Application Notes for PCR COMIT Technology Management System with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for PCR COMIT Technology Management System to interoperate with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Application Enablement Services.

PCR COMIT Technology Management System, utilizing System Management Service on Avaya Aura^{TM} Application Enablement Services, interfaces with Avaya Aura^{TM} Communication Manager to perform the software-based Move, Add, Change and Delete activities directly to the switch.

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

1. Introduction

These Application Notes describe the configuration steps required for PCR COMIT Technology Management System to interoperate with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Application Enablement Services.

PCR COMIT Technology Management System offers flexibility and accountability for managing voice system operations by providing an alternative to use the native interfaces of various PBXs. PCR COMIT Technology Management System utilizes the System Management Service of Application Enablement Services to interface with Communication Manager.

The System Management Service is a web service resident on Application Enablement Services. The web service provides programmatic access to a subset of the administration objects available via Communication Manager System Access Terminal (SAT) screens. A key benefit of the System Management Service is that it allows programmatic access via a standard protocol (SOAP) to function that is otherwise usually only accessible using terminal emulation using SAT forms. The System Management Service enables clients that use SOAP to display, list, add, change and remove specific managed objects on Communication Manager.

1.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature test cases covered the following COMIT Technology Management System objects:

- Stations (add, change, remove, list, status, and display)
- Authorization Codes (add, list, change and remove)

The serviceability testing focused on verifying the ability of the PCR COMIT Technology Management System application to recover from adverse conditions, such as Ethernet disconnects, power failures, and server reboots.

1.2. Support

Technical support on PCR COMIT Technology Management System can be obtained through the following:

- **Phone:** (616) 554-1055
- **Web:** http://www.pcr.com

2. Reference Configuration

PCR COMIT Technology Management System was installed on a Linux Fedora 2.6. PCR COMIT Technology Management System utilized the System Management Service on Avaya Aura^{TM} Application Enablement Services to interface with Avaya Aura^{TM} Communication Manager (Avaya S8300D Server).

