



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for 2Ring Mediator with Avaya Communication Manager – Issue 1.0**

### **Abstract**

These Application Notes describe the compliance testing of 2Ring Mediator with Avaya Communication Manager and Avaya Application Enablement Services. The Mediator product provides a standardized interface to client programs, irrespective of its telecommunication environment, thus allowing CTI applications to run with telephone switches from various manufactures without modification. These Application Notes contain an extensive description of the configurations for 2Ring Mediator, Avaya Communication Manager, Avaya Application Enablement Services which were used for testing. The testing which was performed tested the major functions of the 2Ring Mediator product.

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

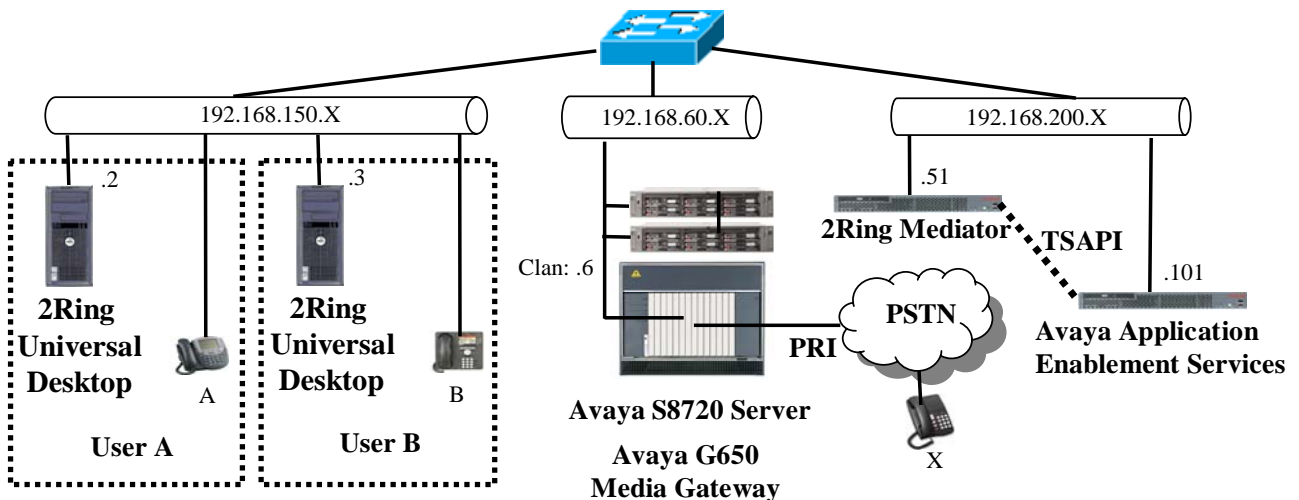
# Table of Contents

<b>1. Introduction.....</b>	<b>3</b>
<b>2. Equipment and Software Validated.....</b>	<b>4</b>
<b>3. Configuration.....</b>	<b>4</b>
3.1. Configure Avaya Communication Manager.....	5
3.1.1. Verify Customer Options.....	5
3.1.2. Configure Stations.....	8
3.1.3. Configure Agent Login.....	8
3.1.4. Configure CTI Link.....	9
3.2. Configure Avaya AES.....	10
3.3. Configure 2Ring Mediator Server.....	14
3.4. Configure 2Ring Unversal Desktop Clients.....	19
<b>4. Interoperability Compliance Testing.....</b>	<b>24</b>
4.1. General Test Approach.....	24
4.2. Test Results.....	25
<b>5. Verification Steps.....</b>	<b>25</b>
<b>6. Support.....</b>	<b>25</b>
<b>7. References.....</b>	<b>26</b>
<b>8. Conclusion.....</b>	<b>26</b>

# 1. Introduction

These Application Notes describe the configuration used to enable the 2Ring Mediator to interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES). The Mediator product provides a standardized interface to client programs, each of which supports one Automatic Call Distribution (ACD) agent, irrespective of which telecommunication environment it is working in, thus allowing CTI applications to run with telephone switches from various manufactures without modification.

The Clients can run various application programs, such as a call center agent interface or customer relationship management system. For the testing described by these application notes, the 2Ring Universal Desktop client included in the 2Ring Mediator software distribution was used. This is a simple client application which allows the client to perform telephony operations, and respond to telephony events.



**Figure 1: Mediator Test Configuration**

In the above diagram the client application, in this case 2Ring Universal Desktop, informs the 2Ring Mediator server of telephony operations which are to be performed, such as making a call. 2Ring Mediator uses the TSAPI interface to instruct AES to perform the required telephony operations. As status changes occur, AES provides 2Ring Mediator with TSAPI events which inform Mediator of those changes. 2Ring Mediator subsequently informs the client application of changes.

The following table contains details about the telephones which were used for testing. Note that the “xxxxx” and “yyyy” sequences represent digit strings for public numbers which were used for testing.

Phone	Model	Extension	Agent ID	Desktop ID	PSTN
A	4620SW IP	60121	61621	UD1	069 907 xxxxxx 61621
B	9640	60093	61622	UD2	069 907 xxxxxx 61622
X					069 yyyy 6174

**Table 1: Extensions Used for Testing**

## 2. Equipment and Software Validated

Software Component	Platform	Version
Avaya Communication Manager	Avaya S8720 Server	R015x.01.1.415.1
Avaya Application Enablement Services	Avaya S8720 Server	r4-2-1-20-5-0
Avaya TN2312BP IP Server Interface	Avaya S8720 Server	HW15/FW042
Avaya TN799DP Control LAN	Avaya G650 Gateway	HW01/FW026
Avaya TN2302AP Media Processor	Avaya G650 Gateway	HW20/FW033
Avaya TN2464CP DS1 Interface	Avaya G650 Gateway	HW01/FW19
Avaya 9640 IP Telephone		2.00
Avaya 4620 SW IP Telephone		2.887
Microsoft .Net Framework	Mediator Server	2.0.50727.42
Platform OS	Mediator Server	MSWIN 2003 SP2
2Ring Mediator	Mediator Server	2.0
Platform OS	Mediator Client	MS XP SP3
2Ring Universal Desktop	Mediator Client	2.0

**Table 2: Hardware/Software Component Versions**

## 3. Configuration

These Application Notes describe the configuration of the following components:

- Avaya Communication Manager
- Avaya Application Enablement Services
- 2Ring Mediator server
- 2Ring Universal Desktop

### 3.1. Configure Avaya Communication Manager

The configuration and verification operations illustrated in this section were all performed using the Avaya Communication Manager System Administration Terminal (SAT).

