Abstract

These Application Notes describe the steps required to integrate Mutare EVM3 with Avaya Aura® Messaging. Mutare EVM3 is a unified messaging solution that delivers voicemail and fax messages to a user's email inbox, smartphone or IM client. In addition, EVM3 provides the Message Archive and the Message Monitor/Escalation features. Message Archive automatically copies and stores all messages on Messaging to a server for permanent storage and retrieval. Message Monitor/Escalation monitors voice mail activity and notifies an escalation agent when a voice message has not been played within a certain amount of time. EVM3 works with Messaging using IMAP and LDAP access. For this compliance test, Google Gmail accounts were used as the email clients.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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 steps required to integrate Mutare EVM3 with Avaya Aura® Messaging. Mutare EVM3 is a unified messaging solution that delivers voicemail and fax messages to a user's email inbox, smartphone or IM client. In addition, EVM3 provides the Message Archive and the Message Monitor/Escalation features. Message Archive automatically copies and stores all messages on Messaging to a server for permanent storage and retrieval. Message Monitor/Escalation monitors voice mail activity and notifies an escalation agent when a voice message has not been played within a certain amount of time. EVM3 works with Messaging using IMAP and LDAP access. For this compliance test, Google Gmail accounts were used as the email clients.

2 General Test Approach

To verify interoperability of Mutare EVM3 with Avaya Aura® Messaging, voice messages were left for subscribers and EVM3 was used to send those messages to a recipient's email inbox. In addition, voice messages were archived and accessed from the EVM3 server using the Message Archive feature. Voice mail activity was also monitored for select mailboxes and notifications were sent to an escalation agent using the Message Monitor/Escalation feature.

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

Interoperability compliance testing covered the following features and functionality:

- EVM3 connectivity to Messaging using IMAP and LDAP access.
- Voice messages delivery to recipient’s email inbox.
- The voice message headers were verified indicating the caller ID and if the voice message was marked as private, important, forwarded, or a reply message.
- Archiving and accessing voice messages on the EVM3 server using the Message Archive feature.
- Monitoring voice mail activity for select mailboxes in real-time.
- Email escalation notifications to an escalation agent using the Message Monitor/Escalation feature.
- Voice message synchronization between Messaging and the EVM3 server.
- Proper system recovery after a reboot of the EVM3 server and loss of IP connectivity.

2.2 Test Results

All test cases passed. Voicemail to a recipient’s email inbox, archiving and retrieving old messages, and sending notifications to an escalation agent or alternate contact were verified.
2.3 Support
For technical support on EVM3, contact Mutare Support via phone or email.

- **Phone:** (855) 782-3890
- **Email:** help@mutare.com
- **Website:** [http://www.mutare.com/support.asp](http://www.mutare.com/support.asp)
3 Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following Avaya products:

- Avaya Aura® Communication Manager running on an Avaya S8800 Server with a G650 Media Gateway.
- Avaya Aura® Messaging served as the voicemail system.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk that provides SIP connectivity for Avaya Aura® Messaging.
- Avaya Aura® System Manager used to configure Session Manager.
- A desktop PC used to access Google Gmail email client. The EVM3 server used SMTP to deliver emails.

In addition, the Mutare EVM3 application was running on a separate server and configured via a Web browser. The network also provided internet connectivity (not shown).
4  Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Hardware Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager running on a S8800 Server with a G650 Media Gateway</td>
<td>6.3.9 SP 9.1 (R016x.03.0.124.0 with Patch 22098)</td>
</tr>
<tr>
<td>Avaya Aura® Messaging</td>
<td>6.3.2 SP 2</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>6.3.11.0.631103</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>6.3.11 Build No. 6.3.0.8.5682-6.3.84751</td>
</tr>
<tr>
<td></td>
<td>Software Update Revision No: 6.3.11.8.2933</td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephones</td>
<td>3.240A (H.323)</td>
</tr>
<tr>
<td>Mutare EVM3 running on Microsoft Windows Server 2008</td>
<td>3.0.5</td>
</tr>
<tr>
<td>Mutare Message Monitor/Escalation</td>
<td>1.1.3</td>
</tr>
</tbody>
</table>
5 Configure Avaya Aura® Messaging

This section provides the procedures for configuring Messaging for integration with EVM3. The procedures include the following areas:

- Enable IMAP and LDAP on System Ports and Access
- Add a Trusted Server for the Mutare EVM server

It is assumed that Messaging has already been configured and connected to Session Manager and Communication Manager as described in [1].

5.1 Enable IMAP and LDAP

From a web browser, enter the Messaging IP address as the URL to access the Messaging web interface. Navigate to Administration ➔ Messaging and then click on System Administration in the left pane. Scroll down to the System TCP/IP Ports section. Configure and enable the LDAP and IMAP ports. The LDAP Port is 389 and the LDAP SSL Port is 636. The IMAP4 Port is 143 and the IMAP4 SSL Port is 993. These are the default ports and should match on EVM3.
5.2 Add Trusted Server

From the Messaging web interface, add the EVM3 server as a trusted server. Configure the fields as shown below and click Save.