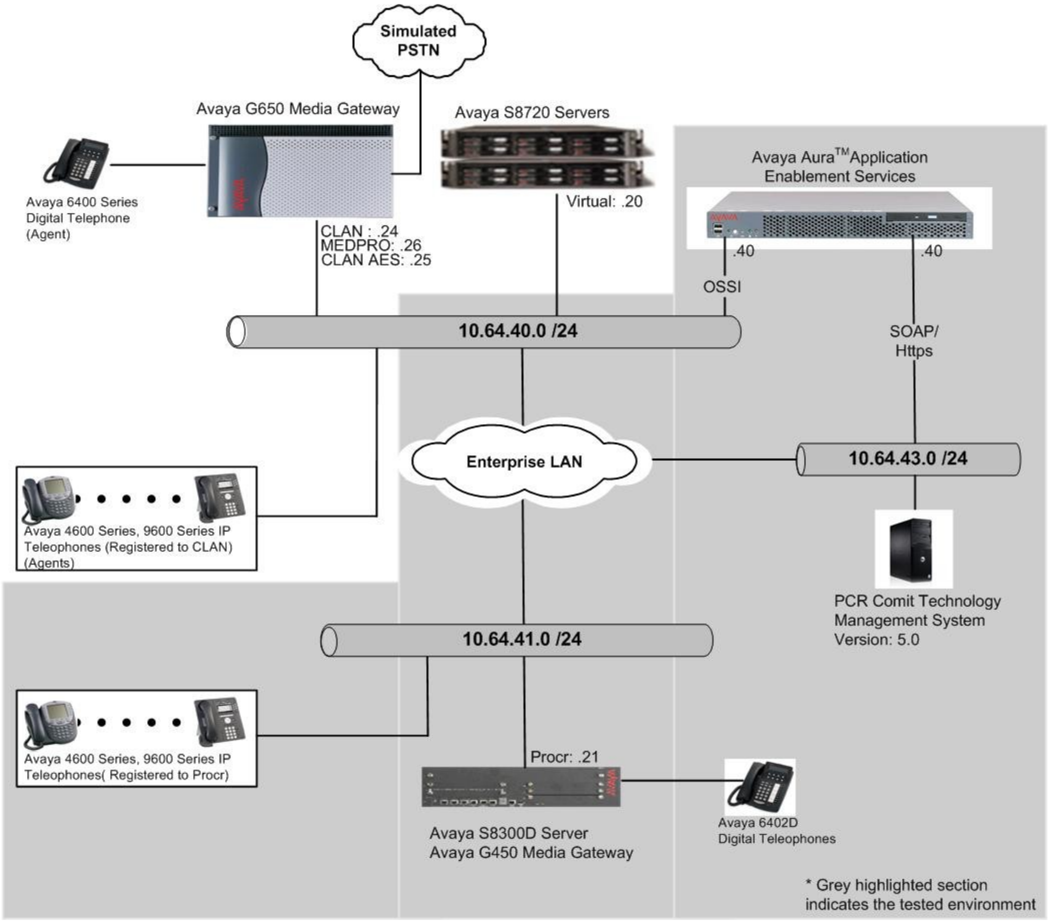

Simulated PSTN
Avaya G650 Media Gateway
Avaya S8720 Servers
Avaya Aura™Application Enablement Services
Avaya 6400 Series Digital Telephone (Agent)
Virtual: .20
CLAN : .24
MEDPRO: .26
CLAN AES: .25
.40
.40
OSSI
10.64.40.0 /24
SOAP/ Https
Enterprise LAN
10.64.43.0 /24
Avaya 4600 Series, 9600 Series IP Teleophones (Registered to CLAN) (Agents)
PCR Comit Technology Management System Version: 5.0
10.64.41.0 /24
Avaya 4600 Series, 9600 Series IP Teleophones(Registered to Procr)
Procr: .21
Avaya S8300D Server
Avaya G450 Media Gateway
Avaya 6402D Digital Teleophones
* Grey highlighted section indicates the tested environment

Figure 1: PCR COMIT Technology Management System with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Application Enablement Services

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway	Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya S8720 Servers with Avaya G650 Media Gateway	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura™ Application Enablement Services	5.2.2 (r5-2-2-105-0)
Avaya 4600 Series IP Telephones	
4625 (H.323)	2.9
Avaya 9600 Series IP Telephones	
9620 (H.323) 9630 (H.323) 9650 (H.323)	3.1 3.1 3.1
Avaya 6400D Series Digital Telephones	-
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Extreme Networks Summit 48	4.1.21
PCR COMIT Technology Management System on Linux Fedora 2.6	5.0

