Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Application Suite with Avaya Aura™ Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required to allow MTS Application Suite to collect call detail records (CDR) from Avaya Aura™ Communication Manager running on Avaya Media Servers using Avaya Reliable Session Protocol (RSP) over TCP/IP. The MTS Application Suite collects, stores, and processes these call records to provide usage analysis, call costing, and billing capabilities.

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.

©2010 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe a compliance-tested call detail recording (CDR) solution comprised of Avaya Aura™ Communication Manager and the MTS Application Suite. The Application Suite includes a call accounting software application that uses call detail records to provide reporting capabilities to business and IT managers to track and manage call usage and telecom expenses as well as other Telephony management functions.

Application Suite is a modular architected solution which resides on a Microsoft Windows server, typically at the customer's premises. The server hosts an SQL database which contains configuration as well as detailed records from the configured data sources, including communication systems. The solution is capable of being configured to capture and record data from a variety of sources simultaneously. Avaya Aura™ Communication Manager communicates via an Avaya Reliable Session Protocol (RSP) session, typically over the local TCP/IP network. For the purposes of this test, the Application Suite server was located on the vendor's premises and connected over a WAN. The Application Suite runs as a background service that terminates the RSP protocol, collects the call records from Avaya Aura™ Communication Manager, and stores the records in the database.

In addition, the Application Suite can be configured to run scheduled jobs to collect data files from a variety of sources, including enterprise directories (LDAP for example). Through this scheduling mechanism, the application can be configured to use an SFTP Client to access CDR record files on Avaya Survivable Remote Processors (LSP), enabling consistent and reliable reporting of communication systems data across a large number of sources under a variety of operating conditions.

Users are able to login through a web interface in order to view ad hoc, or preconfigured reports including data collected from Avaya Aura™ Communication Manager(s). Reports can be scheduled to run at certain intervals; output can be configured to be stored on servers in a variety of formats (.xls/.pdf for example) as well as emailed as attachments.

Avaya Aura™ Communication Manager can generate call detail records for intra-switch calls, as well as inbound and outbound trunk calls. In addition, split records can be generated for transferred and conference calls. The Application Suite can support any CDR format provided by Avaya Aura™ Communication Manager; the configuration tested is a "typical" format which does not include all of the data available from Communication Manager. As part of the Application Suite product implementation process, MTS or their dealers configure the system to accurately parse the CDR data.

1.1. Interoperability Compliance Testing

A variety on inbound and outbound trunk calls over both H.323 TIE and ISDN PSTN trunks were conducted including a series of conference, transfer and hold use cases. Additionally, internal calls were tested. Finally, internal calls on a Local Survivable Processor (LSP) were tested to validate proper collection of records from a survivable server. The testing was

©2010 Avaya Inc. All Rights Reserved.

conducted with the Application Suite server residing remotely, accessible over WAN connections in order to simulate how many customers with multiple office locations deploy these solutions.

On page 2 of the System CDR form on Communication Manager, the actual data fields used in this test are documented. The Application Suite can accommodate any information that Communication Manager is capable of sending to CDR applications by modifying the "custom" CDR format in the Communication Manager forms, and adding additional field definitions on the Application Suite server configuration. The most commonly used data elements MTS deploys with were included in this test.

1.2. Support

Technical support for the MTS Application Suite can be obtained through the following:

- **Email**: tech.support@mtsint.com
- **Phone**: 1(800)745-8725

2. Reference Configuration

Figure 1 illustrates the configuration that was used for the compliance test. The configuration consists of two Avaya Media Servers running Avaya Aura™ Communication Manager. Site A is comprised of Avaya Aura™ Communication Manager that runs on an Avaya S8300 Server with an Avaya G450 Media Gateway. Site B is comprised of Avaya Aura™ Communication Manager that runs on an Avaya S8300 Server residing in an Avaya G350 Media Gateway. Site B was configured as a Survivable Remote Processor to the Site A processor. Each Avaya Aura™ Communication Manager is connected to an IP network comprised of an Extreme Networks Summit 48 Layer III switch and Avaya C363T-PWR Converged Stackable Switch.

Calls to/from the test environment were placed over ISDN and H.323 Trunks connected to other equipment in the lab. These additional elements were not shown in the diagram as they were used to simulate PSTN connected systems and endpoints.

The MTS Application Suite was running on a Windows 2008 server residing at the vendor's location. Real time CDR data was sent via a RSP session over the internet in order to collect CDR records from the primary call server. This configuration re-enforces the flexibility available in both the Avaya and vendor's equipment in that it demonstrates the ability to use centralized management in distributed enterprises. In addition, intra-switch calls were placed between devices connected to the gateway at Site B in order to emulate the conditions where call details are required from remote sites in times when network connectivity between sites is out of service yet business continues.

