Avaya Solution & Interoperability Test Lab

Application Notes for Citrix Communication Gateway with Avaya SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the redirection feature on Citrix Communication Gateway. Citrix Communication Gateway enables emergency phone redirection from a user's work phone to an emergency number defined by the employee in the event of a workforce disruption scenario. Citrix Communication Gateway also provides click to call capability via a standard SIP trunk. When users select a telephone number from within an application, or the Citrix Directory service, the Citrix Communication Gateway places a call to the user. When the user answers, the Citrix Communication Gateway places a second call to the desired destination.

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

1. Introduction

These Application Notes describe the procedures for configuring the redirection feature on Citrix Communication Gateway. Citrix Communication Gateway enables emergency phone redirection from a user's work phone to an emergency number defined by the employee in the event of a workforce disruption scenario. Citrix Communication Gateway also provides click to call capability via a standard SIP trunk. When users select a telephone number from within an application, or the Citrix Directory service, the Citrix Communication Gateway places a call to the user. When the user answers, the Citrix Communication Gateway places a second call to the desired destination.

Figure 1 illustrates a sample configuration consisting of Avaya S8720 Servers, an Avaya G650 Media Gateway, and Citrix Communication Gateway. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included in the test to provide an inter-switch scenario. For completeness, Avaya 4600 Series H.323 IP Telephones, Avaya 9600 Series H.323 IP Telephones, and Avaya 6400 Series Digital Telephones, are included.

