# Application Notes for TCC Atradis with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager – Issue 1.0

## Abstract

These Application Notes contain instructions for TCC Atradis with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager to successfully interoperate.

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

TCC Atradis VoIP Performance Management (PM) is a Real-Time Transport Control Protocol (RTCP) Monitoring tool which provides all the necessary features for VoIP performance management and monitoring. TCC Atradis VoIP PM collects Quality of Service (QoS) data such as jitter, delay, and packet loss. The Standard Edition includes a dashboard and an RTCP monitor.

In addition a System Monitor (Inventory Management Solution) add-on is available, which periodically collects data from Avaya Aura® Communication Manager via Avaya Aura® Application Enablement Services' (AES) System Management Service (SMS) interface. The data collected includes information for trunk measurements, station information, route pattern and so on.

# 2. General Test Approach and Test Results

Interoperability testing contained functional tests mentioned in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

## 2.1. Interoperability Compliance Testing

During Interoperability Compliance testing, several call routing scenarios were testing to ensure that Atradis is able to capture RTCP data. Atradis also has the ability to perform Inventory Management by using Avaya Aura® AES SMS interface, which was tested as well.

## 2.2. Test Results

All planned test cases were passed with the following exceptions:

- In a scenario where a SIP call is routed to another SIP gateway, Atradis displays A@0.0.0.0. This has been notified to Atradis and shall be fixed in a future release.

## 2.3. Support

Customers are served with support, depending on their service contract.
All service requests are sent to:
E-mail: service@atradis.net
Phone: +49 2202 9542 200

## 3. Reference Configuration

**Figure 1** illustrates a sample configuration that consists of Avaya Products and Atradis server. TCC Atradis was installed on a VMWare virtual appliance for Windows 2008 R2 server.

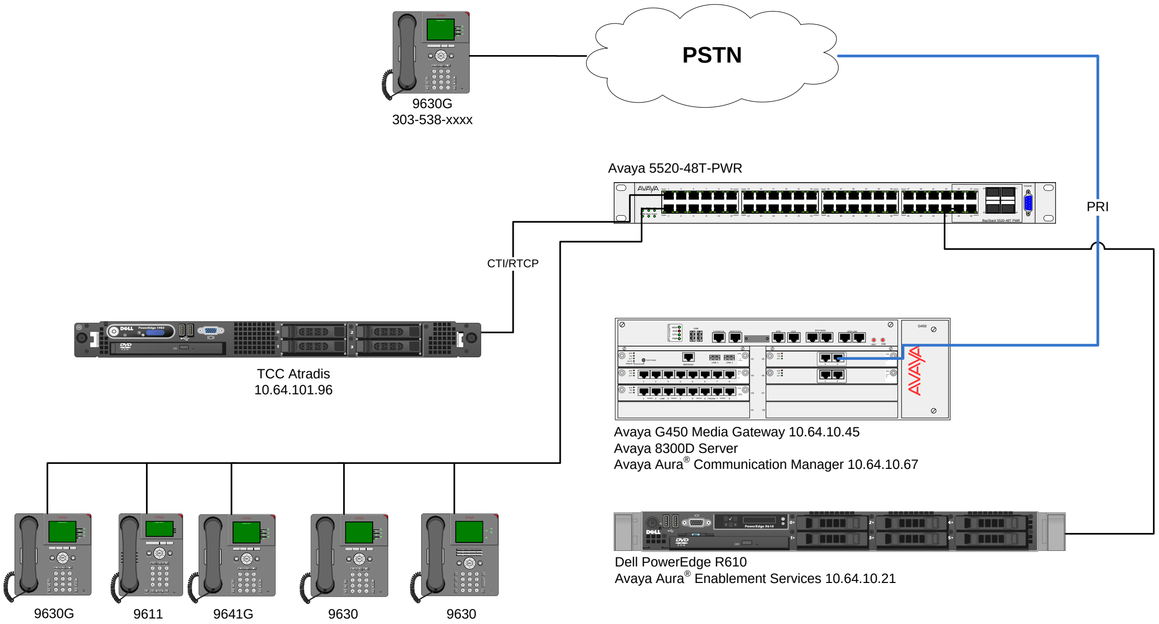


**Figure 1:** Test Configuration for TCC Atradis

# 4. Equipment and Software Validated

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

| **Equipment/Software** | **Release/Version** |
|---|---|
| Avaya S8300D Server<br>Avaya Aura®Communication Manager | R016x.03.0.124.0 |
| Avaya G450 Media Gateway | 31.20.0 |
| Avaya Aura® Application Enablement Services | 6.3 |
| TCC Atradis | 7.3.7.4.2.2 |