- **Trusted Server Name**
  Set to *mutare* in this example.

- **Password and Confirm Password**
  Create a password for the trusted server.

- **Machine Name / IP Address**
  Specify the IP address of the EVM3 server.

- **Service Name**
  Set to *Mutare* in this example.

- **LDAP Access Allowed**
  Enable this option.

- **IMAP4 Super User Access Allowed**
  Enable this option.

- **IMAP4 Super User Connection Security**
  Set to *Must use SSL or encrypted SASL.*

![Add Trusted Server Interface](image_url)
6 Configure Mutare EVM3
This section covers the configuration of EVM3, including the Message Archive and Message Monitor/Escalation features. Refer to [2] for additional information on configuring EVM3.

6.1 EVM3 Administration
This section covers the configuration of EVM3, which includes the following procedures:

- Configure Microsoft IIS
- Run evm2config.exe to set up connectivity to the SQL database and configure an EVM3 Site.
- Configure EVM Settings
- Configure EVM Devices
- Configure EVM Device Groups
- Add EVM Users
- Edit EVM User Settings

6.1.1 Configure Microsoft IIS
EVM3 requires that SMTP be configured in Microsoft Internet Information Services (IIS) in order to send emails. In this compliance test, emails were sent to a Google Gmail account. The SMTP configuration may vary depending on which email system is being used. Therefore, general configuration guidelines are provided.

From IIS, open the SMTP Properties window as shown below.
In the SMTP Properties windows, navigate to the Delivery tab shown below.

From SMTP Properties, click on the Outbound Security button to configure the Basic authentication and enable TLS encryption, if required. For Google Gmail, the following configuration was used. The User name and Password should correspond to a valid email account.
From SMTP Properties, click on the **Outbound Connections** button to configure the appropriate **TCP port** as shown below. In this configuration, TCP port 587 was used.

![Outbound Connections](image1.png)

Lastly, from SMTP Properties, click on the **Advanced** button to configure the SMTP IP address or FQDN in the **Smart host** field as shown below. Click **OK**.

![Advanced Delivery](image2.png)
6.1.2 Run evm2config.exe

Prior to configuring EVM3, run `evm2config.exe` located in the `C:\OD\Programs` directory to set up connectivity to the SQL database and add a valid license. In addition, additional attributes need to be configured for the specified Site Name (e.g., (1)-EVM). Specify the Retrieval Method (IMAP4), System Type (Custom), and Custom Type (AAM) as shown below.

6.1.3 Configure EVM Settings

Using a web browser, go to the EVM Administration webpage using the following URL, `http://<EVM IP Address>/adminlogin.asp`. The following login page is displayed. On the EVM Admin Login page, log in with the appropriate credentials.
Once successfully logged in, navigate to the **EVM Settings** page by selecting the **Settings** option in the menu at the top of the page. There are many different parameters available in EVM3, but most parameters have default values that do not have to change. This section will provide a brief description of the parameters, while the settings of others will just be included in the EVM Settings page shown below.

- **ArchivePath**
  - Set to the message archive directory.

- **EmailFrom**
  - Specify the “Email from” address to use for emails sent to users.

- **EVMURL**
  - Specify the base URL to use for EVM3 links in email messages.

- **ServerIP**
  - Specify the Messaging IP address.

- **ServerPort**
  - Specify the LDAP port used on Messaging.

- **SuperLogin**
  - Set to the user name specified in the Trusted Server configured on Messaging.

- **SuperPwd**
  - Set to the password for the Trusted Server configured on Messaging.

- **UseEvents**
  - Specify whether to process new voicemails based on events.
6.1.4 Configure EVM Devices

EVM sends voicemail deliveries and notifications to different devices. Many devices have specific requirements, such as an audio file in a certain format. Navigate to Devices page shown below and configure the Desktop EVM and EVM3 devices by clicking on the respective Config button.
In the **EVM3** and **Desktop EVM Config** pages, configure the EVM3 email address in the **From Address** field as shown below.

![EVM Device Email](image.png)

### 6.1.5 Configure EVM Device Groups

Navigate to **Device Groups**, and choose **Devices** based on the users that will be in the group and what options they require. In this example, the **Desktop EVM** and **EVM3** devices were added to the **Main** group as shown below.

![EVM Device Groups](image.png)
6.1.6 Add EVM Users
Navigate to the EVM Users webpage to add a user by clicking on the Users option at the top of the page. The following example shows user 77302 being added. Specify the Mailbox extension, Name, and the Device Group. Click Add to add the user to the EVM database.