The information provided in this section describes the configuration of Avaya Communication Manager for this solution. For all other provisioning information such as installation and configuration, please refer to the product documentation in references [1] and [2].

The configuration of the interface to the PSTN and for the routing of calls to and from the PSTN is not described within these application notes.

#### 3.1.1. Verify Customer Options

Use the **display system-parameters customer options** command to verify that Avaya Communication Manager is provisioned to meet the minimum requirements to run Mediator. Those items shown in **bold** indicate required values or minimum capacity requirements. If these are not met in the configuration, please contact an Avaya representative for further assistance.

Parameter	Usage
Maximum Concurrently Registered IP Stations (page 2)	This must be sufficient to support the total number of IP stations. This is only required if IP stations are included in the configuration. Other station types can also be used.
Computer Telephony Adjunct Links? (page 3)	This parameter must be set to “y”.
IP Stations? (page 4)	This parameter must be set to “y”.
IP_Phone (page 10)	This parameter must be set to accommodate the number of IP stations to be used.

**Table 3: System-Parameters Customer-Options Parameters**

```

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

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 100 60
      Maximum Concurrently Registered IP Stations: 12000 4
      Maximum Administered Remote Office Trunks: 0 0
Maximum Concurrently Registered Remote Office Stations: 0 0
      Maximum Concurrently Registered IP eCons: 10 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: 1000 255
Maximum Administered Ad-hoc Video Conferencing Ports: 0 0
      Maximum Number of DS1 Boards with Echo Cancellation: 10 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 0
      Maximum Number of Expanded Meet-me Conference Ports: 0 0

```

**Figure 2: System-Parameters Customer-Options Screen, page 2**

```

display system-parameters customer-options                               Page 3 of 11
                                OPTIONAL FEATURES

      Abbreviated Dialing Enhanced List? n      Audible Message Waiting? n
      Access Security Gateway (ASG)? n          Authorization Codes? y
      Analog Trunk Incoming Call ID? n          CAS Branch? n
      A/D Grp/Sys List Dialing Start at 01? n  CAS Main? n
      Answer Supervision by Call Classifier? n  Change COR by FAC? n
      ARS? y      Computer Telephony Adjunct Links? y
      ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? n
      ARS/AAR Dialing without FAC? n          DCS (Basic)? n
      ASAI Link Core Capabilities? y          DCS Call Coverage? n
      ASAI Link Plus Capabilities? y          DCS with Rerouting? n
      Async. Transfer Mode (ATM) PNC? n
      Async. Transfer Mode (ATM) Trunking? n  Digital Loss Plan Modification? n
      ATM WAN Spare Processor? n              DS1 MSP? n
      ATMS? n      DS1 Echo Cancellation? y
      Attendant Vectoring? n

```

**Figure 3: System-Parameters Customer-Options Screen, page 3**

```

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? n
  Enhanced EC500? y                                               ISDN/SIP Network Call Redirection? y
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)? n
  Hospitality (Basic)? y                                           Multimedia Call Handling (Enhanced)? n
Hospitality (G3V3 Enhancements)? n                                Multimedia IP SIP Trunking? n
  IP Trunks? y

IP Attendant Consoles? y

```

**Figure 4: System-Parameters Customer-Options Screen, page 4**

```

display system-parameters customer-options                               Page 10 of 11
                                MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit      Used
IP_API_A   : 1000      0
IP_API_B   : 1000      0
IP_API_C   : 1000      0
IP_Agent   : 1000      0
IP_IR_A    : 1000      0
IP_Phone  : 12000    4
IP_ROMax   : 12000     0
IP_Soft    : 1000      0
IP_eCons   : 128       0
oneX_Comm  : 12000     0

```

**Figure 5: System-Parameters Customer-Options Screen page 10**

### 3.1.2. Configure Stations

Use the **add station** command to create IP stations for extensions A and B, as shown in **Table 1**.

Parameter	Usage
Extension	Use an unused extension which is compatible with the dial plan.
Type	Use a type value which corresponds to the physical station to be used.
Name	Any alphanumeric string can be assigned as an extension name, which is used for identification purposes.
Security Code	Enter an appropriate numeric string to be used as a security code.

**Table 4: Configuration IP Stations**

```

add station 60121                                     Page 1 of 5
                                                    STATION
Extension: 60121                                Lock Messages? n                BCC: 0
Type: 4620                                     Security Code: xxxxxx        TN: 1
Port: S00101                                       Coverage Path 1: 1              COR: 1
Name: extn 60121                               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: 60121
Speakerphone: 2-way                               Mute Button Enabled? y
Display Language: english
Survivable GK Node Name:
Survivable COR: internal                          Media Complex Ext:
Survivable Trunk Dest? y                          IP SoftPhone? n
                                                    Customizable Labels? y
  
```

**Figure 6: IP Station Screen**

### 3.1.3. Configure Agent Login

Use the **add agent-loginID** command to create agent logins for agents at stations A and B, as shown in **Table 1**.

Parameter	Usage
Name	Use the “Desktop ID” shown in <b>Table 1</b> as the agent name.
Password	Specify a string up to 9 digits long to be used as the agent password. This value is configured for Mediator in <b>Figure 16</b> .
Password (enter again)	Repeat the above parameter.

**Table 5: Agent LoginID Parameters**



```

add agent-loginID 61621                                     Page 1 of 2
                  AGENT LOGINID

Login ID: 61621                                           AAS? n
  Name: UD1                                               AUDIX? n
  TN: 1                                                   LWC Reception: spe
  COR: 1                                                  LWC Log External Calls? n
Coverage Path:                                           AUDIX Name for Messaging:
Security Code:

LoginID for ISDN/SIP Display? n
  Password: 123456
  Password (enter again): 123456
  Auto Answer: station
  MIA Across Skills: system
  ACW Agent Considered Idle: system
  Aux Work Reason Code Type: system
  Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time: :

WARNING: Agent must log in again before changes take effect

```

**Figure 7: Agent-LoginID Form, page 1**

### 3.1.4. Configure CTI Link

Use the **add cti-link** command to add a CTI link for use by TSAPI. The link number can be any value between 1 and 64 which is not currently assigned to another link. Use an unused extension as the value for the “Extension” parameter. The value chosen for the “Name” parameter is a matter of personal preference. A link type of “ADJ-IP” must be specified.

```

add cti-link 4                                           Page 1 of 3
                  CTI LINK

CTI Link: 4
Extension: 69996
Type: ADJ-IP
Name: AES-devcon223-tsapi
COR: 1

