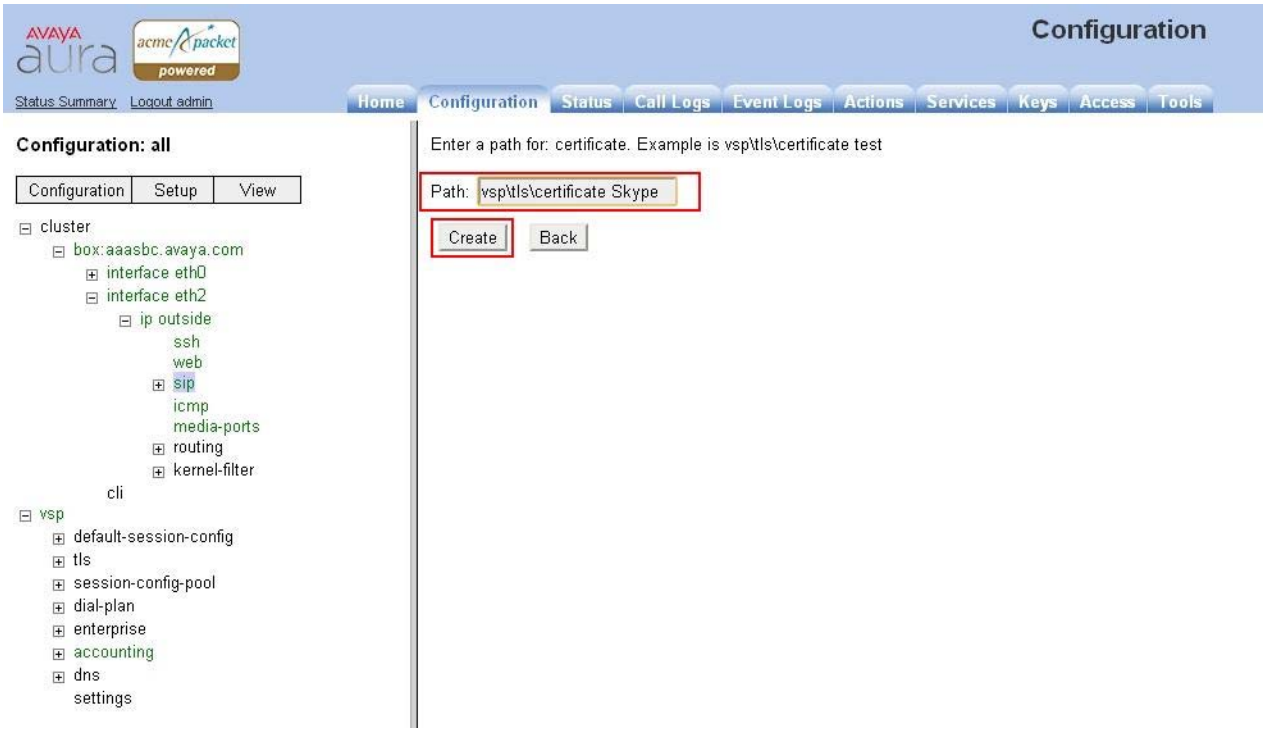


©2011 Avaya Inc. All Rights Reserved.

A TLS certificate now needs to be associated with the newly created TLS port. In the right-hand pane, select **Create** to create an association to the TLS certificate administered in **Section 7.3**.



In the next screen, enter the path to the TLS certificate administered in **Section 7.3** and select **Create**.

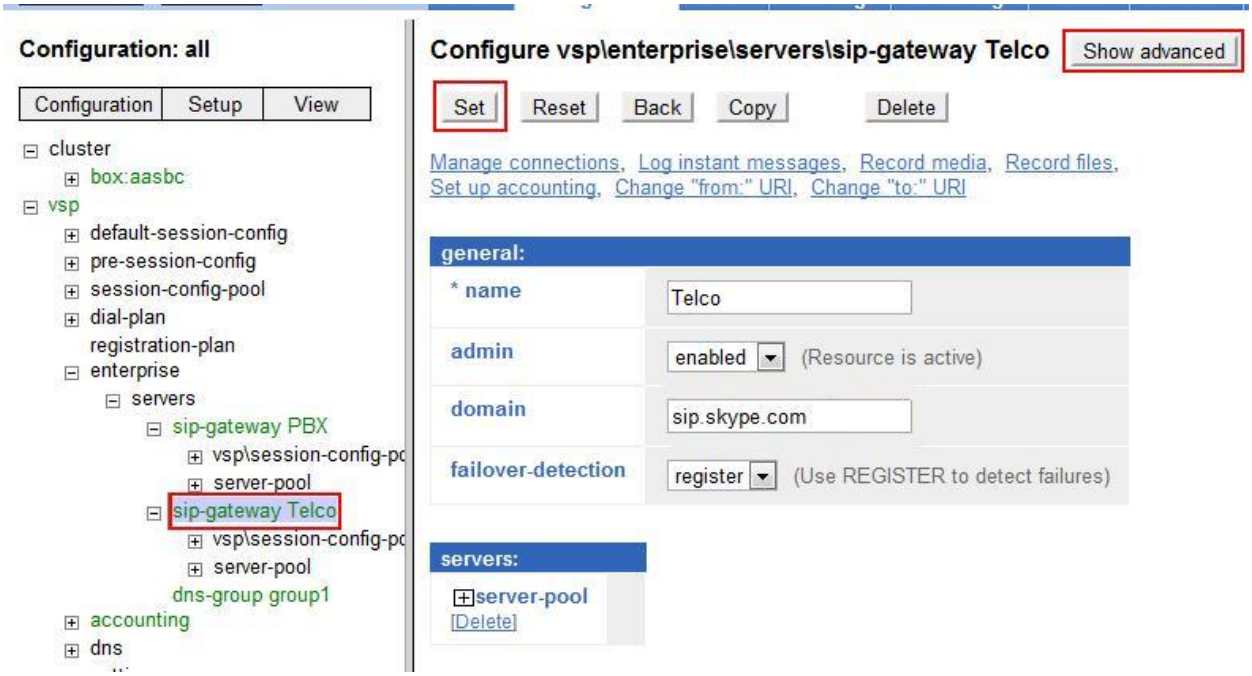


One will then be returned to the previous screen, select **Set** to save.

©2011 Avaya Inc. All Rights Reserved.

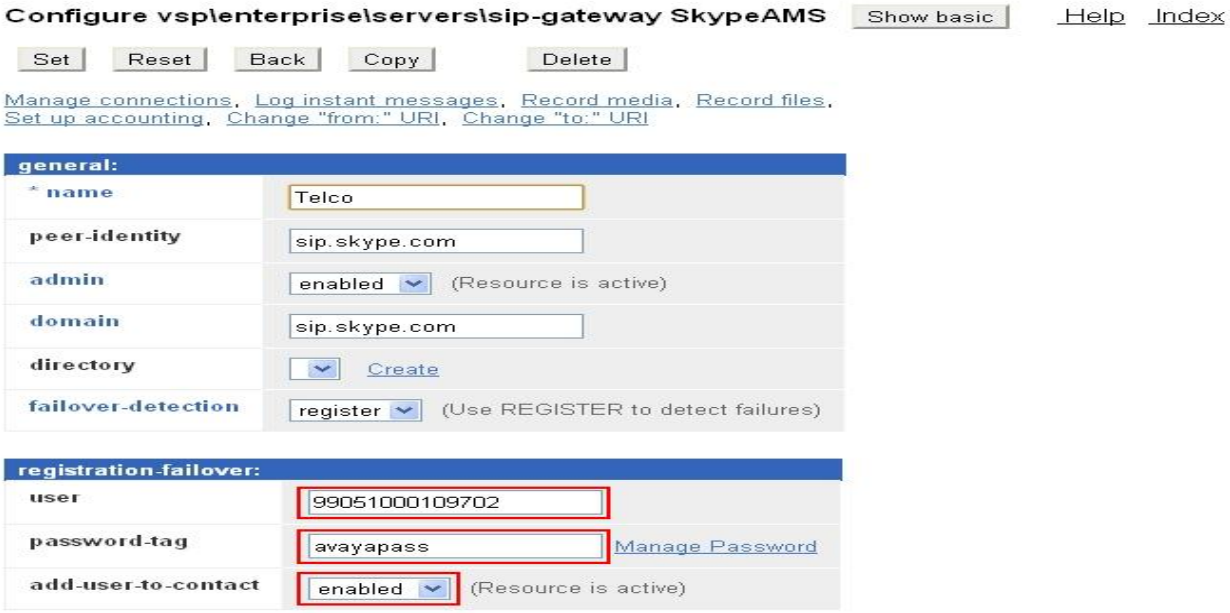
7.5. Administer Authentication

Select **sip-gateway Telco** on the left pane. The **Configure vsp\enterprise\servers\sip-gateway Telco** page is displayed. Click on the **Show advanced** button.