The environment utilized a variety of 6400D Series Digital Telephones, as well as 9600 Series IP Telephone sets.

©2010 Avaya Inc. All Rights Reserved.

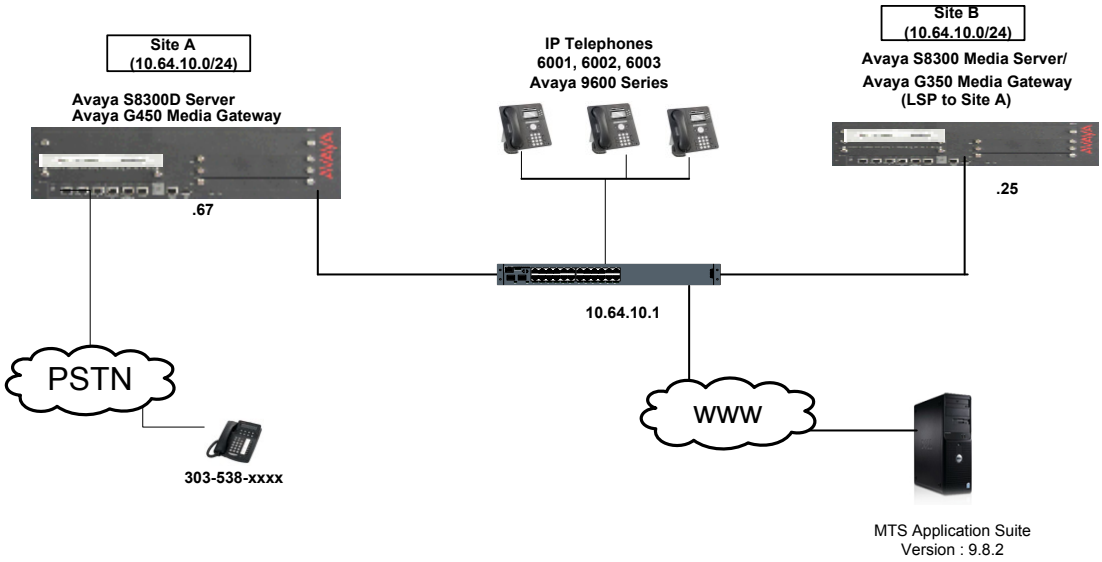


Figure 1: CDR data was collected from Site A real time, and Site B via SFTP

3. Equipment and Software Validated

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

Hardware Component	Version	Description
Avaya S8300 Server/ G450 Media Gateway	6.0	Runs Avaya Aura™ Communication Manager (CM) call processing software.
Avaya S8300 Server/ G350 Media Gateway (SRP/LSP)	6.0	Runs Avaya Aura™ Communication Manager (CM) call processing software. This server is the Survivable Remote Processor
Avaya 9600 Series IP Phones 9620 9630 9650C 9670	 3.1 3.1 3.1 3.1	H.323 IP Sets
Avaya 6408D and 8400 Series Digital Phones	-	Desktop digital phones with programmable call appearance/feature keys, fixed feature buttons, display, and full duplex speakerphone.
Analog Phone	-	
MTS Application Suite on Windows 2008 Server	Application Version 9.8.2 Windows Server 2008	Operating System for the Certification environment. Compatible with Server 2003, Windows 7 and Windows XP

©2010 Avaya Inc. All Rights Reserved.

4. Configure the Avaya Communication Manager

This section describes the procedure for configuring call detail recording (CDR) in Avaya Aura™ Communication Manager. These steps were performed through a System Access Terminal (SAT). The steps were as follows:

- Administer Node Name for the MTS Application Suite Server
- Configure IP Services
- Configure System-wide CDR settings
- Define Intra-Switch CDR Members
- Configure Trunks to be Reported
- Configure Survivable Report User Account
- Configure Survivable Processor CDR Parameters
- Configure Authorization Codes

4.1. Administer Node Name for the MTS Application Suite Server

Avaya Aura™ Communication Manager was configured to generate CDR records using RSP over TCP/IP to the public IP address of the server running the Application Suite. For the Avaya S8300 Server, the RSP link originates at the IP address of the processor Ethernet port (**procr**).