```

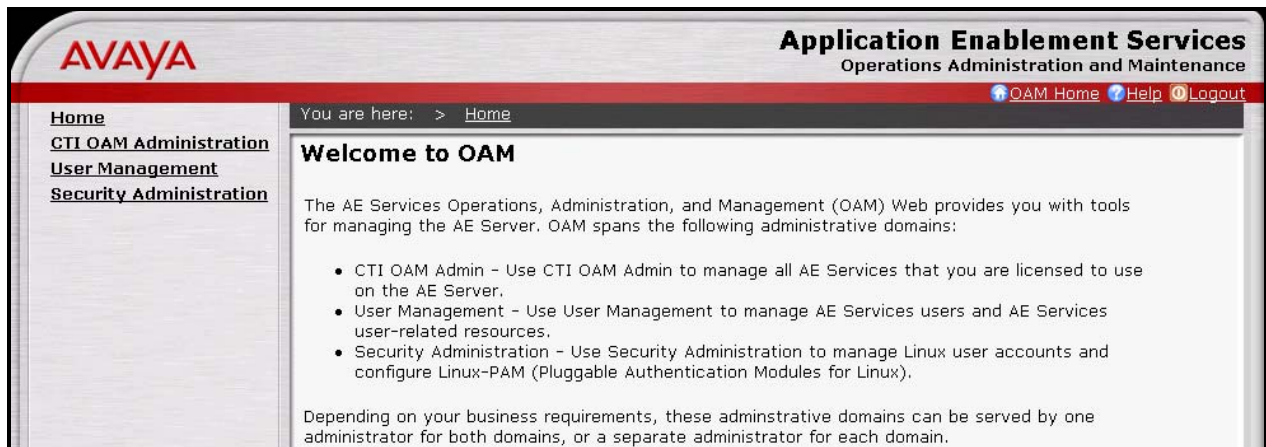
**Figure 8: Cti-link Screen**

## 3.2. Configure Avaya AES

The AES server is configured via a web browser by accessing the following URL:

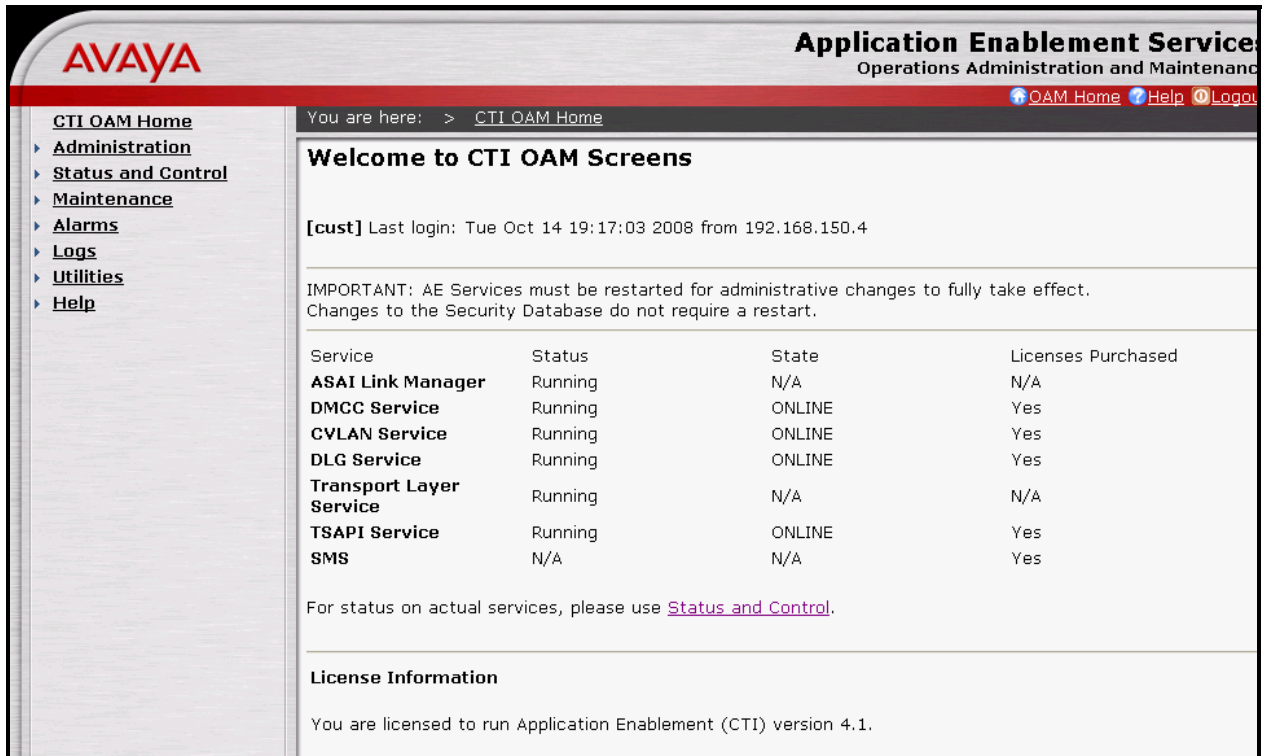
`https://<AES server address>/MVAP/`

Once the login screen appears, enter either the appropriate login credentials.



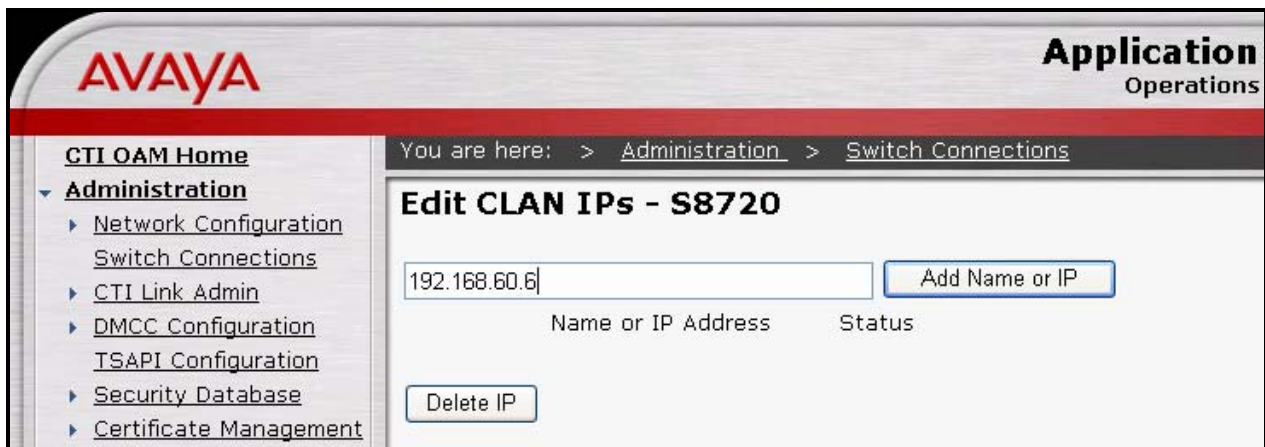
**Figure 9: AES Welcome Screen**

After logging in, select “CTI OAM Admin” which displays the following screen. Verify that the AES server installation has a TSAPI service license. If this is not the case, please contact an Avaya representative regarding licensing.