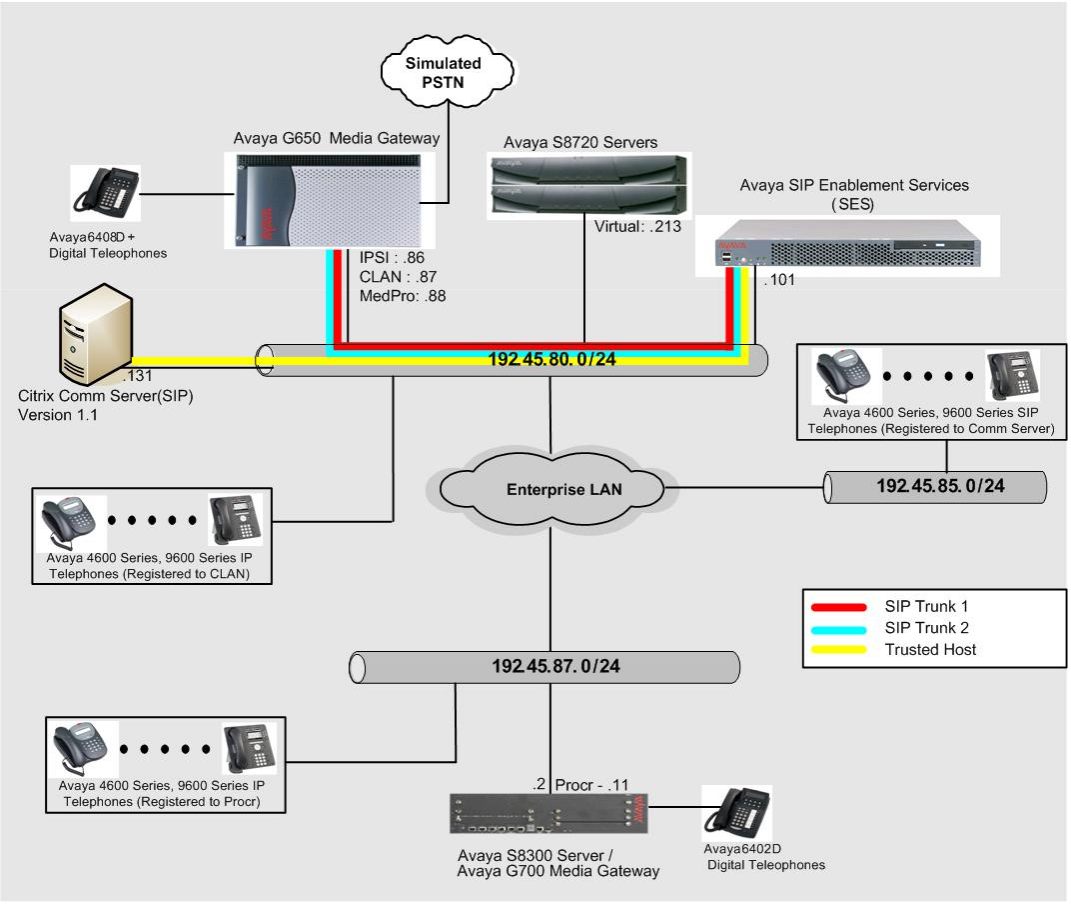


Figure 1: Avaya DevConnect Compliance Test Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8700 Servers	Avaya Communication Manager 5.0 (R015x.00.0.825.4)
Avaya G650 Media Gateway	-
TN2312BP IP Server Interface TN799DP CLAN Interface TN2302AP IP Media Processor	HW11 FW030 HW1 FW 17 HW20 FW108
Avaya S8300 Server with Avaya G700 Media Gateway	Avaya Communication Manager 5.0 (R015x.00.0.825.4)
Avaya SIP Enablement Services	R015x.00.0.825.4
Avaya 4600 Series IP Telephones 4620SW (H.323) 4625SW (H.323)	 2.83 2.83
Avaya 9600 Series IP Telephone 9630 (H.323) 9650 (H.323)	 1.5 1.5
Avaya 6400 Series Digital Telephones	-
Citrix Communication Gateway on Linux Fedora Version 4.0	1.1

3. Configure Avaya Communication Manager

This section provides the procedures for configuring an IP network region, IP node name, trunk groups, signaling groups, stations, Automatic Alternate Routing (AAR), and coverage path on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

3.1. Configure IP Network Region

This section describes the steps for administering an IP network region in Avaya Communication Manager for communication between Avaya Communication Manager and Avaya SES. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- Authoritative Domain – Set to **testroom.com**. This should match the SIP Domain value on Avaya SES, in **Section 4.1**.
- Intra-region IP-IP Direct Audio – Set to **no** to deny direct IP-to-IP audio connectivity between endpoints registered to Avaya Communication Manager or Avaya SES in the same IP network region. Thus, the audio path will always include the media processor board.
- Inter-region IP-IP Direct Audio – Set to **no** to deny direct IP-to-IP audio connectivity between endpoints registered to Avaya Communication Manager or Avaya SES in different IP network regions. Thus, the audio path will always include the media processor board.

Note: *For this solution to work, the shuffling (IP-IP Direct Audio) feature must be turned OFF, as mentioned above.*

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: testroom.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   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
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

3.2. Configure IP Node Name

This section describes the steps for setting IP node name for Avaya SES in Avaya Communication Manager. Enter the **change node-names ip** command, and add a node name for Avaya SES along with its IP address.

```
change node-names ip
                                IP NODE NAMES
    Name                  IP Address
CLAN                   192.45.80.87
MEDPRO                 192.45.80.88
SIP                    192.45.80.101
VAL                    192.45.80.85
default                0.0.0.0
procr                  192.45.80.214
```

3.3. Configure SIP Signaling

This section describes the steps for administering a signaling group in Avaya Communication Manager for communication between Avaya Communication Manager and Avaya SES and Citrix Communication Gateway. During the compliance test, two signaling groups were configured: one for Avaya Communication Manager and Avaya SES and the other for Avaya Communication Manager and Citrix Communication Gateway. The signaling group for the Citrix Communication Gateway does not utilize a Domain Name, instead, it utilizes the IP address of the Citrix Communication Gateway for the Far-end Domain field. Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- Group Type – Set to **sip.**
- Near-end Node Name - Set to **CLAN** as displayed in **Section 3.2**.
- Far-end Node Name - Set to the Avaya SES name configured in **Section 3.2**.
- Far-end Network Region - Set to the region configured in **Section 3.1**.
- Far-end Domain - Set to **testroom.com**. This should match the SIP Domain value in **Section 4.1**.

```
add signaling-group 201
                               SIGNALING GROUP

 Group Number: 201            Group Type: sip
                        Transport Method: tls




   Near-end Node Name: CLAN                 Far-end Node Name: SIP
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1
       Far-end Domain: testroom.com

                                            Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? n
```

```
         Enable Layer 3 Test? n
 Session Establishment Timer(min): 120
```