Enter the following details under **registration-failover**:

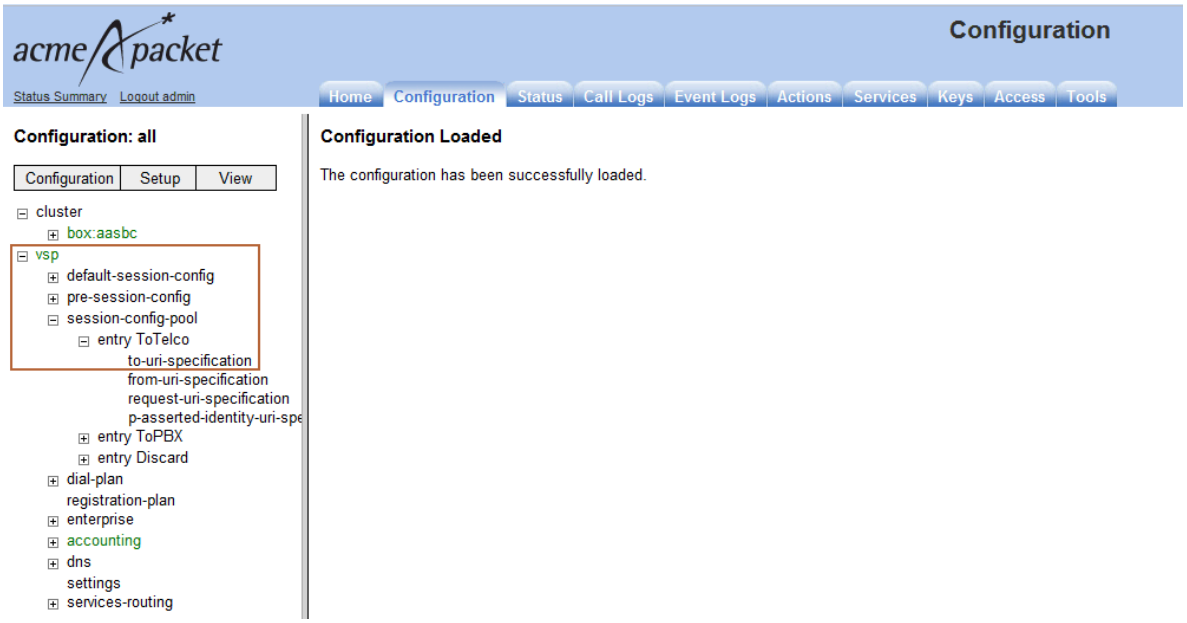
- **User** The SIP User number assigned to the avaya.com SIP profile upon creation in Skype Manager. The number will be seen in the Authentication Details section of the SIP user profile.
- **password-tag** i.e. **avayapass**
- **add-user-to-contact** **enabled**



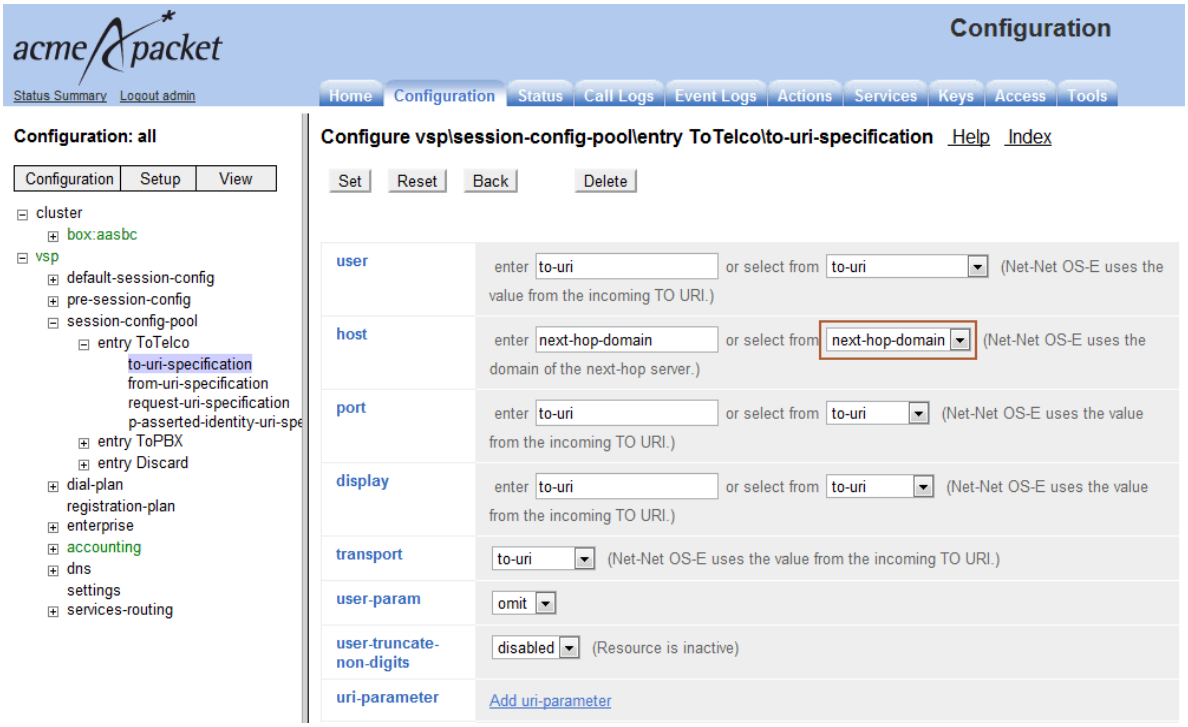
©2011 Avaya Inc. All Rights Reserved.

7.6. Administer Outbound SIP Header Manipulation Rules

The following steps translate the SIP domain names created in **Section 7.2** in the To, From, Request-URI and PAI headers and assign the Skype ID to the user part of the From header as it is required for outbound calls to work. The **Configuration** page is displayed. Expand **vsp → session-config-pool → entry ToTelco → to-uri-specification** on the left pane.

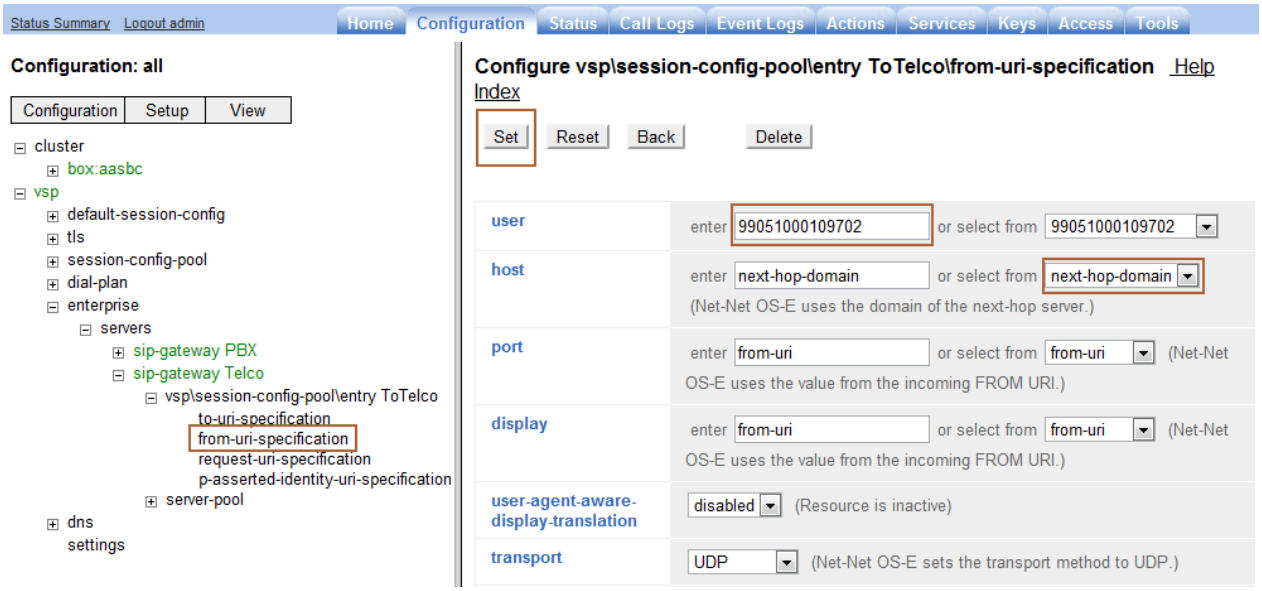


Under **host** select **next-hop-domain** from the drop-down list box then click **Set**.