# 5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure TCC Atradis successfully with Avaya Aura® Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

## 5.1. Configure RTCP Monitoring

Use **change ip-network-region *n*** command to enable RTCP monitoring, where ***n*** is the IP network region that is used for routing calls. On Page 2:

- Set **RTCP Reporting Enabled** to **y**
- Set **Use Default Server Parameters** to **y**

```
change ip-network-region 1                                      Page   2 of  20
                               IP NETWORK REGION

 RTCP Reporting Enabled? y

 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? y
```

Use **change system-parameters ip-options** to configure the IP Address and port for RTCP traffic to send. On Page 1:

- Type in the IP Address of Atradis in **Server IPV4 Address**
- Type in the port where Atradis will receive RTCP traffic in **IPV4 Port**
- Set **RTCP Report Period(secs)** to **5**

```
change system-parameters ip-options                             Page   1 of   4
                          IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                    Packet Loss (%)     High: 40       Low: 15
                    Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10
                  Enable Voice/Network Stats? y
 RTCP MONITOR SERVER
   Server IPV4 Address: 10.64.101.94    RTCP Report Period(secs): 5
               IPV4 Server Port: 5005
   Server IPV6 Address:
               IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                    H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY                 Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5       Primary Search Time (sec): 75
                               Periodic Registration Timer (min): 20
                             Short/Prefixed Registration Allowed? n
```

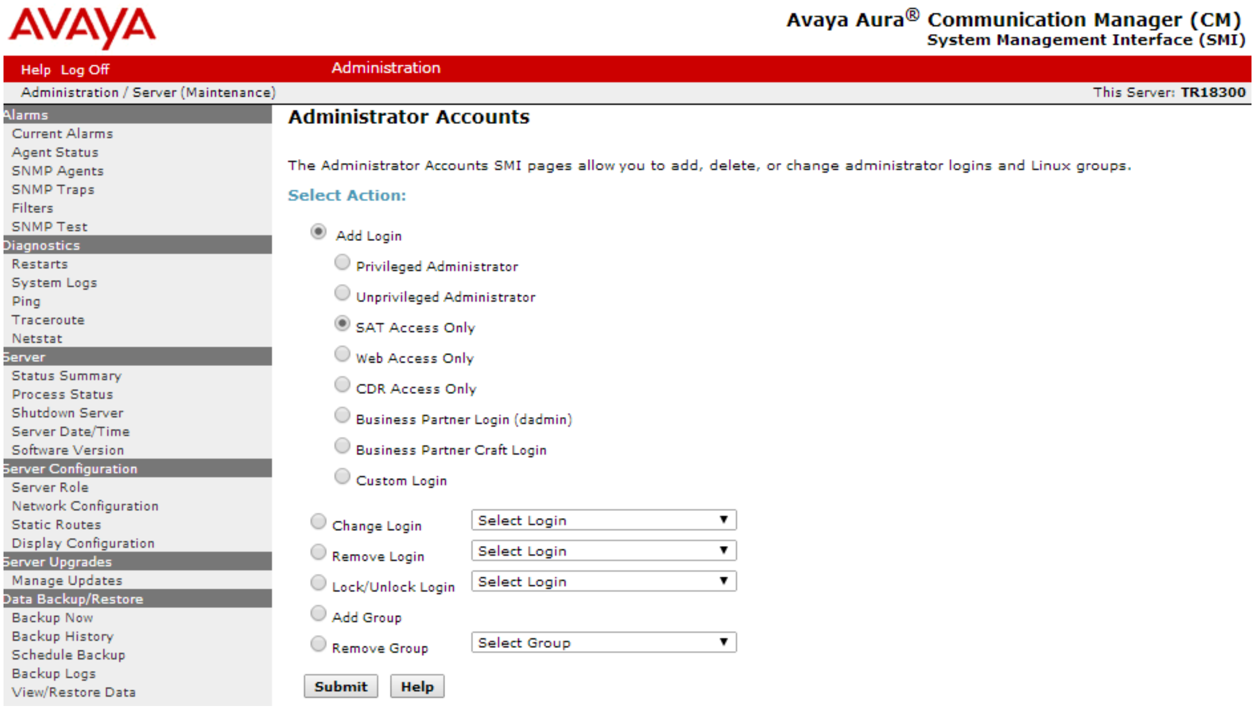
## 5.2. Configure SMS User

Atradis uses the Application Enablement Services SMS interface to gather inventory details.