The configuration of the signaling group between Avaya Communication Manager and Citrix Communication Gateway utilize the same information, except for the Far-end Domain field, which should be set to the IP address of Citrix Communication Gateway.

```
add signaling-group 202
                               SIGNALING GROUP

 Group Number: 202            Group Type: sip
                        Transport Method: tls



   Near-end Node Name: CLAN                Far-end Node Name: SIP
 Near-end Listen Port: 5061              Far-end Listen Port: 5061
                                       Far-end Network Region: 1
       Far-end Domain: 192.45.80.131

                                            Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
                                                   IP Audio Hairpinning? n
         Enable Layer 3 Test? n
 Session Establishment Timer(min): 3
```

3.4. Configure SIP Trunk

This section describes the steps for administering a trunk group in Avaya Communication Manager for communication between Avaya Communication Manager and Avaya SES and Citrix Communication Gateway. During the compliance test, two trunk groups were configured: one for Avaya Communication Manager and Avaya SES and another for Avaya Communication Manager and Citrix Communication Gateway. When a second trunk is utilized, Avaya SES does not recognize the domain name. However, Avaya SES will check the trusted host table. If the IP address of Citrix Communication Gateway is in the trusted host table, then the call will be sent to Citrix Communication Gateway. Enter the **add trunk-group <t>** command, where **t** is an unallocated trunk group and configure the following:

- Group Type – Set to the Group Type field value configured in **Section 3.3**.
- Group Name – Enter a descriptive name.
- TAC (Trunk Access Code) – Set to any available trunk access code.
- Signaling Group – Set to the Group Number field value configured in **Section 3.3**.
- Number of Members **–** Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 201                                          Page   1 of  21
                               TRUNK GROUP

Group Number: 201                 Group Type: sip           CDR Reports: y
  Group Name: to SIP                        COR: 1        TN: 1        TAC: 116
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                    Night Service:
```

```
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                      Signaling Group: 201
                                                    Number of Members: 50
```

The following screen shows the configuration for the trunk between Avaya Communication Manager and Citrix Communication Gateway.

```
add trunk-group 202                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 202                 Group Type: sip           CDR Reports: y
  Group Name: SIP-Citrix                   COR: 1        TN: 1        TAC: 1001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                      Signaling Group: 202
                                                    Number of Members: 10
```

3.5. Configure Coverage Path

Enter **add coverage path c**, where **c** is an unused coverage path number. In the compliance test, the Point1 field under the COVERAGE POINTS section was set to the remote call coverage, **r1001**.

```
add coverage path 202                                        Page   1 of   1
                                 COVERAGE PATH

                  Coverage Path Number: 202
                                                  Hunt after Coverage? n
                      Next Path Number:           Linkage

COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
              Active?             n              n
                Busy?             y              y
       Don't Answer?              y              y         Number of Rings: 2
                 All?             n              n
 DND/SAC/Goto Cover?              y              y
   Holiday Coverage?              n              n

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: r1001          Rng:    Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

Enter the **change coverage remote r** command, where **r** is the remote call coverage table. The remote call coverage was set to r1001, in the previous step. That means the remote call coverage table should be 2, since the remote call coverage table 2 covers for the remote call coverage 1001 to 2000. During compliance testing, the extension 44444 was configured on Citrix Communication Gateway.

```
change coverage remote 2                                        Page   1 of  23

                        REMOTE CALL COVERAGE TABLE
                        ENTRIES FROM 1001 TO 2000

01: 44444                  16:                        31:
02:                        17:                        32:
03:                        18:                        33:
04:                        19:                        34:
```