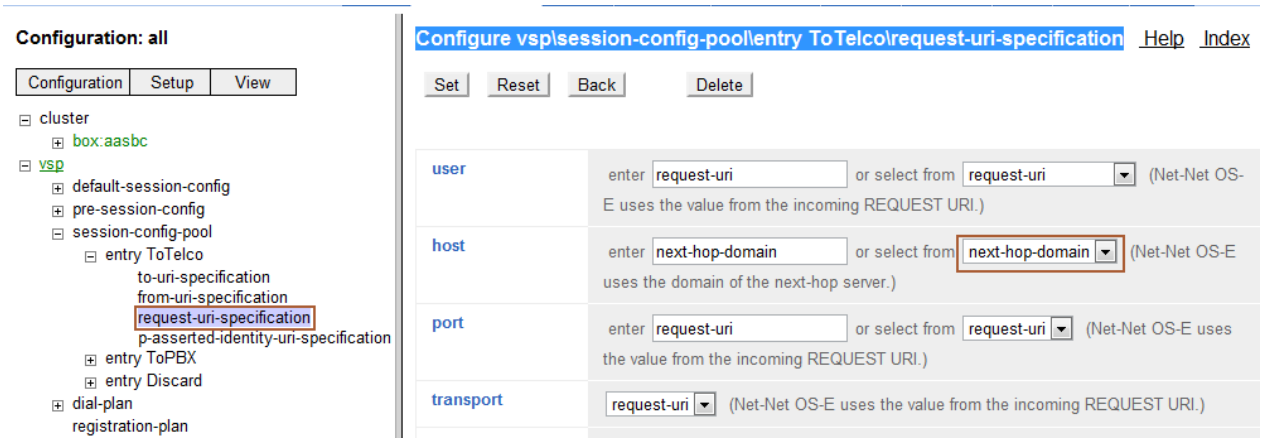


©2011 Avaya Inc. All Rights Reserved.

Select **from-uri-specification** from the left pane. The **Configure vsp\session-config-pool\entry ToTelco\from-uri-specification** page is displayed. Type the Skype Manager assigned **SIP User** in the **user** field. Under **host** select **next-hop-domain** from the drop-down list box then click **Set**.

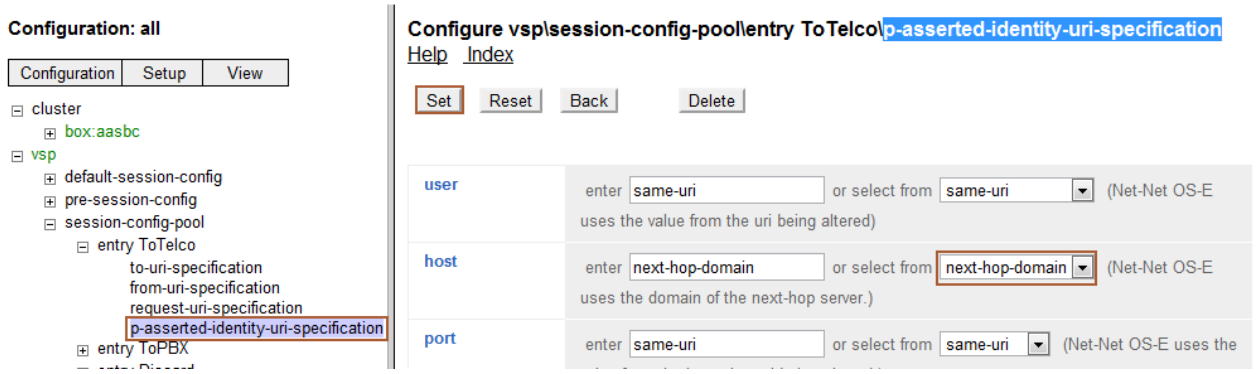


Select **request-uri-specification** from the left pane. The **Configure vsp\session-config-pool\entry ToTelco\request-uri-specification** page is displayed. Under **host** select **next-hop-domain** from the drop-down list box then click **Set**.



©2011 Avaya Inc. All Rights Reserved.

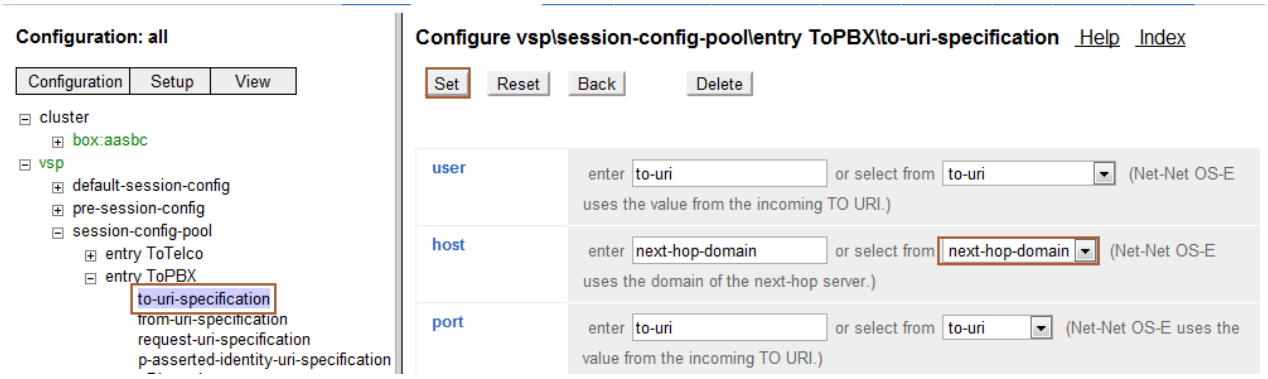
Select **p-asserted-identity-uri-specification** from the left pane. The **Configure vsp\session-config-pool\entry ToTelco\ p-asserted-identity-uri-specification** page is displayed. Under **host** select **next-hop-domain** from the drop-down list box then click **Set**.



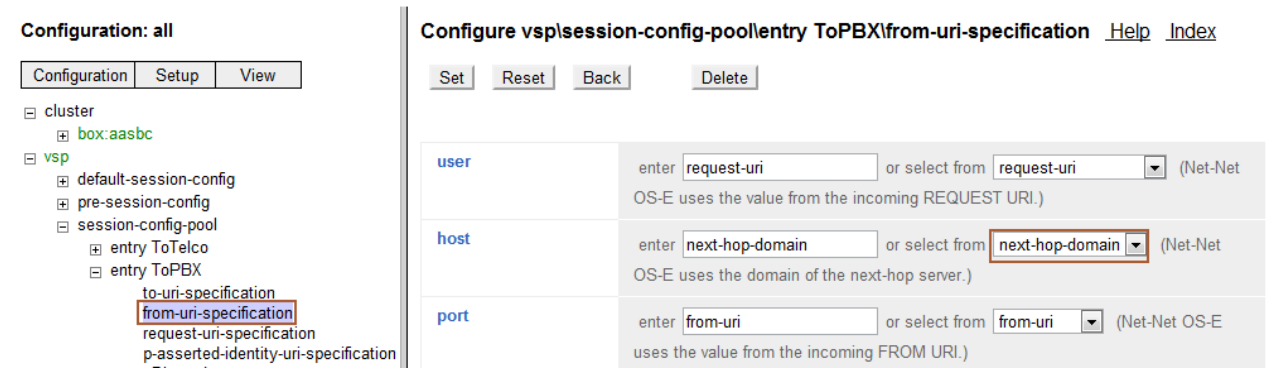
©2011 Avaya Inc. All Rights Reserved.

7.7. Administer Inbound SIP Header Manipulation Rules

The following steps translate the SIP domain names created in **Section 7.2** in the To, From, Request-URI and PAI headers from sip.skype.com to avaya.com. Expand **vsp → session-config-pool → entry ToPBX → to-uri-specification** on the left pane. The **Configure vsp\session-config-pool\entry ToPBX\to-uri-specification** page is displayed. Under **host** select **next-hop-domain** from the drop-down list box.

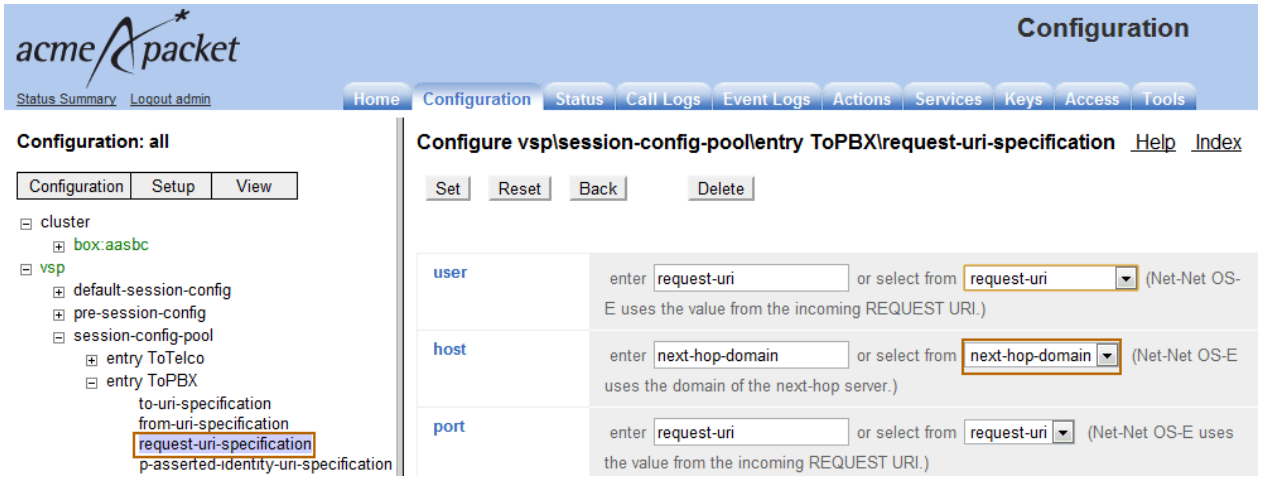


Select **from-uri-specification** from the left pane. The **Configure vsp\session-config-pool\entry ToPBX\from-uri-specification** page is displayed. Under **host** select **next-hop-domain** from the drop-down list box then click **Set**.