Use the **change node-names ip** command to create a new node name, for example, **MTS**. This node name is associated with the IP Address of the Server running the Application Suite.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
MTS                    10.64.10.101
RDTT                   10.64.10.51
LSPTR1                 10.64.10.25
procr                  10.64.10.67
```


©2010 Avaya Inc. All Rights Reserved.

4.2. Configure IP Services

Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, the following information should be provided:

- Service Type: **CDR1**
- Local Node: **procr** [For Avaya G650 Gateways, use the node name of the CLAN board.
- Local Port: **0** [The Local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.]
- Remote Node: **MTS** [The Remote Node is set to the node name previously defined.]
- Remote Port: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in the Application Suite.]

Note that in this test, a secondary CDR was defined. This was the local host running the Avaya RDTT software which was used to compare the data collected by the remote host.

```
change ip-services                                              Page   1 of   4

                                  IP SERVICES
 Service      Enabled      Local        Local       Remote      Remote
  Type                     Node         Port        Node        Port
CDR1                      procr          0         MTS         9000
CDR2                      procr          0         RDTT        9001
```

On **Page 3** of the ip-services form, enable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **y**.

```
change ip-services                                              Page   3 of   4

                              SESSION LAYER TIMERS
  Service      Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type       Protocol     Timer        Message Cntr    Cntr     Timer

 CDR1            y         30               3           3         60
 CDR2            y         30               3           3         60
```


©2010 Avaya Inc. All Rights Reserved.

4.3. Configure System-wide CDR settings

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and the format of the CDR data. The example below shows the settings used during the compliance test.

- CDR Date Format: **month/day**
- Primary Output Format: **customized**
- Primary Output Endpoint: **CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- Enable CDR Storage on Disk?: **y** [Enable the Survivable CDR feature. Default is **n**.]
- Use Legacy CDR Formats?: **n** [Allows CDR formats to use 4.x CDR formats. If the field is set to **y**, then CDR formats utilize the 3.x CDR formats.]
- Intra-switch CDR: **y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the **intra-switch cdr** form.]
- Record Outgoing Calls Only?: **n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- Outg Trk Call Splitting?: **y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- Inc Trk Call Splitting?: **y** [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]

```
change system-parameters cdr                                    Page   1 of   2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID):                        CDR Date Format: month/day
      Primary Output Format: customized      Primary Output Endpoint: CDR1
    Secondary Output Format: customized     Secondary Output Endpoint: CDR2
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? n                 Remove # From Called Number? n
Modified Circuit ID Display? n                              Intra-switch CDR? y
                 Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                  Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? y       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0              CDR Account Code Length: 5
```

Note: The standard format MTS uses was configured as a customized output as described below. There are additional data elements available on the Communication Manager platform, and in

©2010 Avaya Inc. All Rights Reserved.

installations where customers desire these additional items, they would tend to be appended to the end of this form following the date field. To see all available field options, please refer to *Administering Avaya Aura™ Communication Manager* (Reference 2).

```
change system-parameters cdr                                    Page   2 of   2
                          CDR SYSTEM PARAMETERS

     Data Item - Length          Data Item - Length          Data Item - Length
 1: time             - 4   17: auth-code        - 7   33:                   -
 2: space            - 1   18: space            - 1   34:                   -
 3: duration         - 4   19: frl              - 1   35:                   -
 4: space            - 1   20: space            - 1   36:                   -
 5: cond-code        - 1   21: ixc-code         - 1   37:                   -
 6: space            - 1   22: space            - 1   38:                   -
 7: code-dial        - 3   23: in-crt-id        - 3   39:                   -
 8: space            - 1   24: space            - 1   40:                   -
 9: code-used        - 3   25: out-crt-id       - 3   41:                   -
10: space            - 1   26: space            - 1   42:                   -
11: dialed-num       - 15  27: feat-flag        - 1   43:                   -
12: space            - 1   28: space            - 1   44:                   -
13: clg-num/in-tac   - 15  29: date             - 6   45:                   -
14: space            - 1   30: return           - 1   46:                   -
15: in-trk-code      - 4   31: line-feed        - 1   47:                   -
16: space            - 1   32:                  -     48:                   -

                             Record length = 87
```

4.4. Define Intra-Switch CDR members

If the **Intra-switch CDR** field is set to **y** on Page 1 of the system-parameters cdr form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the **Assigned Members** fields, enter the specific extensions whose usage will be tracked. To simplify the process of adding multiple extensions in the **Assigned Members** fields, the "Intra-switch CDR by COS" feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

```
change intra-switch-cdr                                         Page   1 of   3
                          INTRA-SWITCH CDR

                                Assigned Members:   5    of 1000   administered
   Extension          Extension          Extension          Extension
   6001
   6002
   6003
   6005
   6006
```


©2010 Avaya Inc. All Rights Reserved.

4.5. Configure Trunks to be Reported

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group *n*** command, where ***n*** is the trunk group number, to verify that the **CDR Reports** field is set to **y**. This applies to all types of trunk groups.