**Figure 10: AES CTI OAM Welcome Screen**

From the **Administration->Switch Connections** screen, click the “Edit CLAN IPs” button to display the screen shown below. Enter the IP address of the CLAN with which AES is to use for communication with the switch, and click the “Add Name or IP” button.



**Figure 11: CLAN Screen**

On the left margin of the screen, navigate to **Administration->CTI Link Admin->TSAPI Links**. The following screen is displayed. Click the “Add Link” button.



**Figure 12: TSAPI Links Screen**

Fill in the parameters for the link to be added. The “Link” parameter must be a value between 1 and 16 which is not assigned to another link. The value for the TSAPI “Switch CTI Link Number” must be a value between 1 and 64, and must be the same as was used in the Avaya Communication Manager “add cti-link” configuration command in **Figure 8**. Retain the default values in the remaining fields. Click the “Apply Changes” button.



**Figure 13: Add TSAPI Link Screen**

Click “OAM Home” on the menu bar and Navigate to **User Management->Add User**.

Although the “Common Name” and “Surname” fields are required, any text string can be used as content.

Enter an appropriate User Id and Password to serve as the user’s credentials.

The “CT User” field for this user must be set to “Yes”. In this case, the AES user is the Mediator application, which uses AES to monitor stations and initiate TSAPI telephony operations.

**AVAYA** Application Operations

You are here: > User Management > Add User

### Add User

Fields marked with \* can not be empty.

\* User Id

\* Common Name

\* Surname

\* User Password

\* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

**Figure 14: Add User Screen**

### 3.3. Configure 2Ring Mediator Server

After installing the 2Ring Mediator software on the server, use an ASCII editor to edit the “C:\Program Files\2Ring\Mediator Controller\Service\Modules\Cpm\MediatorConfig.xml” file. For each of the Mediator clients shown in **Table 1**, edit or add “<module>” entries using the parameters shown in the table below.

Parameter	Usage
<name>	Enter the Desktop ID to be assigned to the client, as shown in <b>Table 1</b> .
<address>	Enter the IP address of the client PC.
<port>	Enter the port used by the client.

**Table 6: Client Module Parameters**

```

<?xml version="1.0" encoding="utf-8" ?>
<!-- Config file for Mediator -->
<config>
  <name>mediator</name>
  <debug>3</debug>
  <port>8008</port>
  <specific>
    <transformation>
      <uri>CoreTraffic.xslt</uri>
    </transformation>
    <modules>
      <module>
        <name>UD1</name>
        <address>192.168.150.2</address>
        <port>8036</port>
      </module>
      <module>
        <name>UD2</name>
        <address>192.168.150.3</address>
        <port>8036</port>
      </module>
      <module>
        <name>AvayaBridge</name>
        <address>127.0.0.1</address>
        <port>8083</port>
      </module>
    </modules>
  </specific>
</config>

```

**Figure 15: Controller\Service\Modules\Cpm\MediatorConfig.xml Configuration File**

Use an ASCII editor to edit the “C:\Program Files\2Ring\Mediator Controller\Service\Modules\Cpm\Mappings.xslt” file. For each of the clients included in the configuration, change entries within the sections shown in the table below.

Section within File	Usage
<pre>&lt;xsl:template name="extensionToUI"&gt;   &lt;xsl:param name="extension" /&gt;   &lt;xsl:choose&gt;</pre>	<p>There must be one entry within this section for each agent, with the agent’s Extension and as shown in <b>Table 1</b>. Desktop ID must match the value of “name” element in configuration file shown in <b>Figure 15</b> for that module entry, which contains connection parameters of respective client.</p>
<pre>&lt;xsl:template name="extensionToId"&gt;   &lt;xsl:param name="extension" /&gt;   &lt;xsl:choose&gt;</pre>	<p>There must be one entry within this section for each agent, with the agent’s Extension and Agent ID, as show in <b>Table 1</b>. The agent “Extension” is assigned in <b>Figure 6</b>, and the agent “Login ID” in <b>Figure 7</b>.</p>
<pre>&lt;xsl:template name="extensionToPassword"&gt;   &lt;xsl:param name="extension" /&gt;   &lt;xsl:choose&gt;</pre>	<p>There must be one entry within this section for each agent, with the agent’s Extension and Agent Password, as show in <b>Figure 7</b>.</p>

**Table 7: Service\Modules\Cpm\ Mappings.xslt Parameters**

```
<?xml version="1.0" encoding="utf-8"?>

<xsl:stylesheet version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
<xsl:template name="extensionToUI">
  <xsl:param name="extension" />
  <xsl:choose>
    <xsl:when test="contains($extension,'60121')">UD1</xsl:when>
    <xsl:when test="contains($extension,'60093')">UD2</xsl:when>
  </xsl:choose>
</xsl:template>
<xsl:template name="extensionToId">
  <xsl:param name="extension" />
  <xsl:choose>
    <xsl:when test="contains($extension,'60121')">61621</xsl:when>
    <xsl:when test="contains($extension,'60093')">61622</xsl:when>
  </xsl:choose>
</xsl:template>

<xsl:template name="extensionToPassword">
  <xsl:param name="extension" />
  <xsl:choose>
    <xsl:when test="contains(.,'60121')">123456</xsl:when>
    <xsl:when test="contains(.,'60093')">123456</xsl:when>
  </xsl:choose>
</xsl:template>
```

**Figure 16: Service\Modules\Cpm\ Mappings.xslt Configuration File**



Use an ASCII editor to edit the “C:\Program Files\2Ring\Mediator Controller\Service\Modules\AvayaBridge\TsapiBridgeConfig.xml” file. Change entries within the sections shown in the table below.

Section within File	Usage
<config><specific><identity><server>	Enter the TSAPI tlink name, which can be on AES under Administration/Security Database/Tlinks, as shown in <b>Figure 17</b> .
<config><specific><identity><user>	Enter the user name configured in <b>Figure 14</b> .
<config><specific><identity><password>	Enter the user password configured in <b>Figure 14</b> .
<config><specific><monitoredDevices>	Make a “deviceId” entry for each agent with the value of the agent’s extension (allocated in <b>Figure 6</b> ), as shown in <b>Table 1</b> .