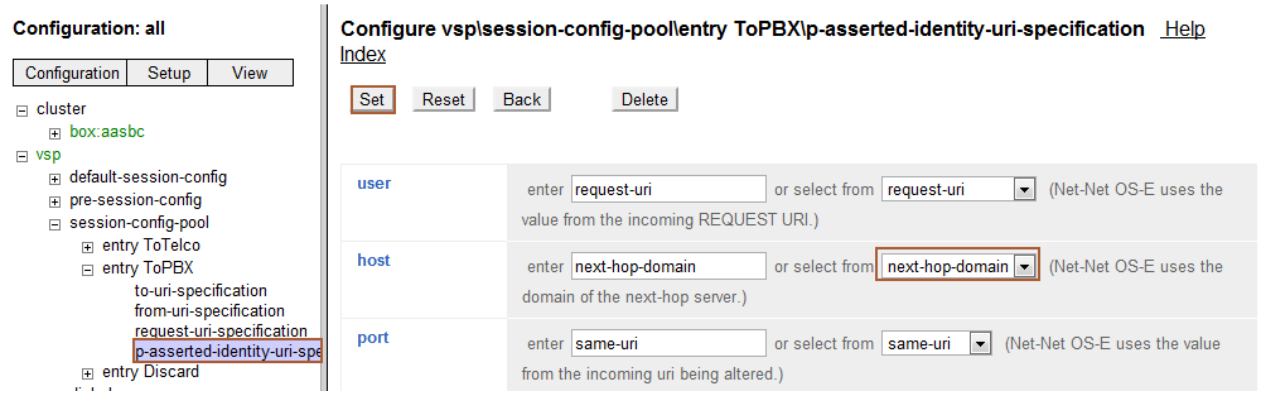


©2011 Avaya Inc. All Rights Reserved.

Select **request-uri-specification** from the left pane. The **Configure vsp\session-config-pool\entry ToPBX\request-uri-specification** page is displayed. Under **host** select **next-hop-domain** from the drop-down list box then click **Set**.



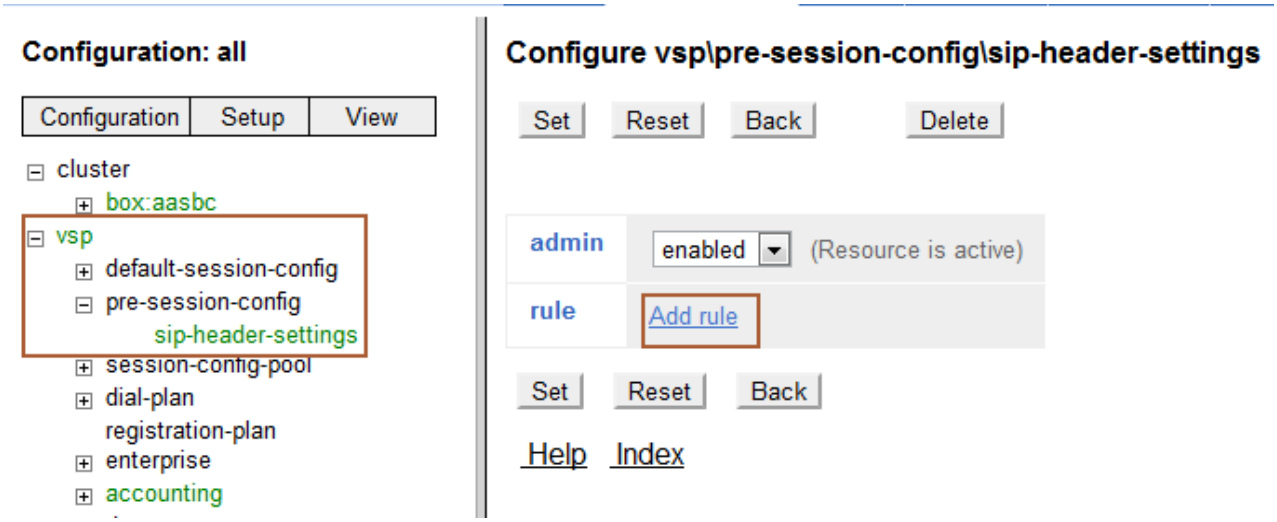
Select **p-asserted-identity-uri-specification** from the left pane. The **Configure vsp\session-config-pool\entry ToPBX\p-asserted-identity-uri-specification** page is displayed. Under **host** select **next-hop-domain** from the drop-down list box then click **Set**.



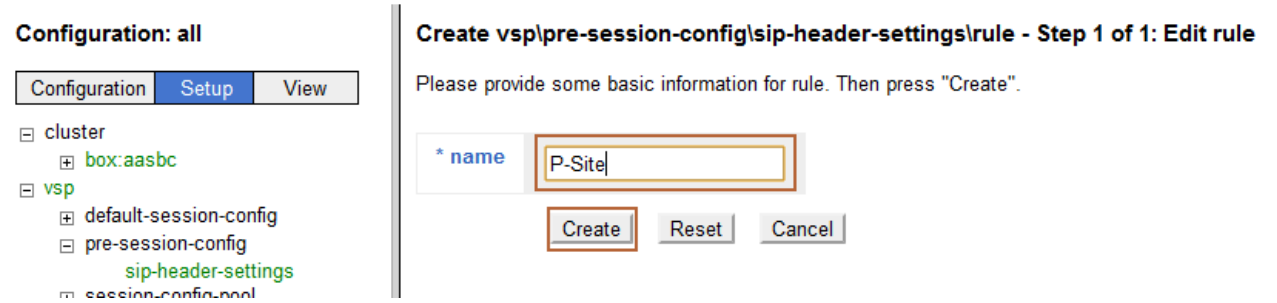
©2011 Avaya Inc. All Rights Reserved.

7.8. Administer SIP Header Rules for Topology Hiding

In the outgoing INVITE message to Skype Connect the Avaya Aura® Session Manager inserts the P-Site proprietary with the private IP address of Avaya Aura® System Manager thereby exposing the private IP addressing scheme to the public Internet. This section describes a SIP header manipulation rule which strips the P-Site header from the outgoing INVITE. Expand **vsp → pre-session-config → sip-header-settings**. The **Configure vsp\pre-session-config\sip-header-settings** page is displayed. Click **Add rule**.

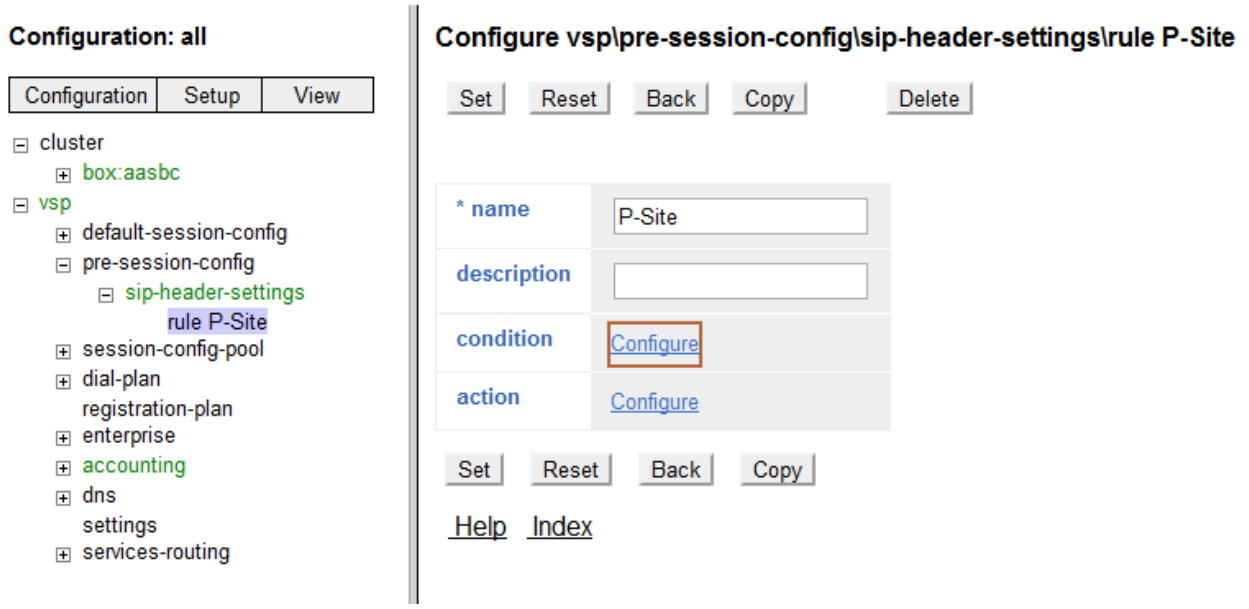


Type a descriptive name for the rule and click **Create**.