```
change trunk-group 1                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 1                   Group Type: isdn          CDR Reports: y
  Group Name: 10.64.10.10              COR: 2        TN: 1        TAC: *001
   Direction: two-way        Outgoing Display? n         Carrier Medium: H.323
 Dial Access? n              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                          Member Assignment Method: auto
                                                    Signaling Group: 1
                                                   Number of Members: 50
```

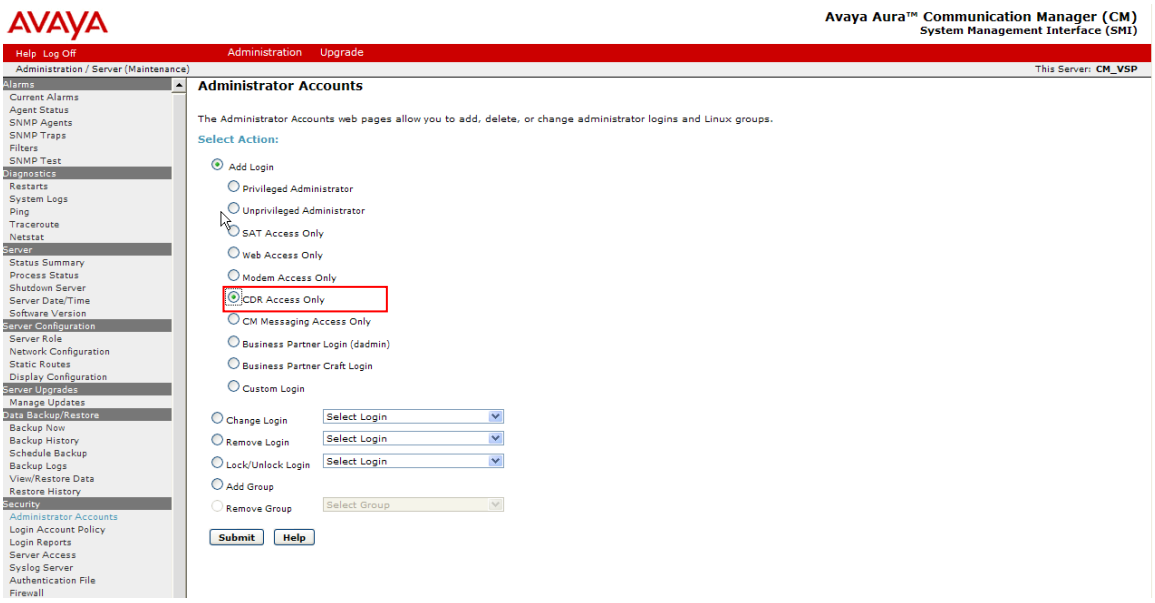
Repeat the above step for all trunks to be reported on. In this test, trunks 1 and 2 were used.

4.6. Configure Survivable Report User Account

Since Communication Manager Release 4.0, Avaya has supported CDR reporting from survivable servers. The idea is, if a survivable server handles calls during a period when the main processor is unavailable, the details are recorded and stored on a disk file on the LSP and the application may use this as an additional source of input. Most applications will check for files on the LSP daily and add the data to the reports if they exist, this is in fact how the Application Suite handles this data source.

Setup included adding a user account in System Manager:

©2010 Avaya Inc. All Rights Reserved.



The CDR_User group is a predefined group that the new user is assigned to by checking the **CDR Access Only** option as shown above. The pre-defined CDR_User group has security limitations that prevent this account from performing other tasks on the communication system.

After clicking **Submit**, a password was created on the following screen.

©2010 Avaya Inc. All Rights Reserved.

4.7. Configure Survivable Processor CDR Parameters

There are two ways to deploy survivable CDR. A Survivable Main server can be setup to write all CDR data to a disk file; this was not used in this case. Alternately, a Survivable Remote Processor can be used and specified on the **change survivable-processor** form to store CDR data to disk. All other settings were default.

```
change survivable-processor LSPTR1                              Page   2 of   3
                    SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local             Local    Remote            Remote
  Type              to dsk  Node              Port     Node              Port
  AESVCS      o       n     procr             8765
  CDR1        o       y
  CDR2        o       y
```

4.8. Configure Authorization Codes

Authorization Codes are often used when classes of users phones are administered with limited calling privileges but exceptions are required such as to call specific customers. Furthermore, supervisors or console operators can use authorization codes in order to enable dialing by restricted users on a pre-approved basis.

Typically, a user who is not authorized to make outbound trunk calls would have a COR assigned to the phone with an FRL that is lower than the trunks. For example, if a trunk is administered in a COR with an FRL value of 3, or the route pattern is assigned an FRL of 3, the FRL on the users station COR would need to be 3 or higher. However, if it is 2 or lower, the user would be unable to access the trunks. Entering an authorization code could enable a user to override this restriction.

The steps to setup authorization codes includes assigning a COR with an FRL that can access the trunk facilities. Authorization code 1234567 was used in this test, it was administered as follows:

```
change authorization-code 1234567                                Page   1 of   1
                 Authorization Code - COR Mapping
        NOTE: 1      codes administered. Use 'list' to display all codes

      AC      COR        AC      COR        AC      COR        AC      COR
1234567       3
```


©2010 Avaya Inc. All Rights Reserved.

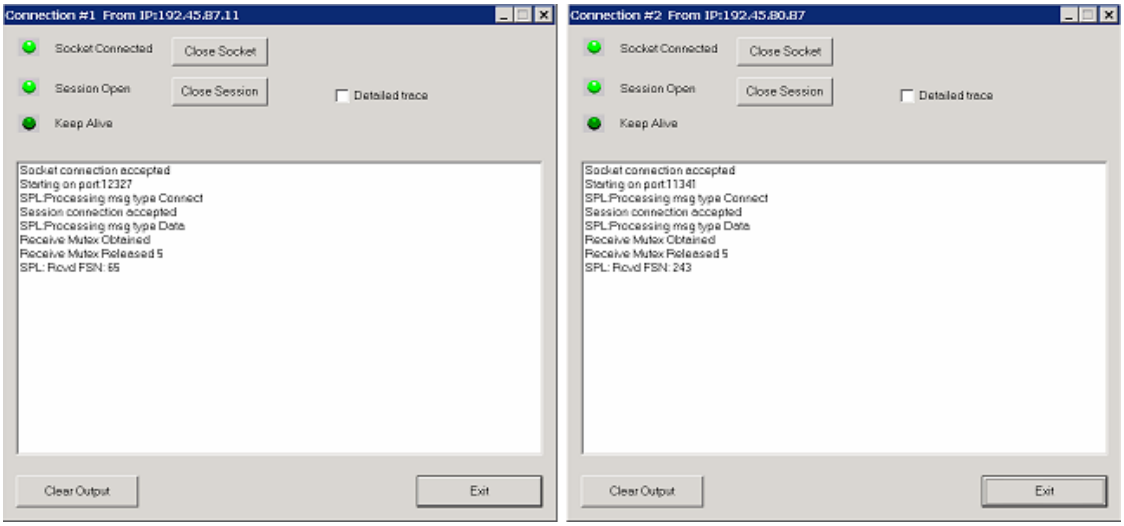
Additionally, the following settings were configured on the **System-Parameters Features** form, default settings were used except for those noted:

```
change system-parameters features                               Page   4 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
          Reserved Slots for Attendant Priority Queue: 5
                            Time before Off-hook Alert: 10
               Emergency Access Redirection Extension:
 Number of Emergency Calls Allowed in Attendant Queue: 5