A privileged user was used in this test; however, a local administrator would want to restrict the user account. User profile 18 was user during the compliance test.

```
list user-profiles

                                 USER PROFILES

                    Extended
    Profile          Profile     User Profile Name
      0                n         services super-user
      1                n         services manager
      2                n         business partner
      3                n         services
      16               n         call center manager
      17               n         snmp
      18               n         customer super-user
      19               n         customer non-super-user
      31               n         Call Center SMS
      32               n         SMS Read Only
```

Create a user account on the Communication Manager **System Management Interface** web page by navigating to the **Administer Accounts** page and selecting the radio button **Add Login**. For the Compliance Test, an account with **SAT Access Only** was used. Click **Submit** to continue the process.



**Administrator Accounts**

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

● Add Login
- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ● SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login ▼

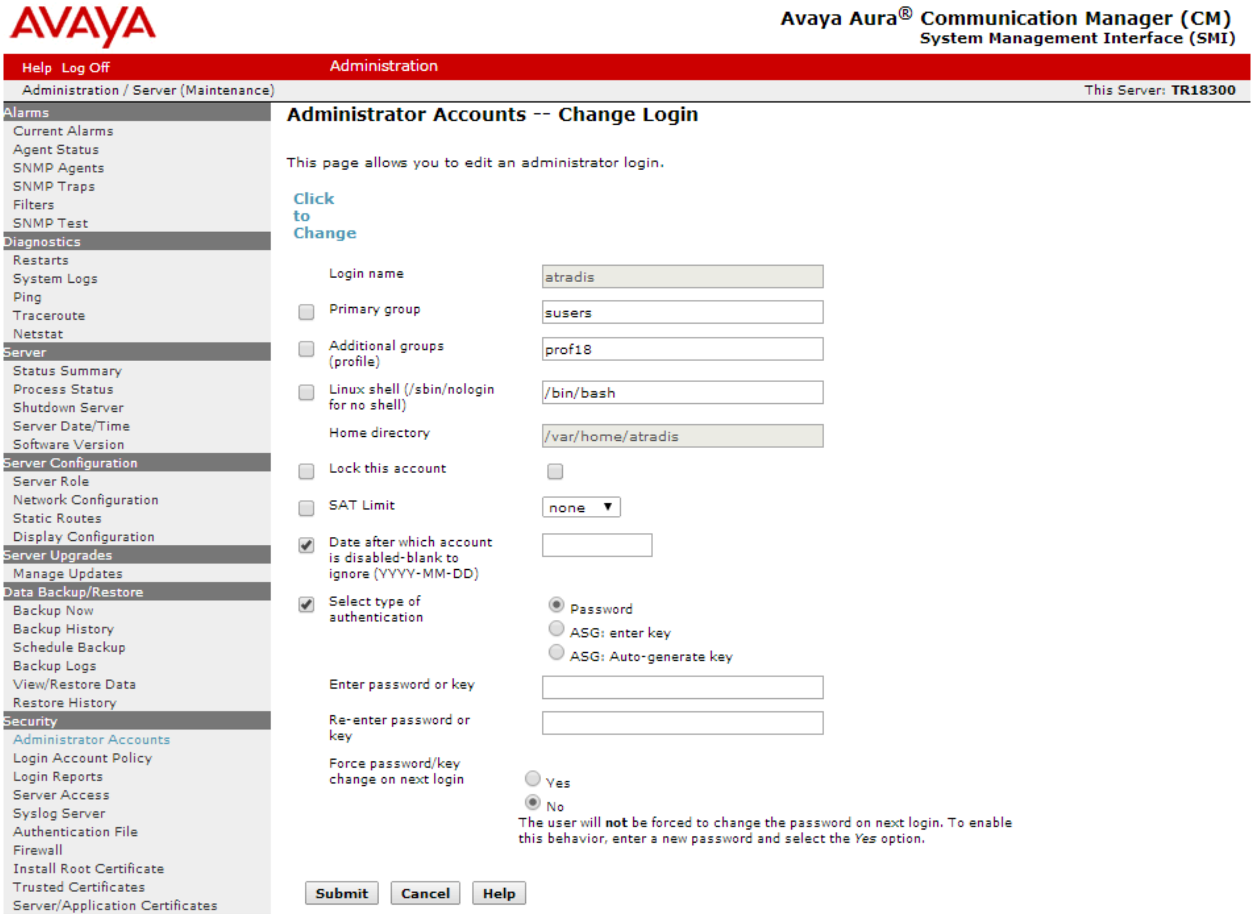
○ Remove Login — Select Login ▼

○ Lock/Unlock Login — Select Login ▼

○ Add Group

○ Remove Group — Select Group ▼

The account used for testing was previously created. The **Change Login** screen below shows the entries used when the account was created. The account was assigned to **Profile 18** defined in **Step 5** above, and a **Password** was created.



**Administrator Accounts -- Change Login**

This page allows you to edit an administrator login.

Click to Change

| | | |
|---|---|---|
| | Login name | atradis |
| □ | Primary group | susers |
| □ | Additional groups (profile) | prof18 |
| □ | Linux shell (/sbin/nologin for no shell) | /bin/bash |
| | Home directory | /var/home/atradis |
| □ | Lock this account | □ |
| □ | SAT Limit | none ▼ |
| ☑ | Date after which account is disabled-blank to ignore (YYYY-MM-DD) | |
| ☑ | Select type of authentication | ● Password<br>○ ASG: enter key<br>○ ASG: Auto-generate key |
| | Enter password or key | |
| | Re-enter password or key | |
| | Force password/key change on next login | ○ Yes<br>● No |

The user will **not** be forced to change the password on next login. To enable this behavior, enter a new password and select the *Yes* option.