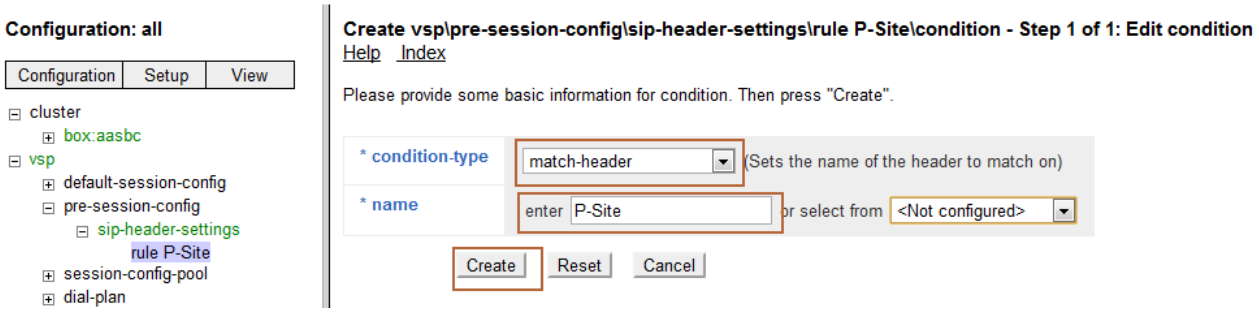


©2011 Avaya Inc. All Rights Reserved.

The **Configure vsp\pre-session-config\sip-header-settings\rule P-Site** page is displayed. Click **Configure**.

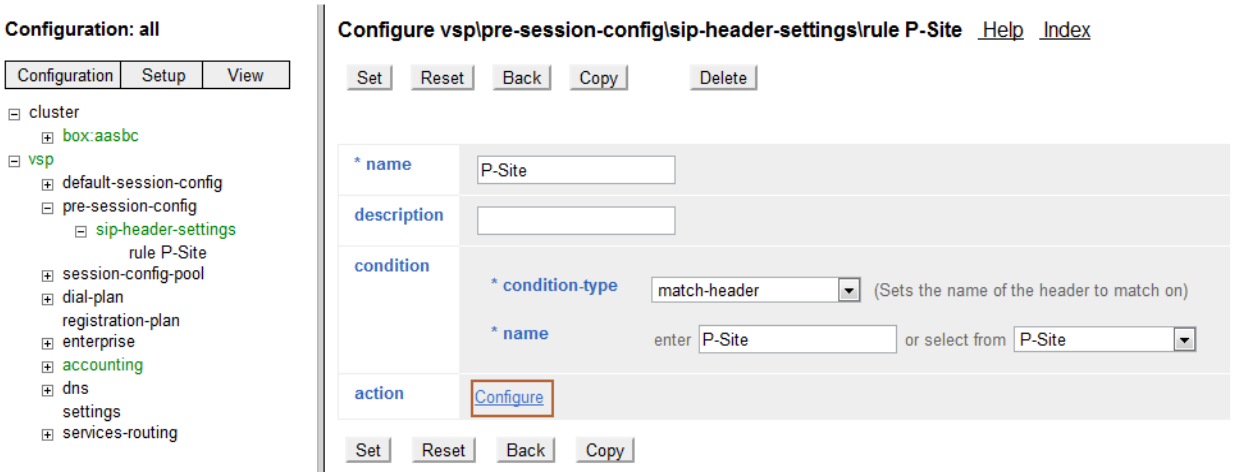


The **Create vsp\pre-session-config\sip-header-settings\rule P-Site\condition** page is displayed. Under **condition-type** select **match-header**. Under **name** type **P-Site** then click Create.

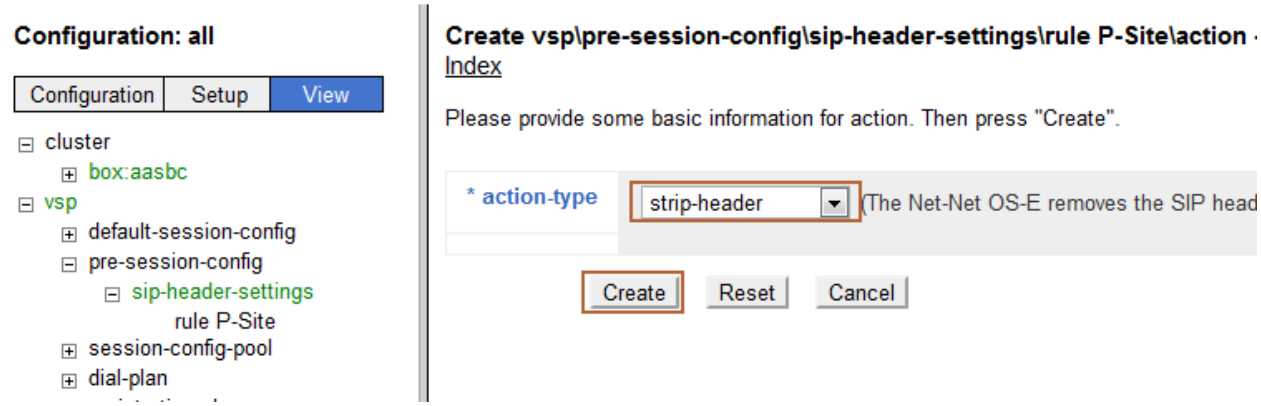


©2011 Avaya Inc. All Rights Reserved.

The **Configure vsp\pre-session-config\sip-header-settings\rule P-Site** page is displayed. Click **Configure**.

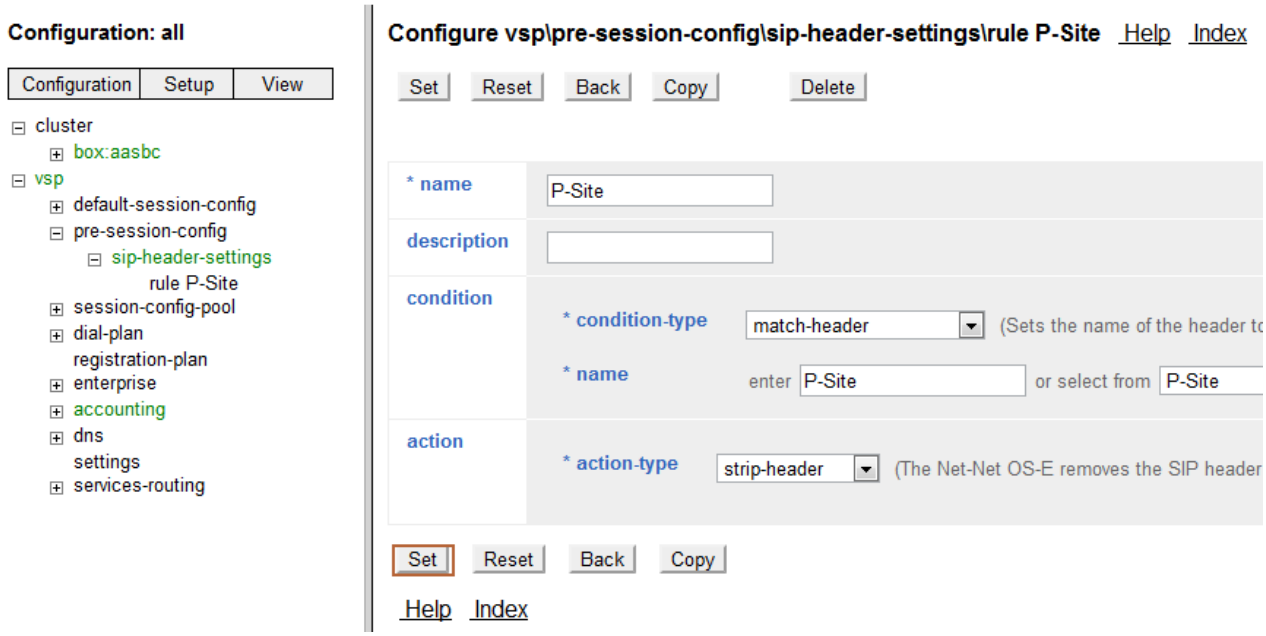


The **Create vsp\pre-session-config\sip-header-settings\rule P-Site\action** page is displayed. Under **action-type** select **strip-header** then click **Create**.



©2011 Avaya Inc. All Rights Reserved.