**Table 8: Service\Modules\Cpm\ Mappings.xslt Parameters**



**Figure 17: AES Tlinks Screen**

```

<?xml version="1.0" encoding="utf-8" ?>
<!-- Config file for Tsapi bridge module -->
<config>
  <name>tsapi</name>
  <debug>3</debug>
  <port>8083</port>
  <bufferSize>8192</bufferSize>
  <mediator>
    <address>127.0.0.1</address>
    <port>8008</port>
  </mediator>
  <specific>
    <workerThreadsCount>3</workerThreadsCount>
    <identity>
      <server>AVAYA#S8720#CSTA#AES-SERVER1</server>
      <user>Mediator</user>
      <password>2Ring-password</password>
      <version>TS1-2</version>
    </identity>
    <monitoredDevices>
      <deviceId>60121</deviceId>
      <deviceId>60093</deviceId>
    </monitoredDevices>
  </specific>

```

**Figure 18: Service\Modules\AvayaBridge\TsapiBridgeConfig.xml Configuration File**



Restart the server and use the MS “Services” applet from the Windows “Control” panel to verify that the “Mediator Controller” service is running.

Name ▲	Description	Status	Startup Type
 Mediator Controller	Mediator Manager Server	Started	Automatic

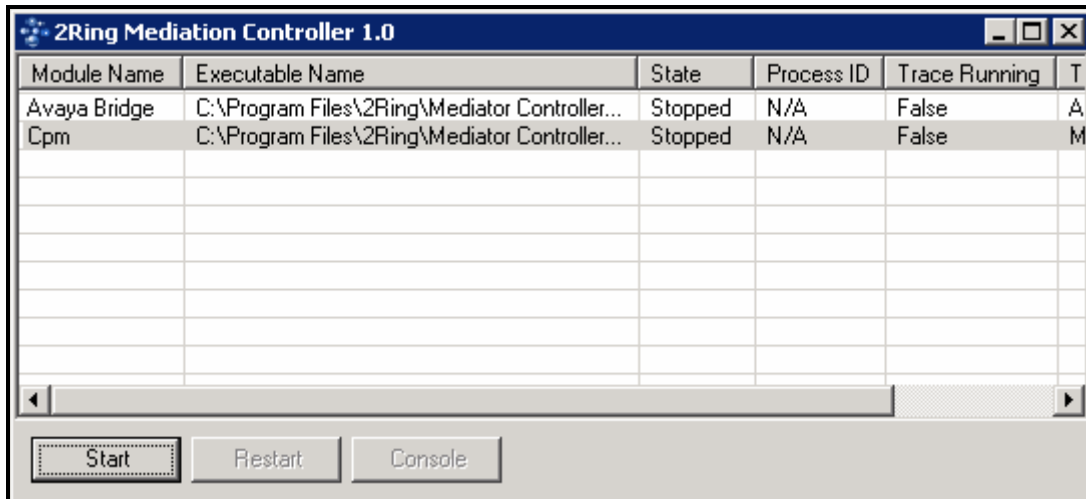
**Figure 19: Mediator Controller Service Status**

Double click the “Mediator Controller UI” icon on the server desktop.



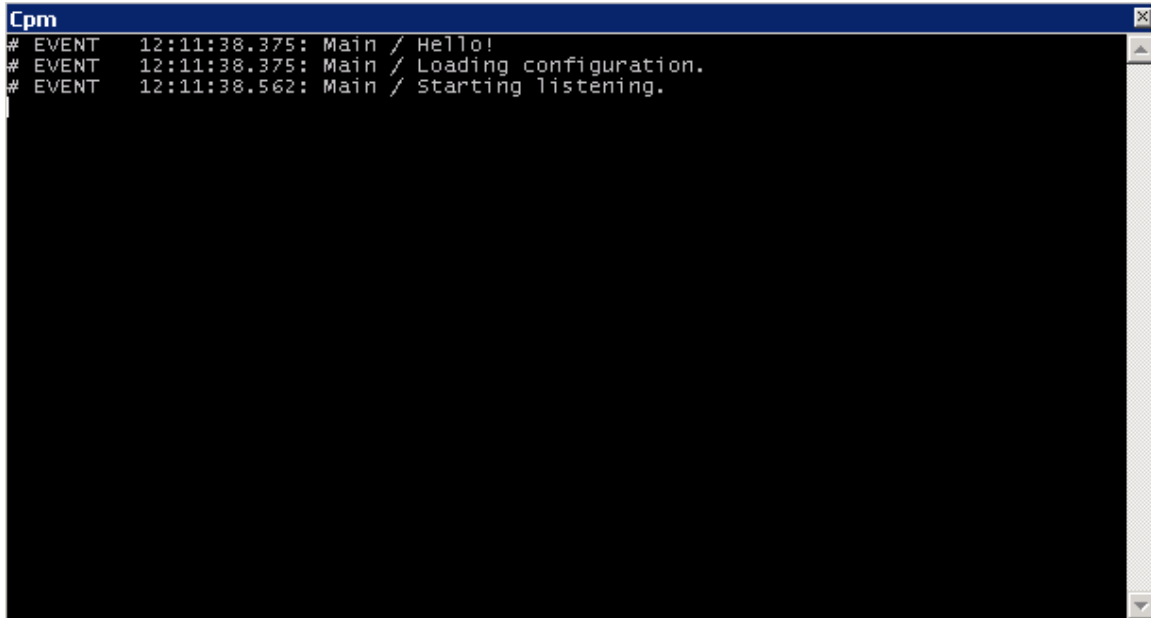
**Figure 20: “Mediator Controller UI” Server Icon**

The Mediator Controller User Interface is now displayed on the screen. Select “Cpm” and then “Start”.