## 5.3. Configure 46xxsetting.txt file

Set the following parameters in 46xxsetting.txt file for Avaya Endpoints:

```
SET RTCPMON <IP-Address>
SET RTCPMONPORT <Port>
SET RTCPMONPERIOD <Period>
```

Note: IP-Address and Port are values for Atradis. Set the period to the interval for RTCP packets to be sent by Avaya Endpoints
Once the parameters are changed, please reboot Avaya Endpoints.

# 6. Configure TCC Atradis voip-monitor.ini file

On the server where TCC Atradis is installed, edit the voip-monitor.ini file. This file is located in C:\Program Files\Atradis\image folder.

## 6.1. RTCP Monitor Server Settings

Configure the RTCP Monitor Server settings as follows:

- Set **logging** to **on**
- Set **Port** to **5005**. Please note that this value must match **IPV4 Port** configured in **Section 5.1**.
- Set **rtcpmonperiod** to the value set for **RTCP Report Period (sec)** in **Section 5.1.**

```
##
## RTCP Monitor Server Settings
##
[rtcp-monitor-server]

#
# RTCP Monitor Logging
#
#  Logs detailed progress and server performance information
#
# logging="off"
#

logging = "on"

#
# RTCP Monitor Silent Mode
#
#  Minimizes logging for installations where log file size
#  is an important consideration
#
# silent="off"
#

silent = "off"

#
# RTCP Monitor Network Address
#
#  An IP address in dotted-decimal format or a fully qualified domain name
#  in DNS name format.
#
#  This setting should be the same as the RTCPMON parameter used in
#  the Avaya IP-Telephone settings file, and in the ACM system-parameters
#  ip-options section.
#
#  The default value is "0.0.0.0", which means that the IP-Address of the first
#  available network interface is used
#
# address="0.0.0.0"
#
```

```
#
# RTCP Monitor Server Port
#
#  Sets the port on which RTCP information is received
#  on the IP address specified in the ADDRESS parameter.
#
#  This setting should be the same as the RTCPMONPORT parameter used in
#  the Avaya IP-Telephone settings file, and in the ACM system-parameters
#  ip-options section.
#
# port="5005"
#

port="5005"

#
# RTCP Monitor Report Period
#
#  Specifies the interval for sending out RTCP monitoring
#  reports ([5..30] seconds).  Default is 5 seconds.
#
#  This setting should be the same as the one used in the Avaya IP-Telephone
settings file,
# and in the ACM system-parameters ip-options section.
#
# rtcpmonperiod="5"
#

rtcpmonperiod="5"
```

## 6.2. RTCP Cleanup Server Settings

For compliance test, the following clean up values were set. These values may vary on customer requirements:

- `purge-after-days="90"`
- `scheduling-interval="day"`
- `scheduling-frequency="2"`
- `start-day-week="7"`
- `start-hour-day="0"`

```
##
## RTCP Cleanup Server Settings
##

[cleanup-server]

#
# Limit For Storing Archived QoS Data
#
#  Specifies the number of days that historical data is kept.
#  For legal reasons, the maximum value is limited to 90 days.
#
# purge-after-days="90"
#

purge-after-days="90"

#
# Scheduling Interval For Cleaning Archived QoS Data
#
#  The interval in which the cleanup takes place.
#  Allowed values are: "day" and "month"
#
# scheduling-interval="day"
#

scheduling-interval="day"

#
# Scheduling Frequency For Cleaning Archived QoS Data
#
#  The time to wait in terms of the scheduling interval,
#  before the cleaning of archived QoS data is started again.
#
#  If the scheduling-interval is set to "day" and scheduling
#  frequency is "14", then the cleanup takes place every two weeks.
#
#  The allowed values are [1..45] for interval "day",
#  and [1] for interval "month".
#
# scheduling-frequency="2"
#

scheduling-frequency="2"
```

```
#
# Day in Week For Cleaning Archived QoS Data
#
#  The day in the week [1..7] at which cleaning archived QoS data
#  should be started.The default value is 7 for Sunday.
#  If a server restart occurs, the next cleanup will wait until
#  the specified day in week has been reached.
#  In the worst case the waiting time is one week.
#
#  The service is then executed in the interval specified
#  by "scheduling-interval" and "scheduling frequency".
#
# start-day-week="7"
#

start-day-week="7"

#
# Hour in Day For Cleaning Archived QoS Data
#
#  The hour of the day [0..23] at which cleaning archived QoS data
#  should be started. The default value is 0 for Midnight.
#  A value of -1 indicates immediate execution at
#  the time the service is started, when the scheduled day in the
#  week has been reached.
#  If a server restart occurs, the next cleanup will wait until
#  the specified day in week and start hour has been reached.
#
#  The service is then executed in the interval specified
#  by "scheduling-interval" and "scheduling frequency".
#
# start-hour-day="0"
#

start-hour-day="0"
```

### 6.3. RTCP Hourly Statistics Server Settings

Configure the RTCP Hourly Statistics as follows:

- Set **scheduling-interval** to **hour**
- Set **scheduling-frequency** to **1**

```
##
## RTCP Hourly Statistics Server Settings
##

[hourly-statistics-server]

#
# Scheduling Interval For Calculating Hourly Statistics
#
#  The interval in which the calculation of hourly statistics
#  takes place.
#  Allowed values are: "minute" and "hour"
#
# scheduling-interval="hour"
#

scheduling-interval="hour"

#
# Scheduling Frequency For Calculating Hourly Statistics
#
#  The time to wait in terms of the scheduling interval,
#  before the calculation of hourly statistics is started again.
#
#  If the scheduling-interval is set to "hour" and scheduling
#  frequency is "1", then the cleanup takes place every hour.
#
#  The allowed values are [1..24] for interval "hour",
#  and [1..1440] for interval "minute".
#
# scheduling-frequency="1"
#

scheduling-frequency="1"

#
# Hour in Day For Calculating Hourly Statistics
#
#  The hour of the day [0..23] at which calculation of hourly statistics
#  should be started.
#  If a server restart occurs, the next calculation of hourly statistics
#  will wait until the specified hour of the has been reached.
#  In the worst case the waiting time is one day.
#
#  A value of -1 indicates immediate execution at
#  the time the service is started.
#  The default value is "-1".
#
```

# 7. Configure Atradis System Monitor

For a system with new installation, the following needs to be configured:

- Configure Scanjob-server
- Configure Web Server

## 7.1. Configure Scanjob-server

Locate the startsrv.cfg file in the installation directory for Atradis. During the compliance test, the file was located under c:\Program Files\Atradis\Server01 folder. Settings in this file will vary depending on customer configuration. Open the file and change as follows:

- Set **dbEnvironment** to the Service name of Oracle Database,  default value is **nsm**
- Set **databaseOwner** to the Oracle Database name, default value is  **atradis**
- Activate import function by setting **import** to **1**
- Activate scan function of Scanjob-server by setting **scan** to **1**
- Enable Scanjob-server by setting **server** to **1**
- Turn on debugging for traces, if needed, by setting **trace** to **8**

```
checkOnline 0
config 0
dbEnvironment nsm
databaseOwner atradis
import 1
scan 1
server 1
importSysLog 0
sysLog 0
importSnmpTrap 0
monitor 0
monitorO 0
scanServerLog log1.txt
sysLogPort 514
trace 8
pingFirst 1
sensorTree 0
slotNo 1024
csExtend 1
serviceStart 7
serviceEnd 17
```

## 7.2. Configure Web Server

To configure the Web Server for Atradis, there are two configuration files that need to be edited.