4. Configure Avaya Aura^{TM} Communication Manager

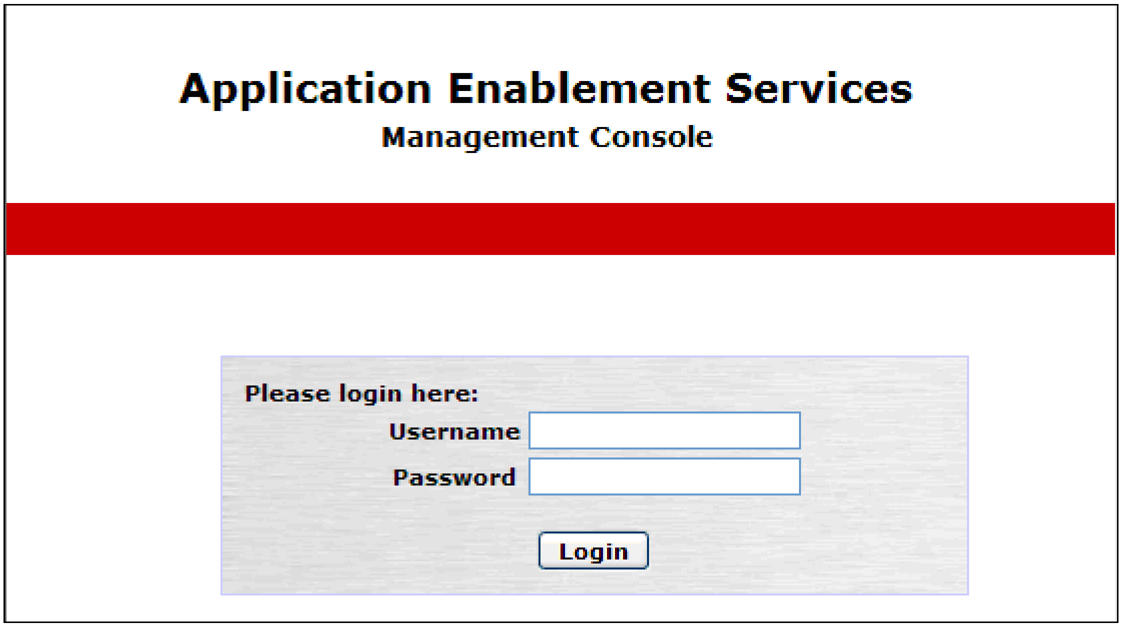
The PCR solution utilizes the System Management Service (SMS) on Application Enablement Services to manage objects on Communication Manager. The assumption has been made that the basic configuration of Communication Manager has been completed. The only item that needs to be configured on Communication Manager is an Administrator account. During compliance testing, the default administrator account was used.

5. Configure Avaya Aura^{TM} Application Enablement Services

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

- Configure SMS Proxy Port Settings
- Configure SMS Properties

Launch a web browser, enter https://<IP address of the Application Enablement Services server> in the address field, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console page.

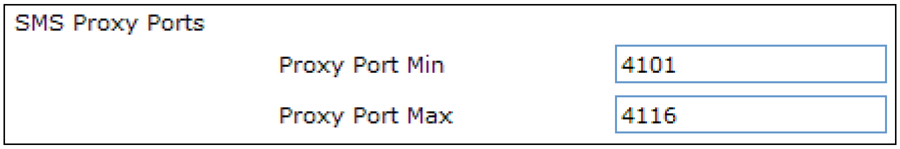


Application Enablement Services

Management Console

5.1. Configure SMS Proxy Port Settings

Navigate to **Networking → Ports**. By default, Application Enablement Services assigns ports 4101 to 4116 for SMS proxy ports. If required, change the **Proxy Port Min** and **Proxy Port Max** values to port numbers that are appropriate for the desired configuration. SMS can use up to 16 ports. The default values were used during compliance testing.