  Deluxe Paging and Call Park Timeout to Originator? n
 Controlled Outward Restriction Intercept Treatment: tone
Controlled Termination Restriction (Do Not Disturb): tone
          Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS        Authorization Codes Enabled? y
                                       Authorization Code Length: 7
                            Authorization Code Cancellation Symbol: #
                                       Attendant Time Out Flag? n
                                    Display Authorization Code? y
              Controlled Toll Restriction Replaces: outward
    Controlled Toll Restriction Intercept Treatment: tone
```

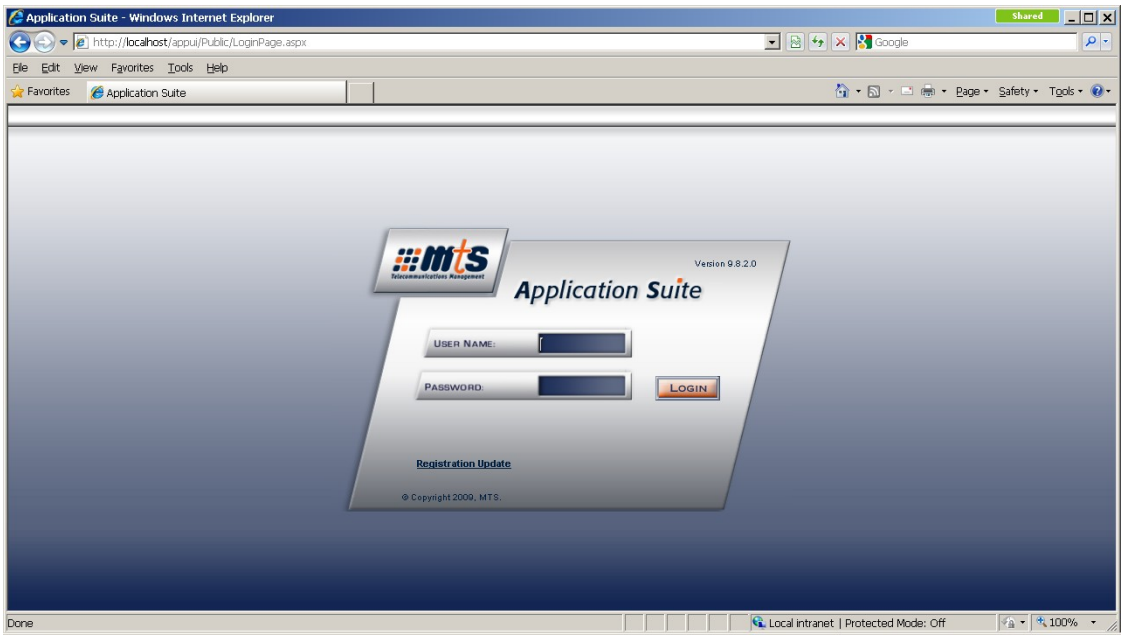

©2010 Avaya Inc. All Rights Reserved.

5. Configure Application Suite

This section describes the configuration of Application Suite. The Application Suite Server will listen for connections from each site using a modified version of the Avaya RDTT application. The following window will appear for each communication system that has established a connection to the server. This window will remain open and run in the background.

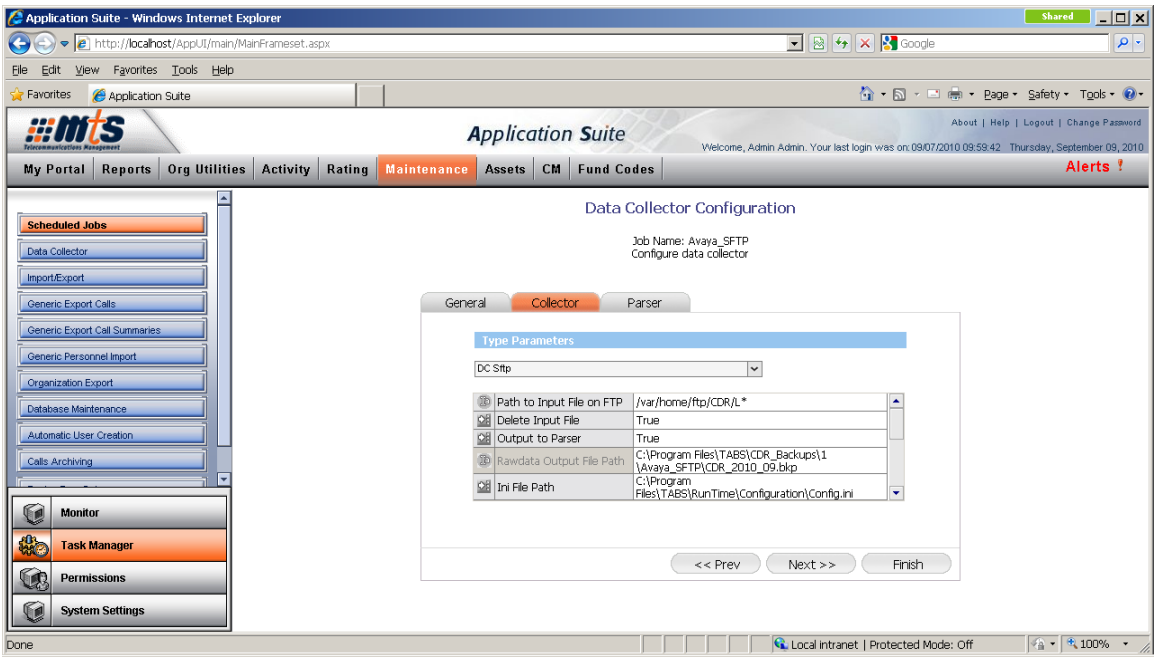


The Application Suite configuration and user interfaces are accessed via web browser at http://<ipaddress> where <ip address> is the name or address of the Application Suite server.



©2010 Avaya Inc. All Rights Reserved.

Users will see a number of tabs or modules according to which optional capabilities were purchased; the following illustrates.

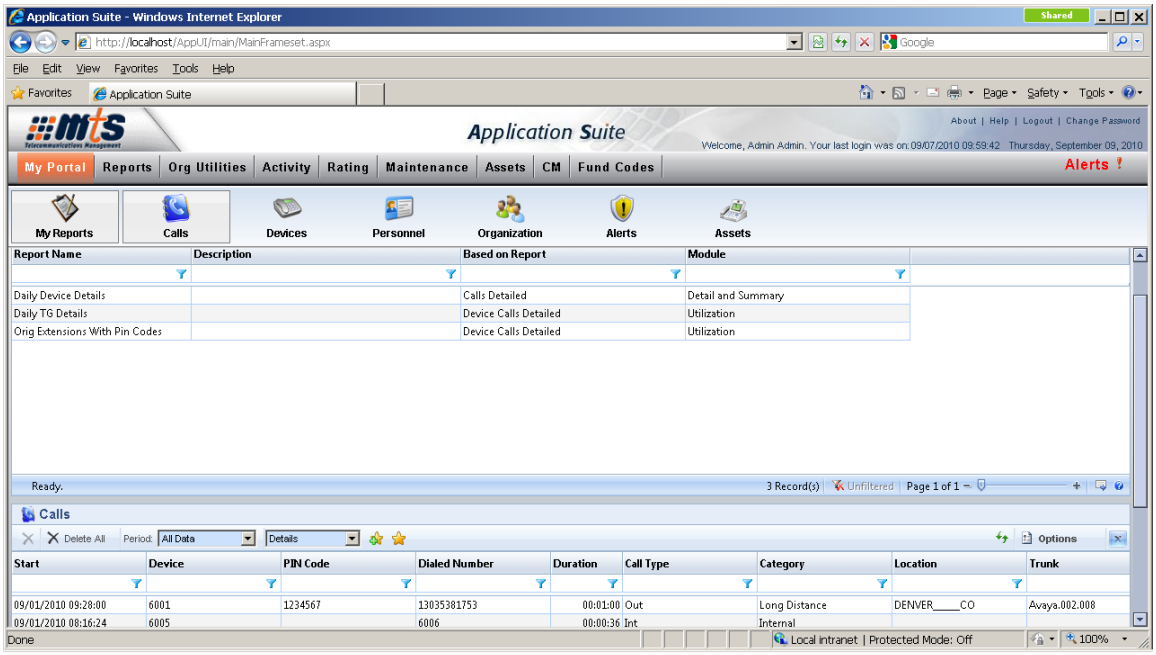


The maintenance module enables an authorized user to configure the Data Collectors or sources of data, including the RSP and FTP interfaces described in the Communication Manager configuration steps above.

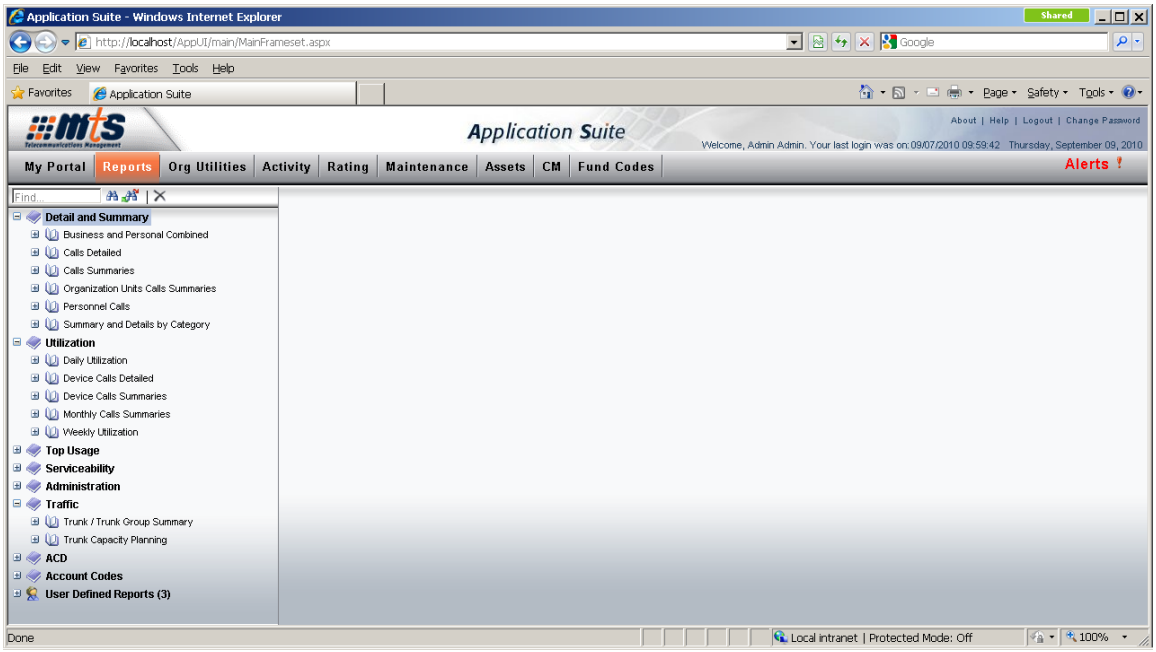