![EVM Users webpage example](image1)

6.1.7 Edit EVM User Settings
To access a user’s EVM settings, click on the View hyperlink in the EVM Users page above. The following page will be displayed. In the user’s EVM Settings page, click Add Device to add a user device. In the following example, an EVM3 device is added, and by default it is activated. The Desktop EVM device may also be added by clicking the Add Device button again, if required. A device requires the user’s Email Address (e.g., ip.77302@gmail.com). The user settings also allow voice messages to be sent in .wav audio format to the recipient’s email inbox. Click Save to save the settings.

![EVM Settings webpage example](image2)
# 6.2 Message Archive

Message Archive for Messaging automatically copies and stores all messages on the voicemail system to a server for permanent storage and easy retrieval. Message Archive is accessed through EVM3. The only configuration required for the Message Archive feature is the `ArchivePath` parameter in the EVM _Settings_ page, which should be set to the message archive directory as shown in Section 6.1.3. To access the usage report and archived messages, select the `Archive` option from the EVM Administration webpage. The EVM Archive webpage is displayed below with links to the Usage Report and Archived Messages. Ensure that the checkbox by the device group, *Main*, is selected.

![Image of EVM Archive page](image-url)
6.3 Message Monitor/Escalation

Message Monitor/Escalation is a web tool used by administrators to track and view mailbox activity as it takes place in real-time. It monitors the message waiting status on selected voice mailboxes and sends a notice in an escalating pattern to backup contacts. Once all waiting messages are played, the escalation process automatically ceases.

Prior to configuring Message Monitor, run MsgMonConfig.exe located in the C:\OD\Programs directory to set up connectivity to the SQL database and add a valid license for the site as shown below.

To configure the Monitor/Escalation feature, browse to the Message Monitor/Escalation administration webpage using the following URL, http://<EVM IP Address>/monitor, and log in with the appropriate credentials.
The Message Monitor/Escalation administration webpage is displayed as shown below. Click on the **Settings** link.

![Message Monitor/Escalation webpage](image)

- **Mailbox Capacity**: 2 users, with 0-50% of capacity used.
- **Recorded Name/Greeting**: 2 users, both named and greeted.
- **Oldest Unplayed Messages**: 2 messages, all less than 1 hour old.
- **Average Wait Time by Mailbox**: 2 messages, all less than 5 minutes old.
In the **Settings** webpage, set the **MSS Host** field to the Messaging IP address and set the **MSS Port** field to IMAP port 143 as specified in **Section 5.1**. Specify the login credentials as configured in the **Trusted Server** on Messaging as shown in **Section 5.2**. The **MSS Login** field should be set to the Trusted Server Name and the **MSS Password** field should be set to the Password of the Trusted Server. Also, enter the appropriate **License Key** as shown below. Click **Save**.

![Message Monitor / Escalation](image)
After configuring the settings, return to the home page and add a user’s voice mailbox to monitor as shown below and click **Add**.

Next, add an escalation agent by navigating to **Escalation → Agents** starting from the home page. Configure an escalation agent as shown below by specifying the **Agent ID**, **Agent Name**, and **Email**. Select the **Active** checkbox and then click **Add**.
Return to the **Escalation** webpage and select the user’s mailbox previously added. In addition, specify the escalation pattern for this mailbox. In the following example, the first escalation notice will be sent 1 minute after the voice message has been left if it hasn’t been played yet. The subsequent escalation will take place 3 minutes later. In the **Agents** column, the escalation agents that should receive the first and second notices are specified. Click **Save**.
7 Verification Steps

This section provides the steps that may be performed to verify proper configuration of Mutare EVM3 with Avaya Aura® Messaging.

1. Run MMTest.exe located in the C:\OD\Programs directory to verify EVM3 connectivity to Messaging. The window below is displayed. Specify the Messaging information, including the IP address, IMAP4 port, and login credentials of the Trusted Server. In addition, specify the mailbox extension and click Connect. Any voice message for the specified mailbox will be displayed in the window below.
2. From the EVM Administration webpage, click on **Status** to verify that EVM is running as shown below.
3. Leave a voice message for a user and verify that the voice message is sent to the recipient’s inbox as shown below.

The voicemail email appears as follows when opened when the Desktop EVM device group is used.
4. Navigate to the **Archived Messages** and verify that the previous voice messages are stored on the server as shown below. To the right of the screen, there are options to listen to the message.

![Archived Messages](image)

5. In **Message Monitor/Escalation**, navigate to the messages of a monitored mailbox to check the status indicating whether it has been received, played, or deleted as shown below.

![Message Monitor/Escalation](image)
6. Navigate to **Escalation Details** to check if any escalation have taken place as indicated in the **Level** column.
8 Conclusion

These Application Notes have described the administration steps required to integrate Mutare EVM3 with Avaya Aura® Messaging. EVM3 was successful in sending email notifications with voice messages to a recipient’s inbox, archiving the voice messages, and monitoring voice mail activity and sending escalations to alternate contacts. All test cases passed with observations noted in Section 2.2.

9 References

This section references the Avaya and Mutare documentation relevant to these Application Notes. Avaya product documentation is available at http://support.avaya.com.

©2015 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.