3.6. Configure Stations

This section describes the steps for administering a station used during the compliance test. When a call is coming to this station, the call will cover to the Citrix Communication Gateway extension. Enter the **change station e** command, where **e** is the extension of a station under test. On Page 1, set the Coverage Path 1 field to the number of the coverage path configured in **Section 3.5**.

```
change station 22001                                            Page   1 of   5
                                    STATION

Extension: 22001                       Lock Messages? n               BCC: 0
     Type: 4620                        Security Code: *                TN: 1
     Port: S00395                    Coverage Path 1: 202             COR: 1
     Name: Dashboard Display-1       Coverage Path 2:                 COS: 1
                                     Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19         Personalized Ringing Pattern: 1
                                           Message Lamp Ext: 22001
           Speakerphone: 2-way          Mute Button Enabled? y
        Display Language: english          Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal           Media Complex Ext:
   Survivable Trunk Dest? y                       IP SoftPhone? y

                                         IP Video Softphone? n


                                        Customizable Labels? y
```

3.7. Configure Call Routing

This section describes the steps for administering Automatic Alternate Routing in Avaya Communication Manager. During the compliance test, the Citrix Communication Gateway was configured as a 5 digit extension, 44444. Enter the **change uniform-dialplan d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial Citrix Communication Gateway extension. Enter the Citrix Communication Gateway extension's first digit (or first few digits or all) for the Matching Pattern field. Enter the length

of the Citrix Communication Gateway extension for the Len field. The Del field set to **0**, and the Net field is set to **aar**.

```
change uniform-dialplan 4                                    Page   1 of   2
                     UNIFORM DIAL PLAN TABLE
                                                          Percent Full: 0

  Matching                    Insert                Node
  Pattern        Len Del      Digits      Net Conv  Num
 44444            5   0                   aar   n
 7                5   0                   aar   n
 72888            5   0                   aar   n
                                               n
```

Enter the **change aar analysis d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial Citrix Communication Gateway extension configured in **Section 3.5**. Enter the number of an unused route pattern for the Route Pattern filed. The route pattern will be defined in the next step. The Call Type field is set to **aar**.

```
change aar analysis 4                                        Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                  Location:  all           Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
     44444                5    5     202      aar          n
     7                    5    5     79       aar          n
     72888                5    5     14       aar          n
                                                           n
```

Enter the **change route-pattern r** command, where **r** is the number of the selected route pattern. Enter the number of the trunk group configured in **Section 3.4** for the Grp No field. Assign a Facility Restriction Level to this routing preference for the FRL field. The FRL value 0 is the least restrictive.

```
change route-pattern 202                                     Page   1 of   3
                    Pattern Number: 202 Pattern Name:
                              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: 202  0                                                           n   user
 2:                                                                  n   user
 3:                                                                  n   user
 4:                                                                  n   user
 5:                                                                  n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                   Dgts Format
                                                           Subaddress
 1: y y y y y n  n            rest                                     none
 2: y y y y y n  n            rest                                     none
```

```
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
```

To allow external/PSTN calls to access the Citrix Communication Gateway, ensure that the proper digit treatment is applied to incoming trunk calls. This can be accomplished by using the **change inc-call-handling-trmt trunk-group x**, where **x** is the incoming calls trunk group number.