Additionally, the Application Suite is designed to be able to import and export data from a variety of sources, thus enabling large organizations to use LDAP or other data sources to feed organizational structure data to extend the usefulness of the solution.

©2010 Avaya Inc. All Rights Reserved.

Users access their scheduled reports, ad hoc reports, and can modify organizational data in the same browser window; actual information a user will have access to will be based on login, role and the organizational structures setup in the system. Following is a typical view a user might see:

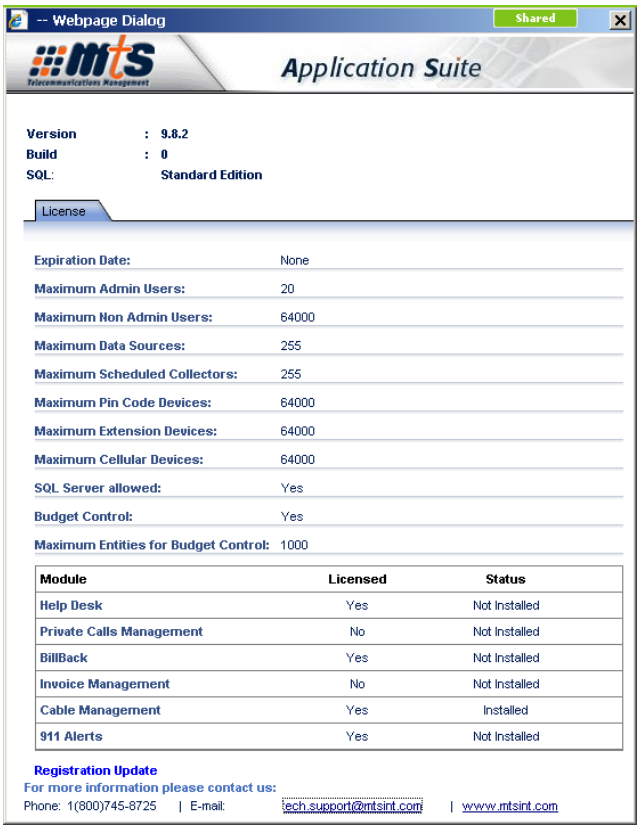


The Application Suite affords a variety of useful reports for managing the Enterprise. The following gives a sense of the broad range of reports available.



©2010 Avaya Inc. All Rights Reserved.

The Help/About screen provides version information, and also contains license configuration data.



©2010 Avaya Inc. All Rights Reserved.

6. General Test Approach and Test Results

The interoperability compliance testing included feature, serviceability, and an LSP test. The feature testing evaluated the ability of the Application Suite to collect and process CDR records for various types of calls. The serviceability testing introduced failure scenarios to see if the Application Suite could resume CDR collection after failure recovery. The Avaya LSP solution was tested by removing the **procr** Ethernet cable in the Avaya G450 Media Gateway.

The general test approach was to manually place intra-switch calls, inbound trunk and outbound trunk calls to and from telephones attached to the Avaya Servers, and to verify that the Application Suite collected the CDR records and properly classified and reported the attributes of the calls. For serviceability testing, physical and logical links were disabled/re-enabled, and media servers were reset.