**Figure 21: Mediator Controller User Interface**

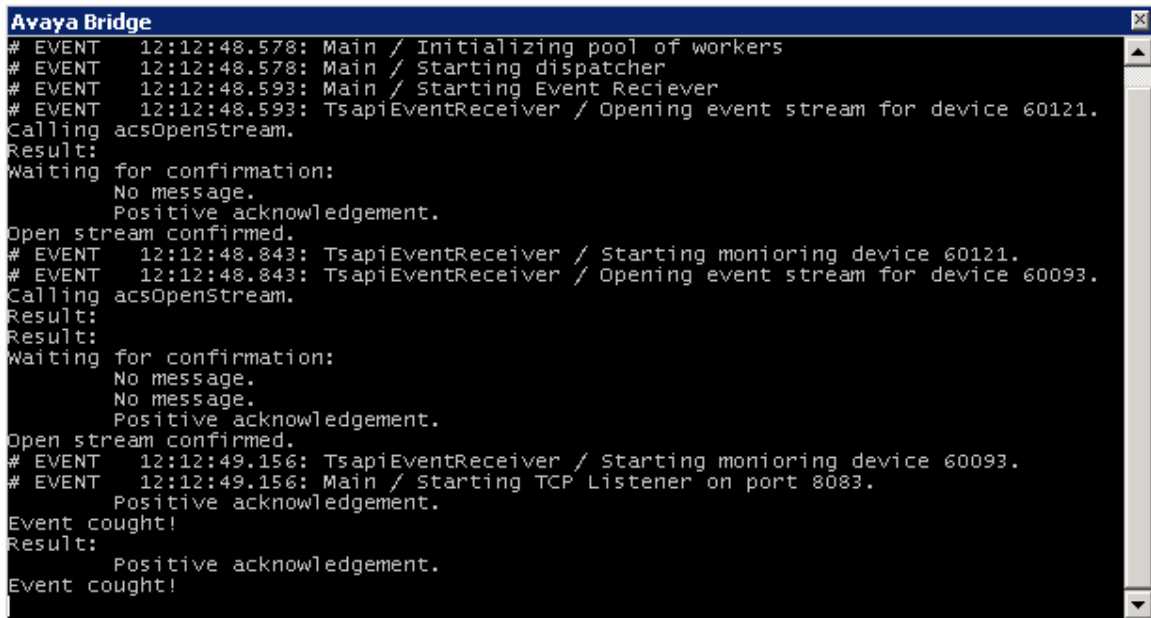
The output of the Cpm Console is then displayed in a command window on the server.



```
Cpm
# EVENT 12:11:38.375: Main / Hello!
# EVENT 12:11:38.375: Main / Loading configuration.
# EVENT 12:11:38.562: Main / Starting listening.
```

**Figure 22: Cpm Console Output**

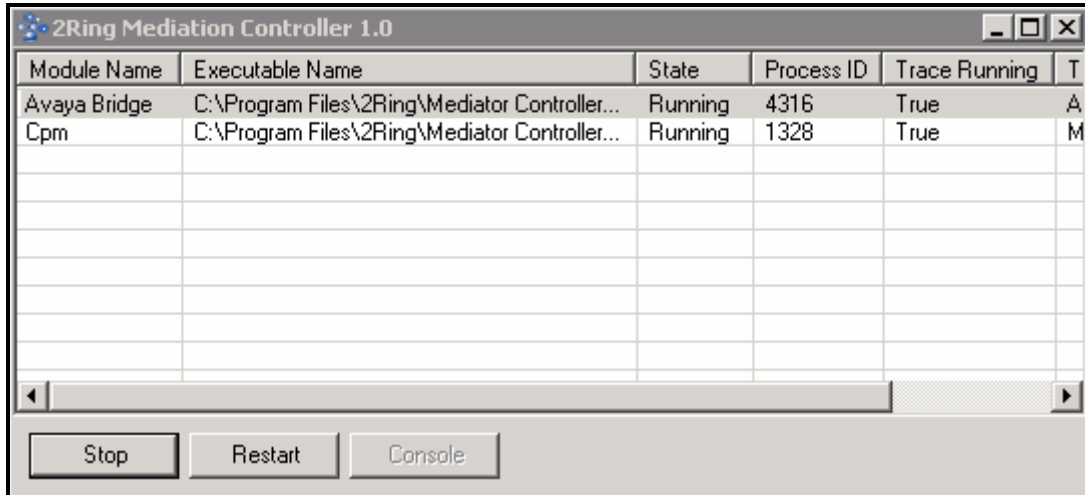
Select “Avaya Bridge” from the screen shown in **Figure 21** and “Start”.



```
Avaya Bridge
# EVENT 12:12:48.578: Main / Initializing pool of workers
# EVENT 12:12:48.578: Main / Starting dispatcher
# EVENT 12:12:48.593: Main / Starting Event Reciever
# EVENT 12:12:48.593: TsapiEventReceiver / Opening event stream for device 60121.
Calling acsOpenStream.
Result:
Waiting for confirmation:
No message.
Positive acknowledgement.
Open stream confirmed.
# EVENT 12:12:48.843: TsapiEventReceiver / Starting monitoring device 60121.
# EVENT 12:12:48.843: TsapiEventReceiver / Opening event stream for device 60093.
Calling acsOpenStream.
Result:
Result:
Waiting for confirmation:
No message.
No message.
Positive acknowledgement.
Open stream confirmed.
# EVENT 12:12:49.156: TsapiEventReceiver / Starting monitoring device 60093.
# EVENT 12:12:49.156: Main / Starting TCP Listener on port 8083.
Positive acknowledgement.
Event caught!
Result:
Positive acknowledgement.
Event caught!
```

**Figure 23: Avaya Bridge Console Output**

The Media Controller UI now shows both services as “Running”.



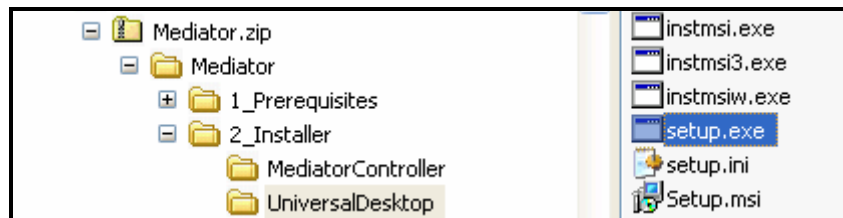
**Figure 24: Mediator Controller User Interface after Services Started**

### 3.4. Configure 2Ring Unversal Desktop Clients

The client to be used with Mediator depends on the environment in which Mediator is used. The client might be a call center agent or an SAP user interface client. Since the verification of Mediator’s interoperability with such clients is outside the scope of the testing described by these application notes, the 2Ring Universal Desktop client included in the 2Ring Mediator software distribution was used for these tests. This is a simple client program which allows a client workstation user to log in to Avaya Communication Manager as an agent, perform telephony operations, and respond to telephony events.

The installation procedure described below installs the Mediator Universal Desktop client application in the client’s “C:\Program Files\2Ring\Mediator Controller” directory. This procedure must be performed for each of the Mediator Client PCs.

Execute the “setup.exe” program from the temporary directory which was copied from the distribution media in **Section 3.3**, as shown below.