### 7.2.1. Configure Apache

In the Apache installation directory, c:\Program Files\Apache Software Foundation\Apache2.2\conf\, edit http.conf file and add the following line:

**Include "c:\Programme\Atradis\web\conf\ssl\ssl.conf"**

### 7.2.2. Configure Atradis Webserver Config-File (webserver-01.cfg)

In the Atradis installation directory, c:\Program Files\Atradis\Web, edit webserver-1.cfg and configure as follows:

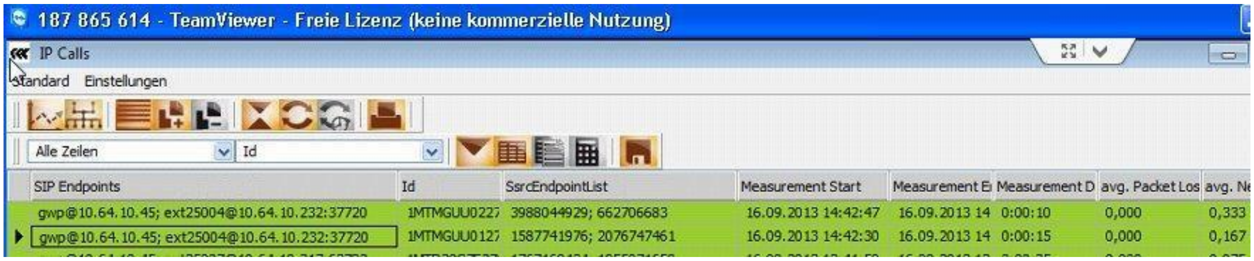
- Set **environment** to the service name of Oracle Database, default value is **nsm**
- Set **systables** to the Atradis user in Oracle Database, default user is **#atradis**
- Set **serverName** to the external Hostname of WebServer

```
[Local]
environment="nsm"
batchSize="20"
serverPort="8001"
database="oracleWithBill"
OracleLib="oci.dll advapi32.dll"
language="en_US.CP1252"
pidFileDir="c:\Programme\Atradis\web\pdf"
startupDelay="0"
haruLibraryDirectory="web"
adminMail="service@atradis.net"

[External]
serverName="vm-xp-02.email.local"
serverPort="443"
serverProtocol="https"

[Database]

systables="#atradis"
```

# 8. Verification steps

## 8.1. Atradis

To verify, Atradis is configured properly, place a call from an extension and keep it up for at least 10 seconds. Open the Atradis console, and verify that Atradis is able to capture the RTCP packets and display the in information correctly.



187 865 614 - TeamViewer - Freie Lizenz (keine kommerzielle Nutzung)
IP Calls
Standard
Einstellungen
Alle Zeilen
Id

| SIP Endpoints | Id | SsrcEndpointList | Measurement Start | Measurement E | Measurement D | avg. Packet Los | avg. Ne |
|---|---|---|---|---|---|---|---|
| gwp@10.64.10.45; ext25004@10.64.10.232:37720 | 1MTMGUU0227 | 3988044929; 662706683 | 16.09.2013 14:42:47 | 16.09.2013 14 | 0:00:10 | 0,000 | 0,333 |
| gwp@10.64.10.45; ext25004@10.64.10.232:37720 | 1MTMGUU0127 | 1587741976; 2076747461 | 16.09.2013 14:42:30 | 16.09.2013 14 | 0:00:15 | 0,000 | 0,167 |

# 9. Conclusion

TCC Atradis was able to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

# 10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, December 2013, Release 6.3, Document Number 03-300509.

[2] *Administering Avaya® Session Manager*, October 2013, Release 6.3, Issue 3

[3] *Administering Avaya® System Manager*, October 2013, Release 6.3.Issue 3

Documentation related to TCC Atradis can be obtained directly from TCC.

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.