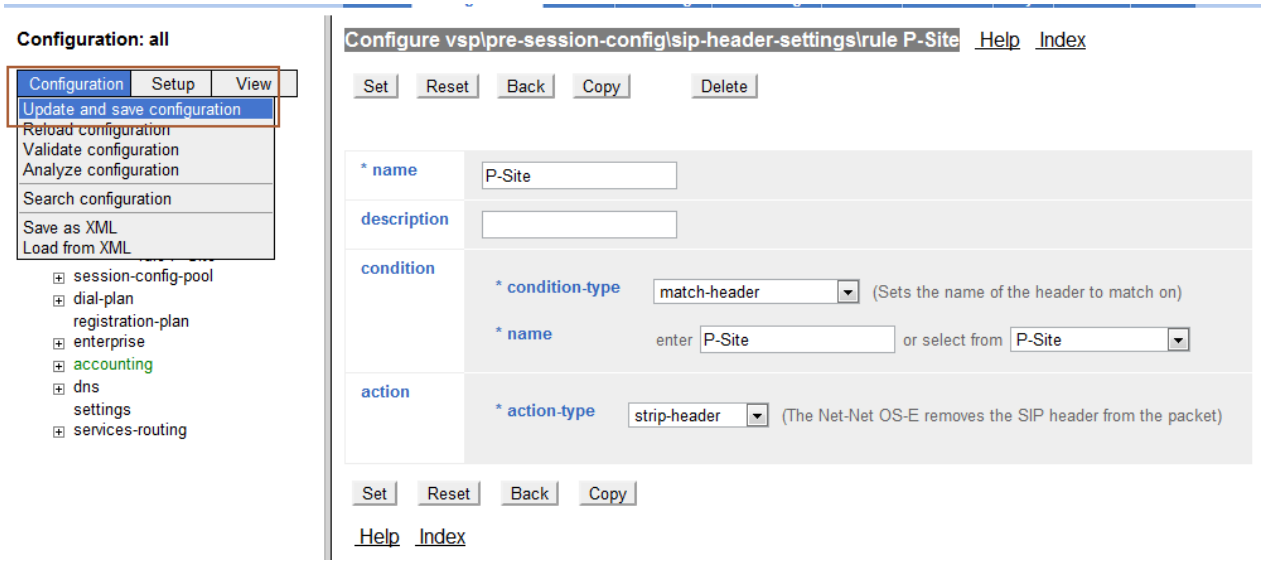
The **Configure vsp\pre-session-config\sip-header-settings\rule P-Site** page is displayed. Click **Set**.



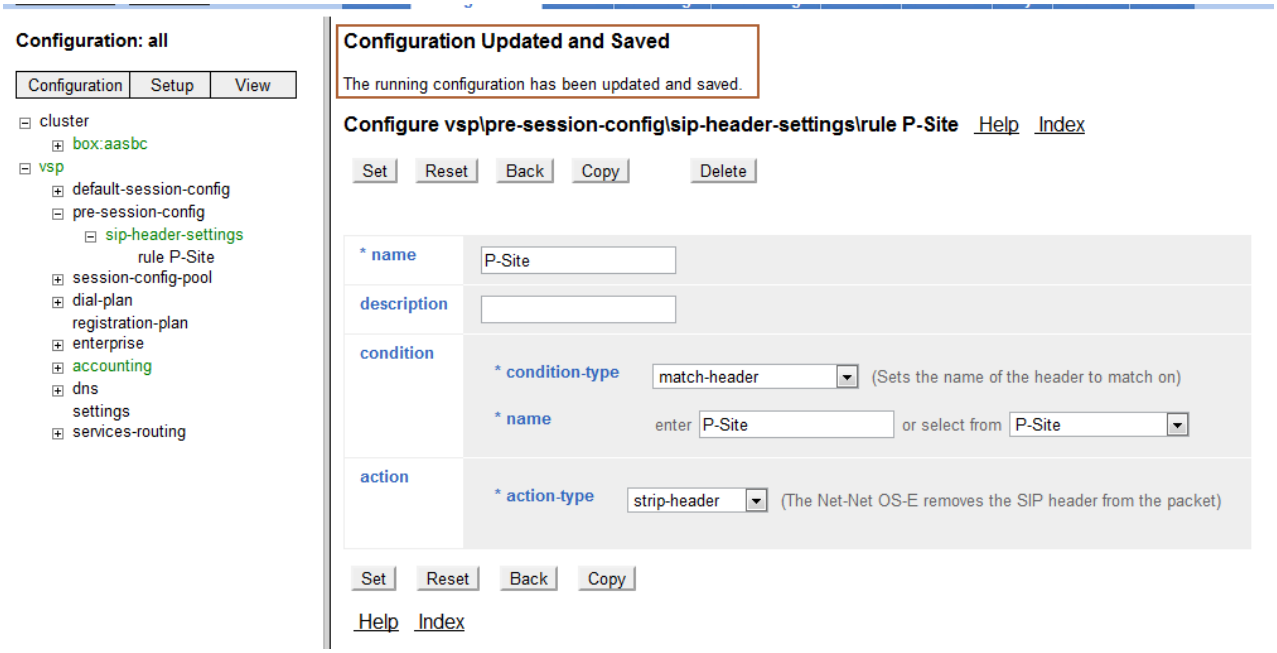
©2011 Avaya Inc. All Rights Reserved.

7.9. Save the Configuration

Click **Configuration** on the left pane then select **Update and save configuration**.



Once the configuration is written to disk the **Configuration Updated and Saved** message is displayed.



©2011 Avaya Inc. All Rights Reserved.

8. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya phones and Avaya Aura® Session Border Controller.
- A Beta version of the Skype Connect service, to which the simulated enterprise was connected.

The main test objectives were to verify the following features and functionality:

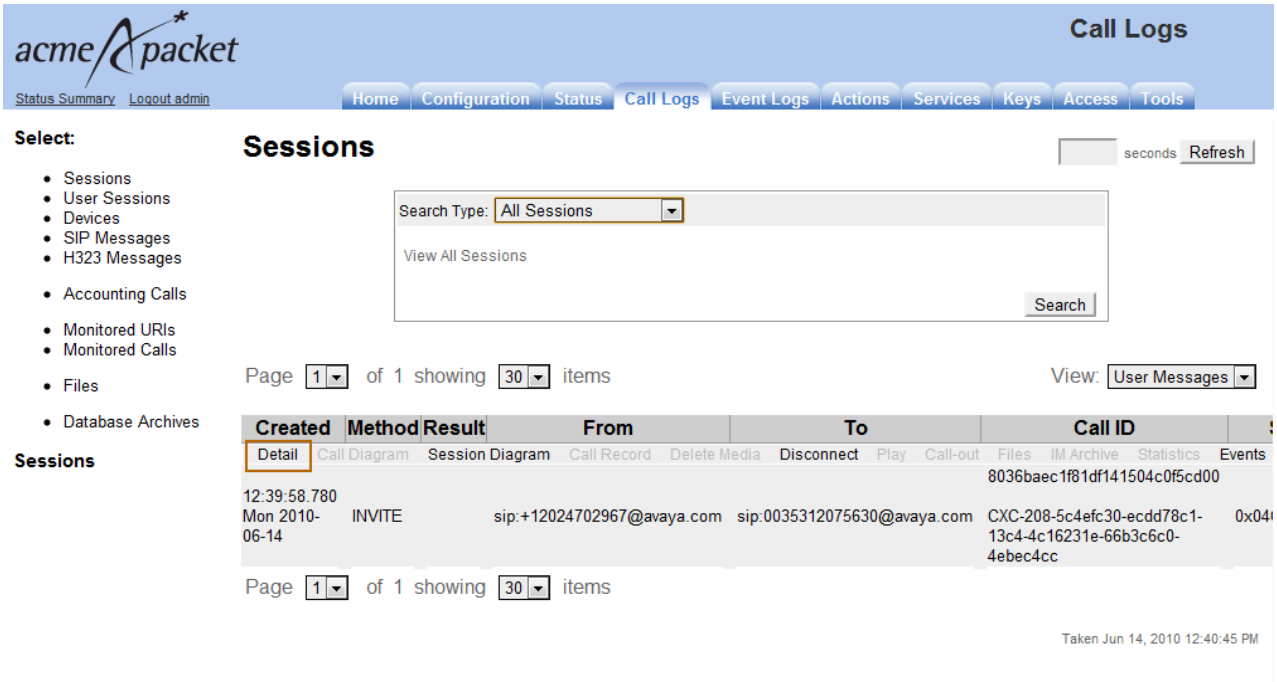
- Inbound and outbound PSTN and Skype P2P service calls from the simulated enterprise site via Skype Connect.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729 and G.711 codecs.
- DTMF tone transmission using RFC 2833.
- Long duration calls.

9. Verification Steps

The Session Border Controller stores the SIP signaling traces of each test call in the Call Log database. Log in to the Session Border Controller through the GUI and click on **Call Logs**.

©2011 Avaya Inc. All Rights Reserved.

The Sessions page is displayed. Calls can be filtered by Call ID and called/calling number. Click on **Detail** once a particular call is selected to display the SIP message trace (not shown).



9.1. Troubleshooting Tools

The Communication Manager **list trace station**, **list trace tac**, and **status trunk-group** commands are helpful diagnostic tools to verify correct operation and to troubleshoot problems. The logging and reporting functions within the Session Border Controller and the System Manager Common Console may be used to examine the details of SIP calls. In addition, if port monitoring is available, a SIP protocol analyzer such as Wireshark (a.k.a. Ethereal) can be used to capture SIP traces at the various interfaces. SIP traces can be instrumental in understanding SIP protocol issues resulting from configuration problems.

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager R6.1, Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Session Border Controller R6.0 can be configured to interoperate successfully with the Skype Connect service. This solution provides users of Avaya Aura® Communication Manager R6.0.1 the ability to support inbound and outbound calls and basic supplementary features over a public SIP trunk to Skype Connect. These Application Notes further demonstrated that the Avaya Aura® Session Border Controller could be utilized to remove P-Site header information on egress SIP messages to the Skype Connect service as well as provide required domain name conversion for inbound and outbound calls. These Application Notes also demonstrated that the Avaya Aura® Session Border Controller can interoperate with the Skype Connect service over TLS. The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation.