All executed test cases passed. The Application Suite successfully collected the CDR records from Avaya Aura™ Communication Manager via a RSP connection for all types of calls generated including intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls. For serviceability testing, the Application Suite was able to resume collecting CDR records after failure recovery including buffered CDR records for calls that were placed during the outages.

The Application Suite also successfully collected the CDR records from the Avaya S8300 Server using the SFTP command.

7. Verification Steps

The following steps were used to verify the configuration:

- On the SAT of Communication Manager, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that the Application Suite received the CDR record for the call. Compare the values of data fields in the CDR record with the expected values and verify that the values match. A local instance of CDR link 2 terminating on a PC running Avaya RDTT collected identical records locally and was used to compare results to Application Suite reports.
- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in the Application Suite, and verify the report's accuracy.

8. Conclusion

These Application Notes describe the procedures for configuring Application Suite to collect call detail records from Avaya Aura™ Communication Manager running on Avaya Servers. The Application Suite successfully passed all compliance testing.

©2010 Avaya Inc. All Rights Reserved.

9. Additional References

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

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Release 6.0, Issue 8.0, June 2010, Document Number 555-245-205

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

A User Guide as well as additional documentation is available from MTS at www.mtsint.com.

©2010 Avaya Inc. All Rights Reserved.

©2010 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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

©2010 Avaya Inc. All Rights Reserved.