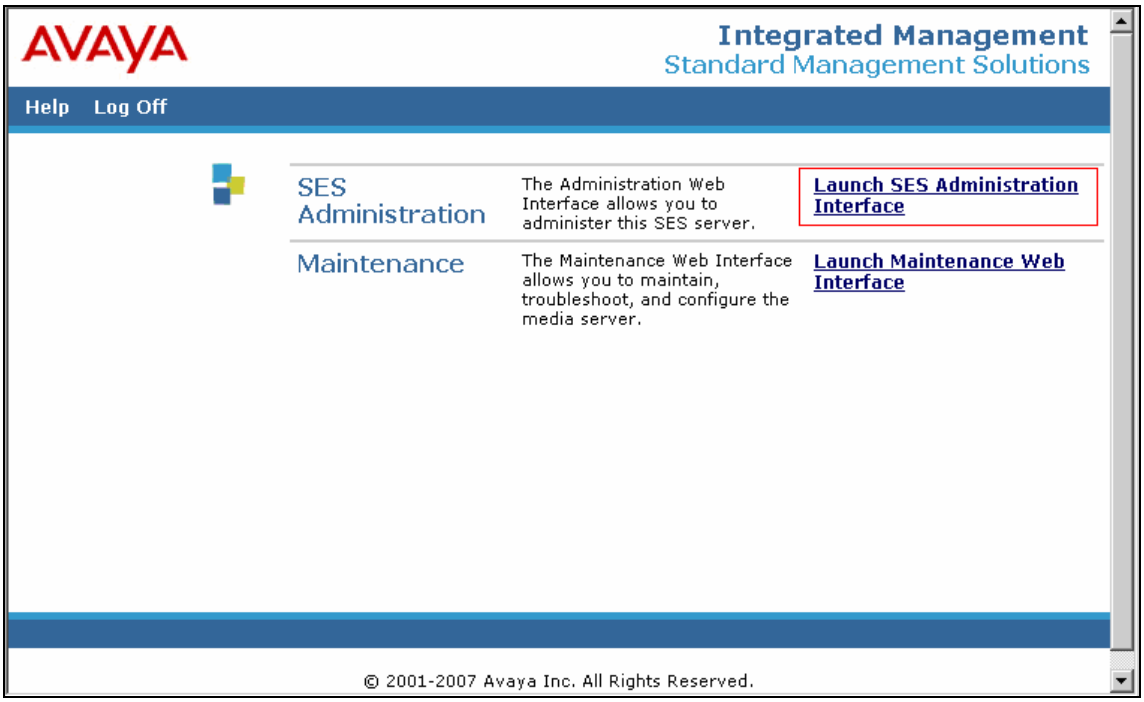
```
change inc-call-handling-trmt trunk-group 80                    Page   1 of  30
 Service/      Called    Called      Del Insert          Per Call Night
 Feature        Len      Number                        CPN/BN   Serv
tie             5  22942            5   22001
```

4. Configure Avaya SIP Enablement Services

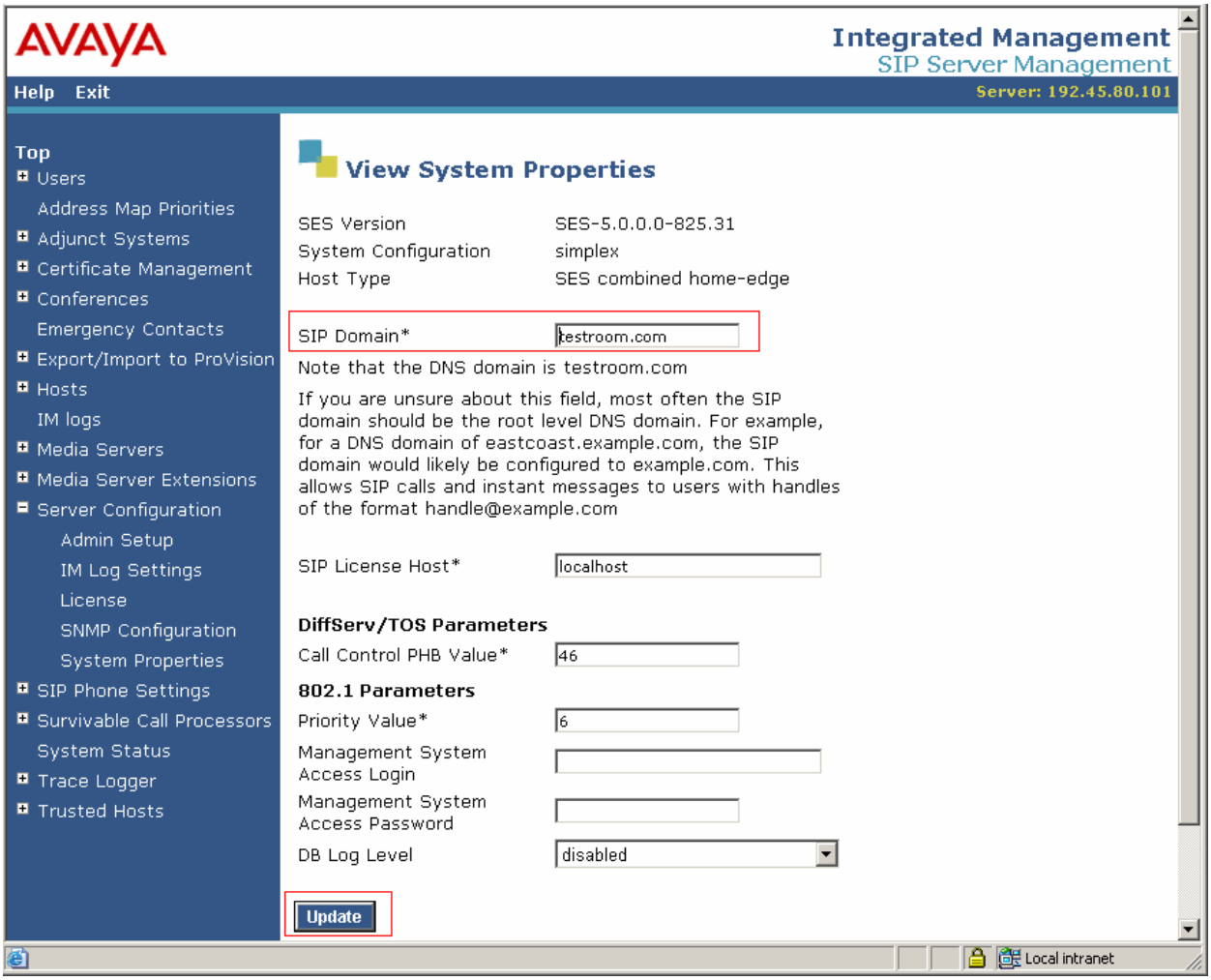
This section describes the steps for creating SIP trunk between Avaya SES and Avaya Communication Manager, and Citrix Communication Gateway. In this section, the procedures for configuring server properties, a media server interface and a trusted host on Avaya SES will be discussed. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