©2011 Avaya Inc. All Rights Reserved.

11. References

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

[1] *Avaya Aura® Session Manager Overview*, Doc # 03603323, Issue 1 Release 6.1

[2] *Administering Avaya Aura® Session Manager*, Doc # 03603324, Issue 1 Release 6.1

[3] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc # 03603325, Issue 1 Release 6.1

[4] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Issue 6.0

[5] *Avaya Aura™ Session Border Controller System Administration V6.0*, https://support.avaya.com/css/P8/documents/100111137

The Skype product documentation is available at http://www.skype.com/intl/en-us/business/ unless otherwise noted.

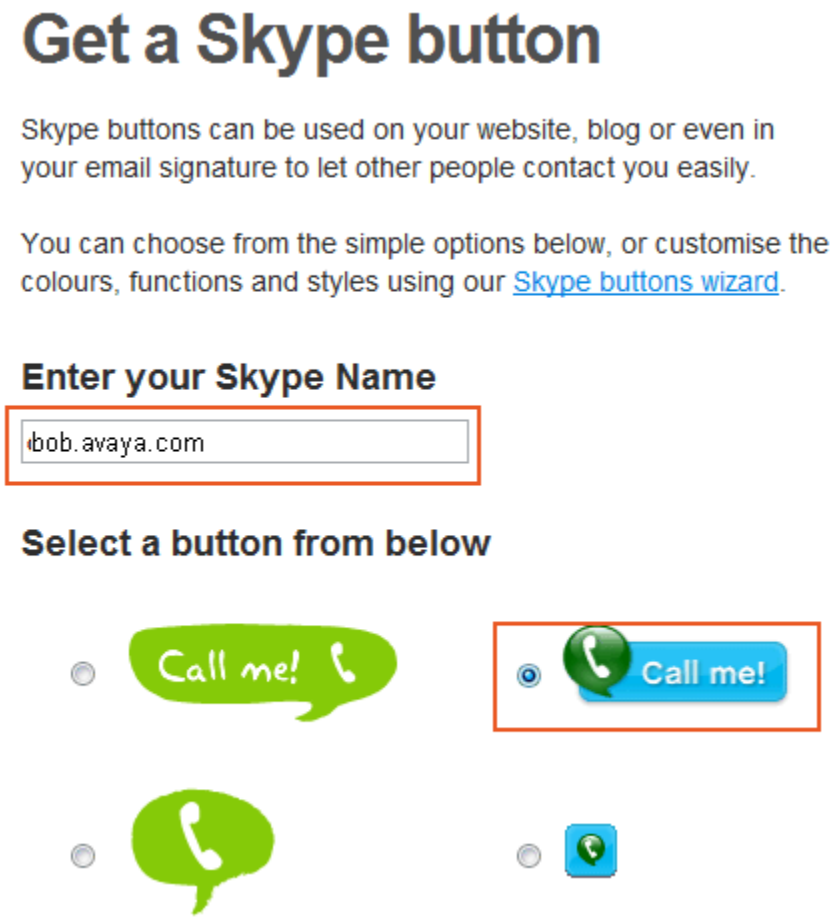
[6] *Skype Connect product datasheet*, 2011. http://www.skype.com/go/skype.connect.product.datasheet

©2011 Avaya Inc. All Rights Reserved.

Appendix A – Skype Button

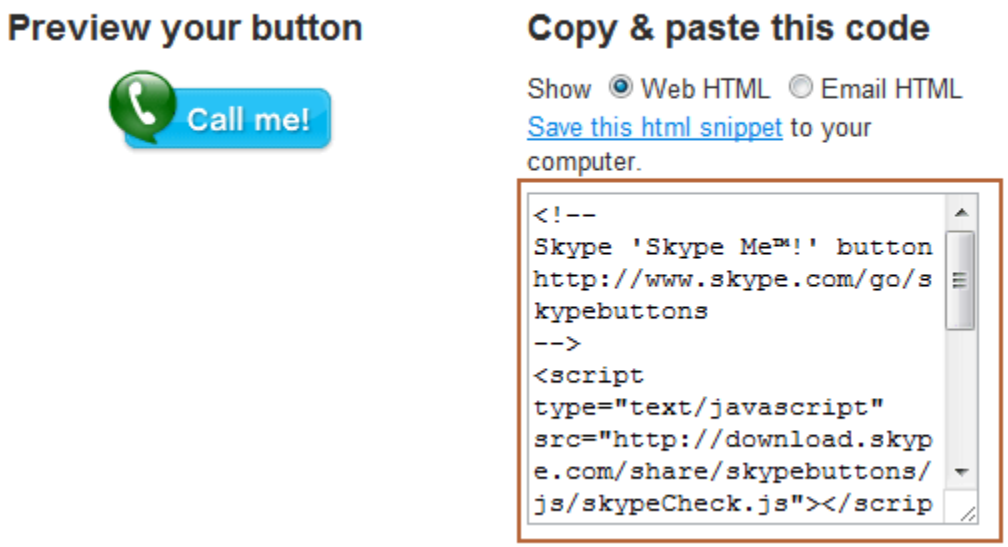
In **Section 6.6** the provisioning of a Business User is discussed. The Business User is associated with a unique Skype Name which can be dialed from the Skype Client application or can be used in click-to-call applications. This section describes the steps for embedding a Skype Button in HTML code to allow Internet users to dial the Skype Name of a Business User.

Go to http://www.skype.com/intl/en-us/tell-a-friend/get-a-skype-button/ . The **Get a Skype Button** page is displayed. Enter the **Skype Name** from **Section 6.6** and select a Skype Button.



©2011 Avaya Inc. All Rights Reserved.

Scroll down to the bottom of the page. Copying and pasting the HTML snippet from the text box into an existing webpage will allow Internet users to initiate a call to Business Users.



©2011 Avaya Inc. All Rights Reserved.

Appendix B – Avaya Aura® SBC Configuration File

```
#
#  Copyright (c) 2004-2011  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 09:58:57 Mon 2011-05-23
#
config cluster
 config box 1
  set hostname aaasbc.avaya.com
  set timezone Etc/GMT
  set name aaasbc.avaya.com
  set identifier 00:ca:fe:22:12:43
  config interface eth0
   config ip inside
    set ip-address static 20.0.0.36/25
    config ssh
    return
    config snmp
     set trap-target 20.0.0.40 162
     set trap-filter generic
     set trap-filter dos
     set trap-filter sip
     set trap-filter system
    return
    config web
    return
    config web-service
     set protocol https 8443
     set authentication certificate "vsp\tls\certificate ws-cert"
    return
    config sip
     set tcp-port 5060 "" "" any 0
    return
    config icmp
    return
    config media-ports
    return
    config routing
     config route Default
      set gateway 20.0.0.1
     return
     config route Static0
      set destination network 192.11.13.4/30
```


©2011 Avaya Inc. All Rights Reserved.

```
   set gateway 20.0.0.39
  return
  config route to86
   set destination network 86.0.0.0/24
   set gateway 20.0.0.1
  return
  config route Static2
   set admin disabled
  return
  config route Static3
   set admin disabled
  return
  config route Static4
   set admin disabled
  return
  config route Static5
   set admin disabled
  return
  config route Static6
   set admin disabled
  return
  config route Static7
   set admin disabled
  return
  config route Static1
   set admin disabled
  return
 return
return
config ip mgmt
 config routing
  config route Default
  return
  config route Static0
  return
  config route Static1
  return
  config route Static2
  return
  config route Static3
  return
  config route Static4
  return
  config route Static5
  return
  config route Static6
```


©2011 Avaya Inc. All Rights Reserved.

```
   return
   config route Static7
   return
  return
 return
return
config interface eth2
 config ip outside
  set ip-address static 86.47.122.10/25
  config ssh
   set authentication password
   set account root
  return
  config web
  return
  config sip
   set udp-port 5060 "" "" any 0
   set tls-port 5061 "" "" any 0
   set certificate vsp\tls\certificate Skype
  return
  config icmp
  return
  config media-ports
  return
  config routing
   config route Default
    set admin disabled
   return
   config route 8.8.8.8
    set admin disabled
    set destination host 8.8.8.8
    set gateway 86.47.122.7
   return
   config route "APKT Mouta"
    set admin disabled
    set destination host 81.134.16.151
    set gateway 86.47.122.7
   return
   config route SkypeAMS
    set destination host 80.252.85.76
    set gateway 86.47.122.7
   return
  return
  config kernel-filter
   config allow-rule allow-sip-udp-from-peer-1
    set destination-port 5060
```