SMS Proxy Ports

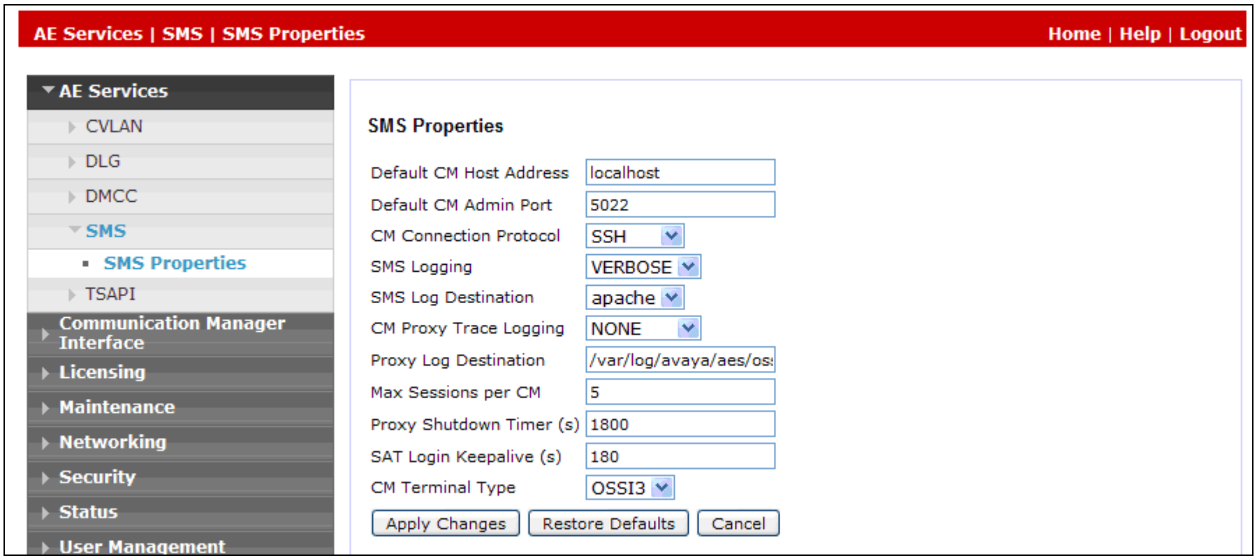
Proxy Port Min	4101
Proxy Port Max	4116

5.2. Configure SMS Properties

Navigate to **AE Services → SMS → SMS Properties**. Enter the following values for the specified fields:

- **Default CM Host Address** – Enter the Communication Manager Host Address (e.g. **10.64.43.40 or localhost**). SMS will attempt to connect to this CM host address, as long as no host address is explicitly specified in the authorization header of a client request. If this field is blank, all SMS requests must explicitly include the target CM host address.

Default values were used for all the remaining fields during compliance testing.



SMS Properties

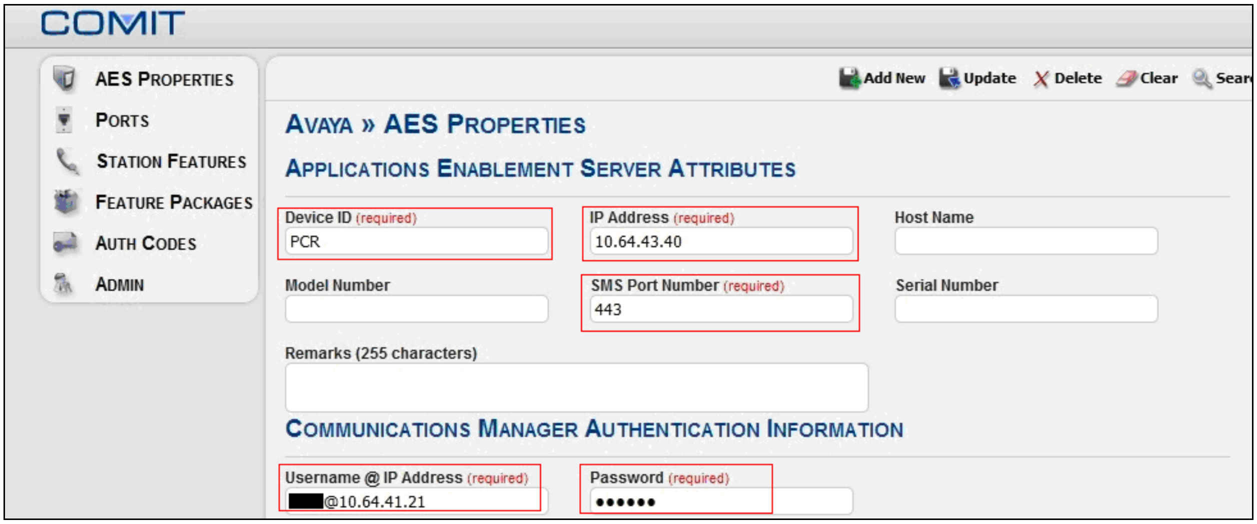
Default CM Host Address	localhost
Default CM Admin Port	5022
CM Connection Protocol	SSH
SMS Logging	VERBOSE
SMS Log Destination	apache
CM Proxy Trace Logging	NONE
Proxy Log Destination	/var/log/avaya/aes/os:
Max Sessions per CM	5
Proxy Shutdown Timer (s)	1800
SAT Login Keepalive (s)	180
CM Terminal Type	OSSI3