4.1. Configure SES Server Properties

Launch a web browser, enter **https://<IP address of SES server>/admin** in the URL, and log in with the appropriate credentials. Click on the **Launch SES Administration Interface** link upon successful login.



In the Integrated Management SIP Server Management page, select the **Server Configuration → System properties** link from the left pane of the screen. Verify the SIP Domain matches the Far-end Domain field value configured for the signaling group on Avaya Communication Manager in **Section 3.1**. Click on the **Update** button, after the completion.



4.2. Configure Media Server Interface

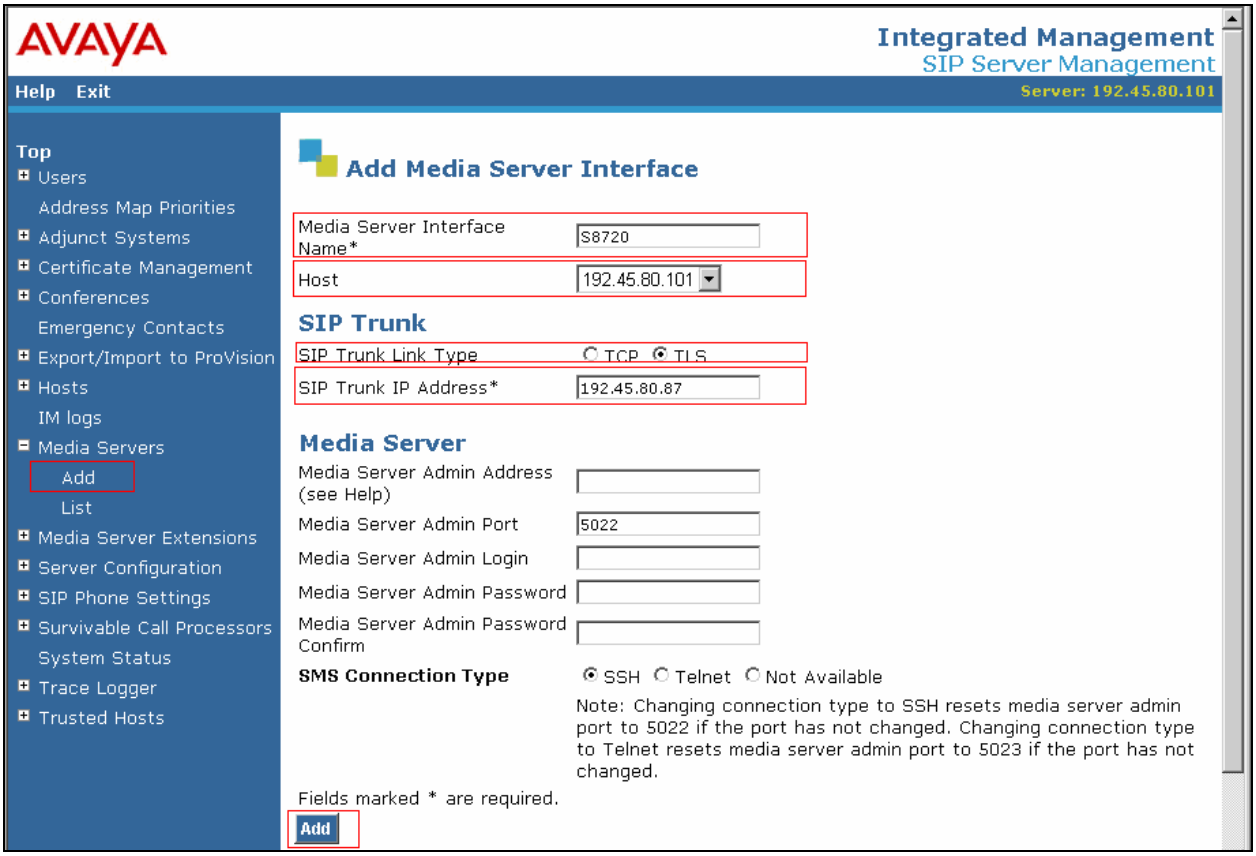
This section provides steps to add SIP-enabled media servers to the SIP domain. In the Integrated Management SIP Server Management page, select the **Media Servers → Add** link from the left pane of the screen. The following screen shows the Add Media Server Interface page. The highlighted fields were configured for the compliance test:

- Media Server Interface Name – Enter a descriptive name for the media server interface.
- Host – From the alphabetized drop-down list of names, select the name of the SES server that you want to associate with the Avaya Communication Manager Media server's SIP trunk.
- SIP Trunk Link Type – Select one of the listed protocols to be used for the SIP link between the media server and the specified host:
    - TCP (Transport Control Protocol)

- TLS (Transport Link Security) – This is the default protocol, which is selected for all servers.

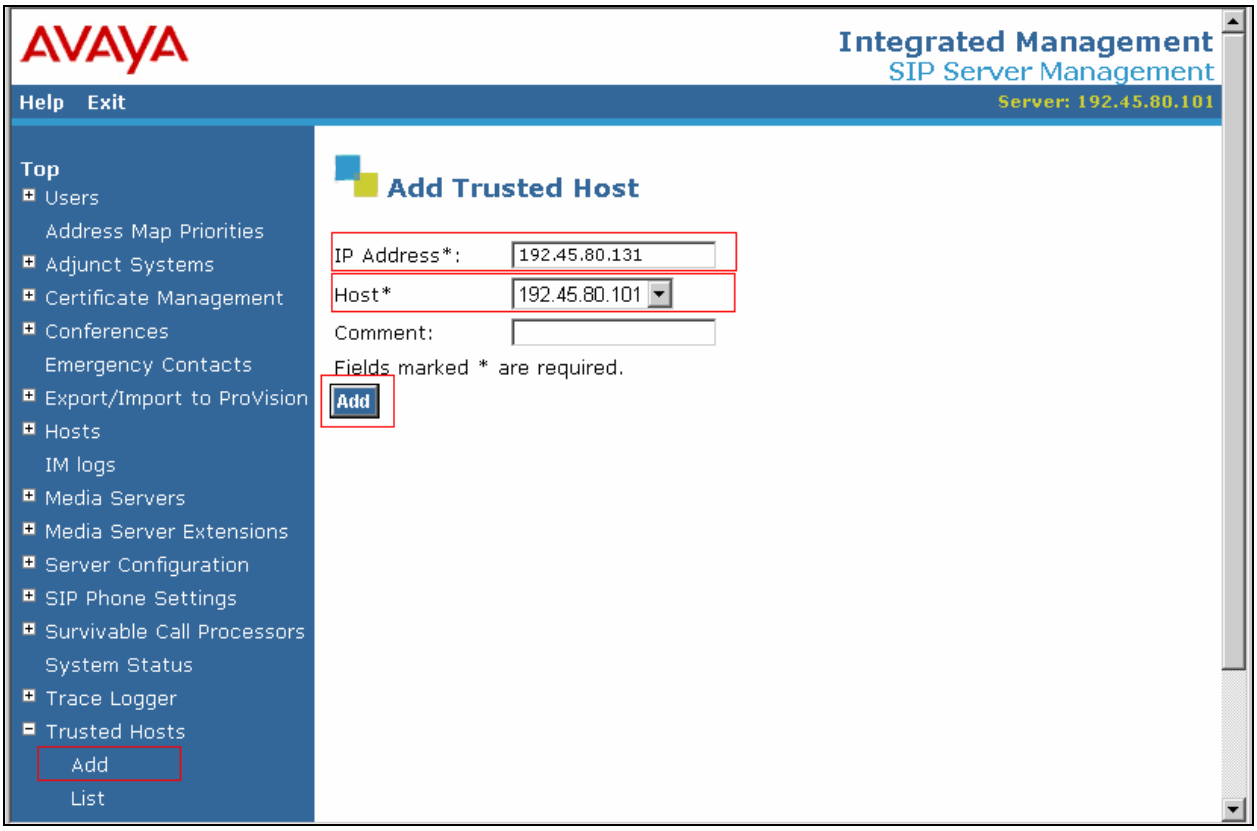
- SIP Trunk IP Address – Enter the IP address for the CLAN (or media server's procr) IP address that terminates the SIP link from SES.