©2011 Avaya Inc. All Rights Reserved.

```
      set source-address/mask 86.47.122.0/24
      set protocol udp
     return
     config deny-rule deny-all-sip
      set destination-port 5060
     return
    return
   return
  return
  config cli
   set prompt aaasbc.avaya.com
  return
 return
return

config services
 config event-log
  config file access
   set filter access info
   set count 3
  return
  config file system
   set filter system info
   set count 3
  return
  config file errorlog
   set filter all error
   set count 3
  return
  config file db
   set filter db debug
   set filter dosDatabase info
   set count 3
  return
  config file management
   set filter management info
   set count 3
  return
  config file peer
   set filter sipSvr info
   set count 3
  return
  config file dos
   set filter dos alert
   set filter dosSip alert
   set filter dosTransport alert
```


©2011 Avaya Inc. All Rights Reserved.

```
   set filter dosUrl alert
   set count 3
  return
  config file krnlsys
   set filter krnlsys debug
   set count 3
  return
 return
return

config master-services
 config cluster-master
  set group 2
 return
 config accounting
  set group 6
 return
 config authentication
 return
 config database
  set group 6
  set media enabled
 return
 config registration
 return
 config sampling
  config database
   config status
    config interface-details
    return
    config interface-throughput
    return
    config system-heap
    return
    config available-memory
    return
    config trunk-groups
    return
    config cpu-usage
    return
    config sip-stack
    return
    config call-admission-control
    return
    config dos-transport-counters
    return
```


©2011 Avaya Inc. All Rights Reserved.

```
    config dos-sip-counters
    return
    config dos-url-counters
    return
   return
  return
 return
return

config vsp
 set admin enabled
 config default-session-config
  config media
   set anchor enabled
   set rtp-stats enabled
  return
  config sip-directive
   set directive allow
  return
  config log-alert
   set apply-to-methods-for-filtered-logs INVITE+REGISTER
  return
  config third-party-call-control
   set admin enabled
   set handle-refer-locally disabled
  return
 return
 config tls
  config default-ca
   set ca-file /cxc/certs/sipca.pem
  return
  config certificate ws-cert
   set certificate-file /cxc/certs/ws.cert
  return
  config certificate Skype
   set certificate-file /cxc/certs/Skype
  return
  config certificate aasbc.p12
   set certificate-file /cxc/certs/aasbc.p12
   set passphrase-tag aasbc-cert-tag
  return
 return
 config session-config-pool
  config entry toGamma
   config to-uri-specification
    set host 83.245.6.117
```


©2011 Avaya Inc. All Rights Reserved.

```
 return
 config from-uri-specification
  set user 0035391733202
  set host local-ip
  set display 0035391733202
 return
 config request-uri-specification
  set host 83.245.6.117
 return
 config p-asserted-identity-uri-specification
  set user 0035391733202
  set host local-ip
  set display 0035391733202
  set create true
  set use-original-from-header true
 return
 config header-settings
  set pAssert-mode enabled
  config reg-ex-header 0
   set destination P-Asserted-Identity
   set create From .* <sip:0035391733202@83.245.6.117>
  return
 return
return
config entry SMr61
 config to-uri-specification
  set host next-hop-domain
  set transport TCP
 return
 config from-uri-specification
  set host next-hop-domain
  set transport TCP
 return
 config request-uri-specification
  set host next-hop-domain
  set port next-hop
  set transport TCP
 return
 config sip-directive
  set directive allow
 return
 config accounting
  set target database "vsp\accounting\database\group localdb"
 return
 config log-alert
 return
```


©2011 Avaya Inc. All Rights Reserved.

```
return
config entry Discard
 config sip-directive
 return
return
config entry toSkypeAMS
 config to-uri-specification
  set host sip.skype.com
  set transport omit
 return
 config from-uri-specification
  set user 99051000109702
  set host sip.skype.com
  set display omit
  set transport omit
 return
 config request-uri-specification
  set host sip.skype.com
  set transport omit
 return
 config p-asserted-identity-uri-specification
  set host sip.skype.com
  set transport omit
 return
 config contact-uri-settings-out-leg
  set add-maddr disabled
 return
 config media
  set anchor enabled
  set inactivity-timeout enabled "0 days 01:00:00"
  set rtp-stats enabled
 return
 config in-encryption
  set mode offer
  set require-tls true
 return
 config out-encryption
  set mode offer
  set require-tls true
 return
 config sip-directive
  set directive allow
 return
 config authentication
  set handle-challenge-locally enabled
 return
```


©2011 Avaya Inc. All Rights Reserved.

```
 config log-alert
  set apply-to-methods-for-filtered-logs INVITE+REGISTER
 return
return
config entry FromSkypeAMS
 config in-encryption
  set mode offer
  set require-tls true
 return
 config out-encryption
  set require-tls true
 return
 config sip-directive
  set directive allow
 return
 config authentication
  set handle-challenge-locally enabled
 return
 config log-alert
 return
return
return
config dial-plan
 config route Default
  set admin disabled
  set priority 500
  set location-match-preferred exclusive
  set session-config vsp\session-config-pool\entry Discard
 return
 config route toGamma00353
  set admin disabled
  set peer server "vsp\enterprise\servers\sip-gateway Gamma"
  set session-config vsp\session-config-pool\entry toGamma
  set request-uri-match phone-prefix 00353 5
 return
 config route toSkypeAMS
  set peer server "vsp\enterprise\servers\sip-gateway SkypeAMS"
  set request-uri-match phone-prefix 00 5
 return
 config route toMX
  set admin disabled
  set peer server "vsp\enterprise\servers\sip-gateway MX"
  set request-uri-match phone-prefix 01306 5
 return
 config route fromSkypetoSM
  config condition-list
```


©2011 Avaya Inc. All Rights Reserved.

```
   set operation OR
   set request-uri-condition user match 99051000109702
   set request-uri-condition user match 12024703313
  return
  set peer server "vsp\enterprise\servers\sip-gateway SMr61"
  set session-config vsp\session-config-pool\entry SMr61
  set request-uri-match condition-list
 return
return
config enterprise
 config servers
  config sip-gateway SMr61
   set domain avaya.com
   set failover-detection ping
   set outbound-session-config-pool-entry vsp\session-config-pool\entry SMr61
   config server-pool
    config server PBX1
     set host 20.0.0.20
     set transport TCP
    return
   return
  return
  config sip-gateway Gamma
   set failover-detection ping
   set outbound-session-config-pool-entry vsp\session-config-pool\entry toGamma
   config server-pool
    config server Gamma
     set host 83.245.6.117
    return
   return
  return
  config sip-gateway SkypeAMS
   set peer-identity sip.skype.com
   set domain sip.skype.com
   set failover-detection register
   set user 99051000109702
   set password-tag avayapass
   set add-user-to-contact enabled
   set inbound-session-config-pool-entry vsp\session-config-pool\entry FromSkypeAMS
   set outbound-session-config-pool-entry vsp\session-config-pool\entry toSkypeAMS
   config server-pool
    config server SkypeAMS
     set host sip.skype.com
     set transport TLS "vsp\tls\certificate Skype"
     set port 5061
    return
```


©2011 Avaya Inc. All Rights Reserved.

```
    return
   return
   config sip-gateway MX
    set failover-detection ping
    config server-pool
     config server MX
      set host 20.0.0.10
      set transport TCP
     return
    return
   return
  return
 return
 config accounting
  config database
   config group localdb
    config server localdb
     set type local
     set username postgres
     set password-tag dbpassword
    return
   return
  return
 return
 config dns
  config resolver
   config server 193.88.6.227
    set type dns-only
    set name SkypeTestDNS
   return
  return
  config host sip.skype.com
   set address 80.252.85.76
  return
  config service sip.skype.com sip any
   set rule 80.252.85.76 5061 0 0
  return
 return
 config settings
  set read-header-max 8191
 return
return

config external-services
return
```


©2011 Avaya Inc. All Rights Reserved.

```
config preferences
 config gui-preferences
  set enum-strings RequestURIStringSource 83.245.6.117
  set enum-strings URIStringSource 0035391733202
  set enum-strings GeneralURIStringSource 0035391733202
  set enum-strings DisplayURIStringSource 0035391733202
  set enum-strings SIPSourceHeader P-Asserted-Identity
  set enum-strings RequestURIStringSource sip.skype.com
  set enum-strings URIStringSource 99051000109702
  set enum-strings GeneralURIStringSource sip.skype.com
 return
return
config access
 config permissions superuser
  set cli advanced
 return
 config permissions read-only
  set config view
  set actions disabled
 return
 config users
  config user admin
   set password 0x00450df4f8c0700d7cfc8fbc2a173fe7f6b2d630e32e1daed35ba005a2
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x00eab23aba77bb7c2b3cbcdc78bb39489297c66b9a6e61a262a76625e6
   set permissions access\permissions read-only
  return
  config user init
   set password 0x00bc74e4e043fb499485f78f14a6a26cc816ad64871b2e5ed8367ec4fa
   set permissions access\permissions superuser
  return
  config user craft
   set password 0x00ad62ac693367bea4327d1d928775b6a634b28b0f5afce57a4a11be66
   set permissions access\permissions superuser
  return
  config user dadmin
   set password 0x00be7791ef88476292ea9de8c5d6c6084a5dbaec4eacef5284b04f4c90
   set permissions access\permissions read-only
  return
 return
return
config features
return
```


©2011 Avaya Inc. All Rights Reserved.

©2011 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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