6. Configure PCR COMIT Technology Management System

This section provides the procedures for configuring PCR COMIT Technology Management System to interface with Application Enablement Services. Enter the following values for the specified fields:

- **Device ID**: Enter the computer name of the server hosting the PCR COMIT Technology Management System application.
- **IP Address**: Enter the Application Enablement Services server IP address, **10.64.43.40**.
- **SMS Port number**: Enter **443**, since it is using https.
- **Username@IP Address**: Enter *username@< ip address>* where *username* is the Communication Manager administrator account, and <*ip address*> is the IP address of Communication Manager (procr), **xxxxx@10.64.41.21**.
- **Password**: Enter the administrator account password in Communication Manager.

Default values were used for the remaining fields during the compliance test, and click the **Submit** button (not shown).



Avaya » AES Properties

Applications Enablement Server Attributes

Device ID (required): PCR	IP Address (required): 10.64.43.40	Host Name:
Model Number:	SMS Port Number (required): 443	Serial Number:

Remarks (255 characters):

Communications Manager Authentication Information

Username @ IP Address (required): [redacted]@10.64.41.21	Password (required): ••••••

7. General Test Approach and Test Results

All test cases were performed manually. The administration objects were modified on Communication Manager using the System Access Terminal (SAT). The PCR COMIT Technology Management System application was used to modify single record objects one at a time. For each object (Station, Authorization Code), several Operation parameters were chosen for modification. Not all Operation parameters were tested.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cables on each server, and powering down/up each server, and rebooting each server to verify proper recovery.

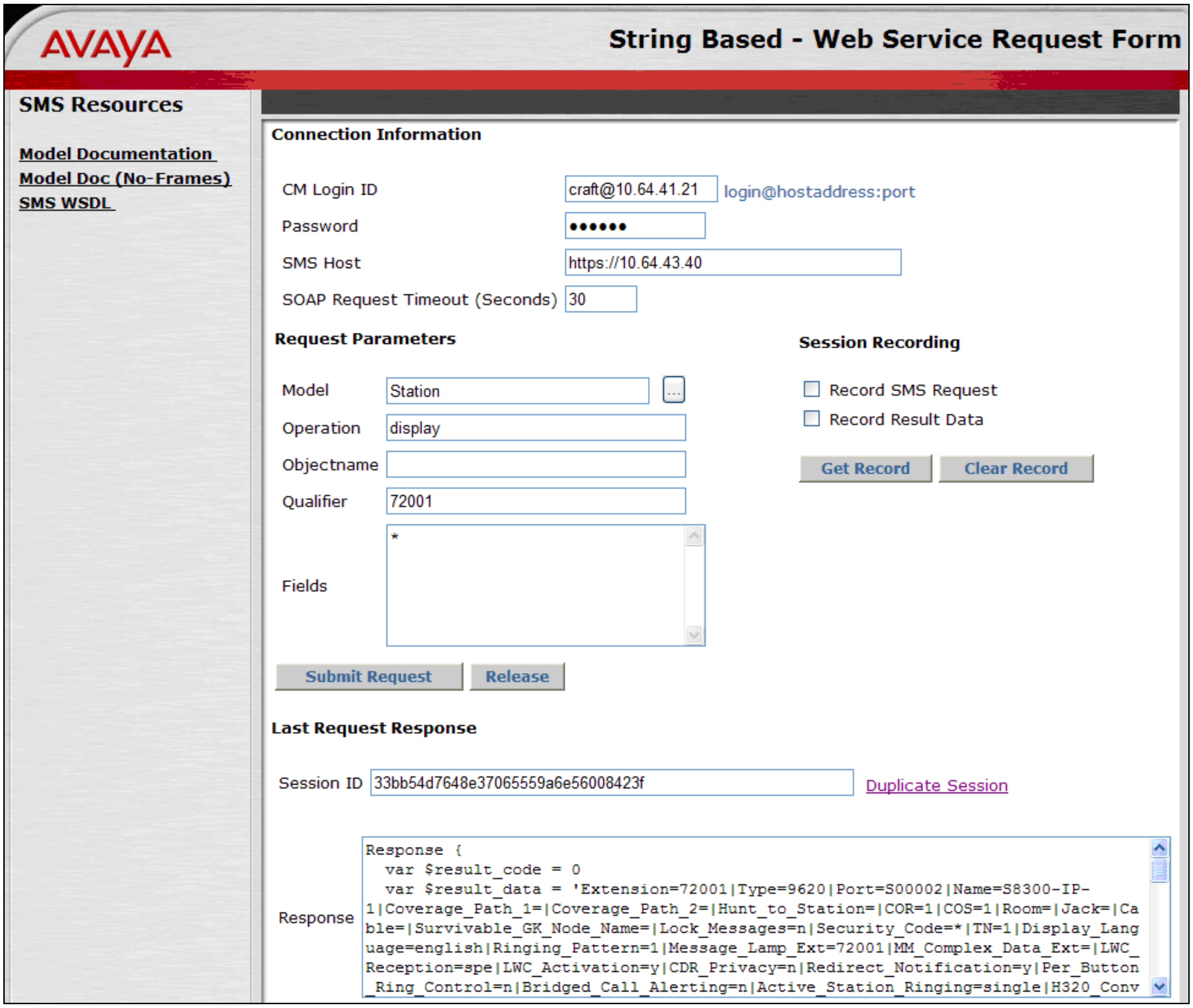
All test cases executed and passed with an exception. PCR COMIT Technology Management System was not able to perform **change** on the authorization Code model. Instead, PCR COMIT Technology Management System utilized a two-steps procedure (**remove** and **add**).