Click **Add** when finished.



4.3. Configure Trusted Host

This section provides steps to add a trusted host to the SIP domain. In the Integrated Management SIP Server Management page, select the **Trusted Hosts → Add** link from the left pane of the screen. The following screen shows the Add Trusted Host page. The highlighted fields were configured for the compliance test. Click **Add** when finished.



5. Configuring Citrix Communication Gateway

Citrix configures the Communication Gateway application for their end customers. For installation and configuration of the application, refer to [3], or contact Citrix Technical Support.

6. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying the call redirection, and click2call features utilizing the SIP trunk between Avaya Communication Manager and Citrix Communication Gateway.

6.1. General Test Approach

The general test approach was to place intra-switch, inter-switch and PSTN calls manually to a station that had coverage directed to the Citrix Communication Gateway. Citrix Communication Gateway then locates the employee by dialing the number at which the employ provisioned the number where they can be reached. Busy calls from intra-switch, inter-switch and PSTN callers are able to leave voice messages, using a call redirect feature. Citrix Communication Gateway is able to place two calls to two different stations and bridge these two phones using the click to call feature.

6.2. Test Results

The feature and functionality test cases passed.

7. Verification Steps

The following steps may be used to verify the configuration:

- Verify a call redirect – From the SAT, enter the command **status trunk s**, where **s** is the number of the trunk group configured in **Section 3**, and verify the trunk group member is freed, after the call redirected.
- Verify click to call – Let Citrix Communication Gateway call two numbers ("a" and "b"). As station "a" picks up, station "b" should ring. At this point, enter the command **status trunk s**, where **s** is the number of the trunk group configured in **Section 3**, and verify that two trunk group members are freed.

8. Support

For technical support on Citrix Communication Gateway, contact Citrix support at:

- Phone: (866) 281-0347
- E-mail: commgsupport@citrix.com

9. Conclusion

These Application Notes describes the procedures for configuring SIP redirection feature between Citrix Communication Gateway and Avaya Communication Manager. Citrix Communication Gateway successfully performed a call redirection, and click to call. One observation during the compliance test was, the shuffling must be turned OFF, as indicated in **Section 3.1**.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administration Guide for Avaya Communication Manager*, Release 4.0, Issue 5, January 2008, Document Number 03-300509.

[2] *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services*, Issue 5, January 2008, Document Number 03-600768

The following document was provided by Citrix.
[3] *Citrix® Communication Gateway Administrator's Guide*, Release 1.0

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.