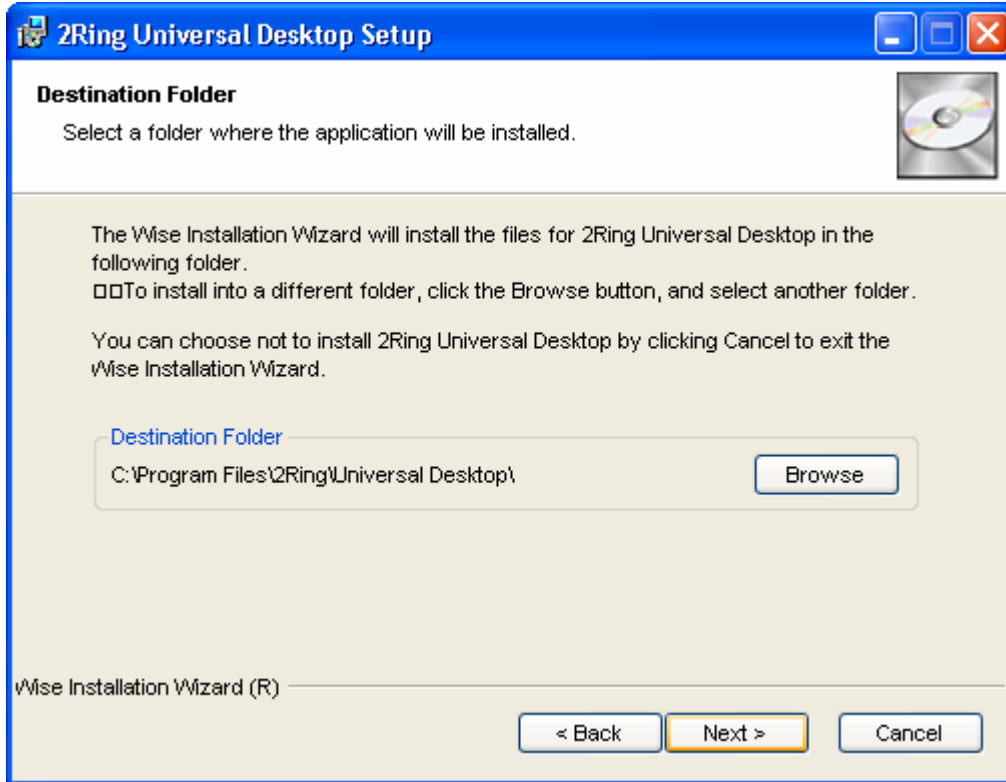
**Figure 25: Client Installation Program**

Click "Next.



**Figure 26: Universal Desktop Installation Welcome Screen**

Click “Next”.

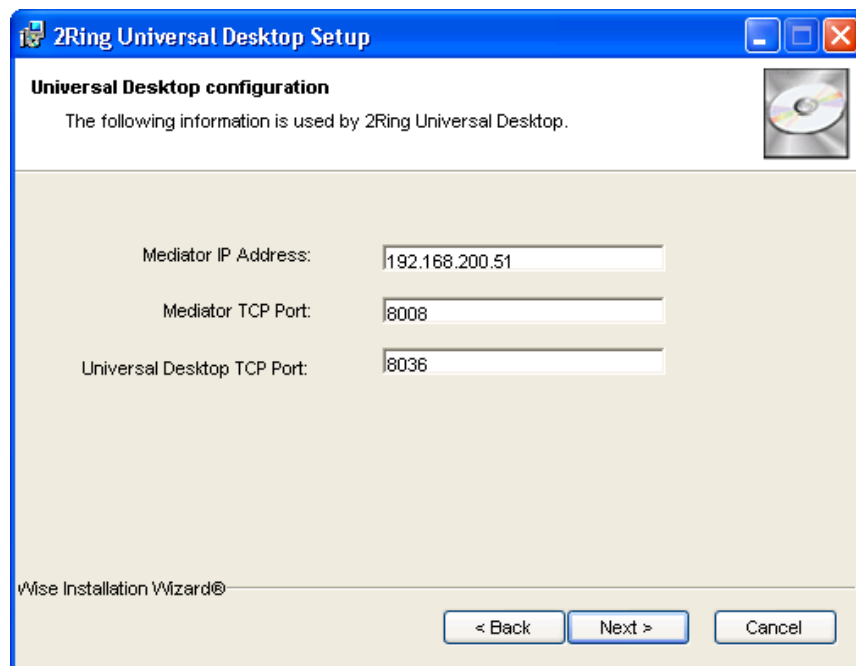


**Figure 27: Universal Desktop Installation Folder Selection Screen**

Enter the parameters for this screen as shown in the following table.

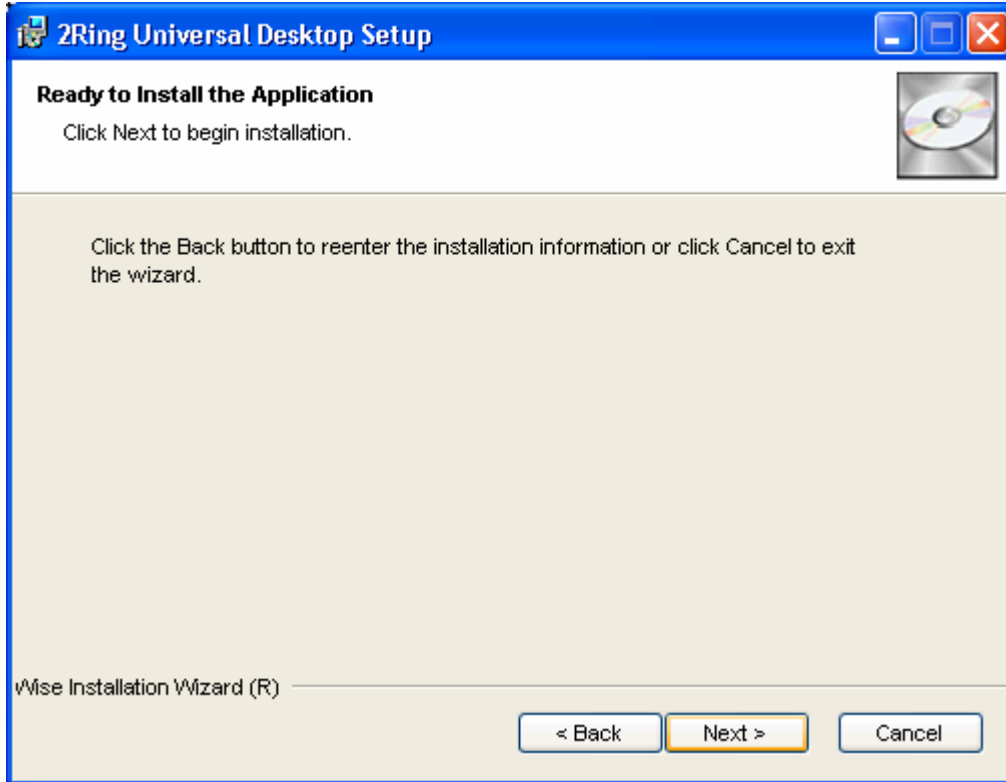
Parameter	Usage
Mediator IP Address	Enter the IP address of the Mediator server.
Mediator TCP Port	Enter the default port address which is configured for Mediator in <b>Figure 18 for the parameter &lt;config&gt;&lt;mediator&gt;&lt;port&gt;</b> .
Universal Desktop TCP Port	Enter the port address to be used by Universal Desktop. Note that this must match the address which is configured for this client in <b>Figure 15 for the parameter &lt;config&gt;&lt;specific&gt;&lt;modules&gt;&lt;module&gt;&lt;port&gt;</b> .