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the System Management Service.

Navigate to *https://<ip address>/sms/sms_test.php,* where *<ip address>* is the IP address of the Application Enablement Services server. The Web Service Request Form is displayed as shown in the screen below. Enter the **Username** and **Password** configured in **Section 6** for the **CM Login ID** and **Password**, respectively. Fill in appropriate **Request Parameters** for the configuration and click the **Submit Request** button. In this example, a request was sent to display station 72001.

Verify that a response is populated into the **Response** box and that **var $result_code = 0**.



CM Login ID: craft@10.64.41.21 login@hostaddress:port

Password: ••••••

SMS Host: https://10.64.43.40

SOAP Request Timeout (Seconds): 30

Model: Station

Operation: display

Objectname:

Qualifier: 72001

Fields: *

Session ID: 33bb54d7648e37065559a6e56008423f

Response:

```
Response {
  var $result_code = 0
  var $result_data = 'Extension=72001|Type=9620|Port=S00002|Name=S8300-IP-
1|Coverage_Path_1=|Coverage_Path_2=|Hunt_to_Station=|COR=1|COS=1|Room=|Jack=|Ca
ble=|Survivable_GK_Node_Name=|Lock_Messages=n|Security_Code=*|TN=1|Display_Lang
uage=english|Ringing_Pattern=1|Message_Lamp_Ext=72001|MM_Complex_Data_Ext=|LWC_
Reception=spe|LWC_Activation=y|CDR_Privacy=n|Redirect_Notification=y|Per_Button
_Ring_Control=n|Bridged_Call_Alerting=n|Active_Station_Ringing=single|H320_Conv
```

9. Conclusion

These Application Notes describe the configuration steps required for PCR COMIT Technology Management System to successfully interoperate with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Application Enablement Services. All executed feature and serviceability test cases passed.

10. Additional References

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

[1] *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010.

[2] *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Document 02-300357, Issue 11, Release 5.2, November 2009.

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.