**Table 9: Universal Desktop Address Selection Parameters**



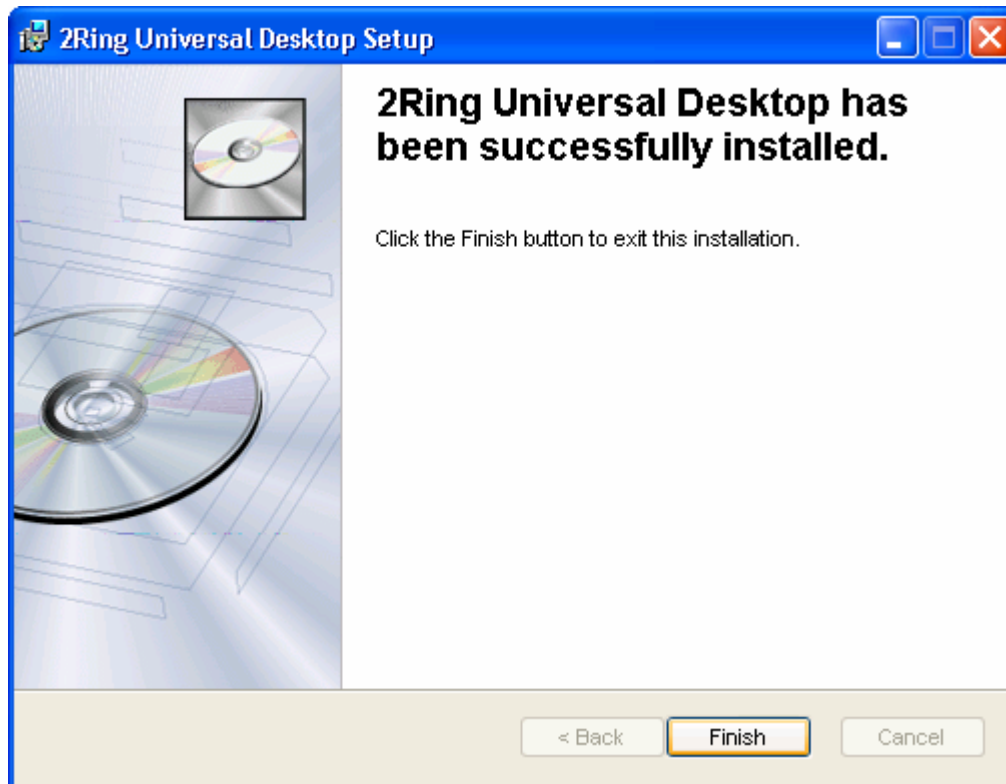
**Figure 28: Universal Desktop Address Selection Screen**

Click “Next”.



**Figure 29: Universal Desktop Confirmation Screen**

Click “Finish” when the following screen appears.



**Figure 30: Universal Desktop Installation Completion Screen**

## 4. Interoperability Compliance Testing

The objective of the compliance testing done on the 2Ring Mediator product was to verify that it is compatible with Avaya Communication Manager. This includes verifying that the essential Mediator features function properly when used with Avaya Communication Manager, and that Avaya Communication Manager features are not hindered by the interaction with Mediator. Furthermore, Mediator’s robustness was verified.

### 4.1. General Test Approach

The test method employed can be described as follows:

- Avaya Communication Manager was configured to support various local IP telephones, as well as a networked PBX connection and a PSTN connection.
- A PSTN interface was attached to Avaya Communication Manager, which was used to communicate with external telephones.
- The following test scenarios were used to test the various Mediator features:
  - Perform agent login/logout from Universal Desktop.
  - Change agent status to ready/not ready from Universal Desktop.
  - Verify that call status changes are reflected correctly by from Universal Desktop.



- Verify that the Universal Desktop can be used to initiate and terminate calls.
- Verify that the Universal Desktop can answer and release incoming calls.
- Verify that the Universal Desktop can reject incoming calls.
- Mediator's robustness was further tested by verifying ability to recover from interruptions to the connection to following components:
  - The Mediator server.
  - The Avaya Communication Manager system with which 2Ring Mediator Server communicates via Avaya Application Enablement Services.

All testing was performed manually. The tests were all functional in nature, and no performance testing was done.

## 4.2. Test Results

All tests produced the expected result.

## 5. Verification Steps

The following steps can be performed to verify the correct installation and configuration of Mediator:

- Log into the Avaya AES and perform the following:
  - Verify that CTI OAM Status and Control "Switch Connection Summary" shows that the connection between Avaya AES and Avaya Communication Manager is operational.
  - Verify that CTI OAM Status and Control "Services Summary" shows that TSAPI service is operational.
- Verify that the AES web interface can be used to make a call between two local extensions.
- Verify that the Mediator service is running via the MS "Services" applet (see **Figure 19**).
- Verify that the Mediator "Avaya Bridge" and "Cpm" services are running (see **Figure 24**).

All tests involving calls were performed with both locally-attached telephone stations as well as telephones attached to the PSTN.

## 6. Support

Support for Mediator is available at:

E-mail: [support@2ring.com](mailto:support@2ring.com)

Phone: +421 2 58224097

## 7. References

- [1] *Administrator Guide for Avaya Communication Manager*, January 2008, Issue 4.0, Document Number 03-300509.
- [2] *Feature Description and Implementation for Avaya Communication Manager*, January 2008, Issue 6, Document Number 555-245-205.
- [3] *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide Release 4.2*, May 2008, Issue 10, Document Number 02-300357.
- [4] *Mediator 2.0 Administration Guide*, September 2008

## 8. Conclusion

These Application Notes describe the conformance testing of the 2Ring Mediator communicating with Avaya Communication Manager via the Avaya Application Enablement Services TSAPI interface. A detailed description of the configuration required for both the Avaya and the 2Ring equipment is documented within these Application Notes. The Mediator passed all of the tests performed, which included both functional and robustness tests.

---

**©2009 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](mailto:devconnect@avaya.com).